РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»

Это руководство “Практика управления рисками в статистических организациях”, было подготовлено под эгидой Группы Высокого Уровня ЕЭК ООН по модернизации официальной статистики, Комитетом по организационной структуре и оценке, под председательством Джеки Майды (Статистическое Управление Канады).

В основном руководство было подготовлено группой специалистов из Статистического Управления Италии во главе с Фабрицио Ротунди, в сотрудничестве с командой, координируемой профессором Алессандро Хинной из Римского Университета “Тор Вергата”. Руководство содержит раздел посвященный гибкому управлению рисками, подготовленный “Целевой группой по управлению рисками в контексте гибкого развития”, под руководством Бена Уитстоуна и Рича Уильямса (Управление национальной статистики Великобритании).

Версию руководства в формате PDF можно скачать здесь: **Guidelines on Risk Management Practices in Statistical Organizations**

Руководство «Практика управления рисками в статистических организациях»

Резюме

Раздел 1 СТРУКТУРА УПРАВЛЕНИЯ РИСКАМИ

РАЗДЕЛ 2 ПРОЦЕСС УПРАВЛЕНИЯ РИСКМИ

РАЗДЕЛ 3 УКРЕПЛЕНИЕ СЕЩУСТВУЮЩЕГО УПРАВЛЕНИЯ РИСКМИ В НАЦИОНАЛЬНЫХ СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ГИБКИХ ПРИНЦИПОВ

Error rendering UI Children macro: No valid page was given. Please provide a valid page. Note: Blogpost can not be used!

Выражение признательности

- Рабочая команда
- НСО и статистические организации

Annex - Focus on risk management

Section 1. Risk framework

Section 2. Risk management process

- Chapter 4: Risk treatment
- Chapter 7: Risk management information system
- Chapter 8: Risk management maturity model
- Chapter 9: Lessons learned
- Chapter 10: Enhancing Existing Risk Management in National Statistical Institutes by Using Agile Principles

http://www1.unece.org/stat/platform/display/GORM/List+of+reviewsList of reviews

http://www1.unece.org/stat/platform/display/GORM/ReferencesReferences

Глоссарий

Резюме

1. Введение

Данные руководящие принципы по осуществлению управления рисками в статистических организациях были разработаны при координации группы высокого уровня по вопросам модернизации официальной статистики ЕЭК ООН, Комитетом по модернизации организационной структуры и оценки (КМОСО), под председательством Джейки Майда (Статистическое управление Канады).

Проект, в основном, выполняла рабочая группа из итальянского статистического управления (Итстат) во главе с Фабрицио Ротунди в сотрудничестве с командой, координируемой профессором Алессандро Хинна из Римского университета «Тор Вергата».

В Руководстве содержится специальный раздел «Гибкость в управлениии риском», подготовленный «Целевой группой по управлению рисками в контексте развития гибкости» под руководством Бена Уитстоуна и Рита Уильямса (Британское бюро национальной статистики). Данный раздел был добавлен по просьбе участников семинара по вопросам управления рисками, проведённого в Женеве 24-25 апреля 2016 года.

2. Значение руководящих принципов для статистических организаций

национальных статистических организаций (НСО), поскольку это касается как организационных, так и производственных процессов. Фактически, управление рисками, с одной стороны, нацелено на усиление организационного управления в целом, поддерживая процесс принятия решений при выборе приоритетов; с другой стороны, его целью является выявление, анализ и устранение неопределенностей, которые могут препятствовать процессу работы над качеством.

Цель данных руководящих принципов предоставить национальным статистическим организациям (НСО), заинтересованным в непосредственном осуществлении системы управления рисками, ссылку на практику, разработанную в рамках организаций ЕЭК ООН, содержащую некоторые ключевые факторы: эффективное развитие, устойчивость (с точки зрения ресурсов и сложности), согласование с процессами управления, изменениями.

Таким образом, задача состоит в том, чтобы найти практику управления рисками, которая может быть организована в соответствии с потребностями НСО, без необходимости «самой лучшей» в теоретическом или методологическом смысле, скорее реально осуществимым методом.

Исходя из практики, уже используемой теми НСО, которые в настоящее время участвуют в процессах модернизации, следует способствовать положительной динамике дискуссии

целью извлечения выгоды из положительного опыта, приспосабливая его к внутреннему контексту - дабы было возможно избежать или легко устранить самые повторяющиеся ошибки в процессах принятия решений.

Это также может привести к стандартизации процессов управления, в соответствии с с производственными процессами(см. «Общий типовой процесс статистического производства» и «Общая модель активности статистических организаций»). Однако, необязательно, что такой подход может создать общий разнообразный регистр рисков (организационный, статистический, информационно-технологически и т.д.), кторый позволит НСО заблаговременно разрабатывать надлежащие процедуры.

3. Три опроса для получения информации и подробного анализа

Три опроса были проведены следующим образом.

1-ый опрос на тему практики управления рисками

В этом опросе была собрана информация об уровне развития систем и методов управления рисками в НСО. Он было проведен во всех НСО ЕЭК ООН с общим коэффициентом ответов более 50%. Данный опрос собрал информацию о следующем:

- Применение управления рисками;
- Характерные особенности введённого процесса управления рисками;
- Характерные особенности процесса внедрения управления рисками;
- Заключительные замечания по процессу и системе управления рисками.

2-ой опрос - углубленный и краткий опрос

Среди НСО, ответивших на первый опрос, некоторые страны были отобраны для предоставления конкретной информации о методах управления рисками, которые, как представляется, особенно актуальны для НСО. Второй опрос был адресован 14 организациям, 7 - для углубленного опроса и 7 - для краткого. Общий коэффициент ответов составил почти 80%. Была собрана следующая информация:

1. Углубленный опрос

- **Качественные и контекстно-аналитические углубленные вопросы,** составленные в соответствии с ограниченным набором элементов, которые считаются основными, а также стратегическими для поиска практики применения
- **Запрос на методологические или оперативные документы,** к которым можно получить доступ или предоставить общий доступ (то есть формализованные организационные процедуры);
- **Количественные вопросы**, предназначенные для оценки с помощью ситуативных показателей адаптации / тиражирования практики в других контекстах, кроме стран, которые разработали или приняли их.

2. Краткий опрос

Краткая анкета была применена в НСО, и в первом опросе дала результаты о методах управления рисками, показывающие некоторые конкретные особенности, которые были выявлены другими НСО. Краткий опрос собрал качественную и количественную информацию, включая количество рисков, преданный делу персонал, обученный персонал и т. д.

3-ий опрос - углубленный и краткий опрос

С целью утверждения и подкрепления руководящих принципов, было подготовлено заключительное исследование для получения полной картины способов внедрения систем управления рисками среди статистических организаций. Оно включило в себя шесть различных вопросников, касающихся управления рисками; статистический анализ качества; управление статистическим производственным процессом; управление организационными процессами; внутренний контроль и / или внутренний аудит; услуги, поддерживающие статистическое производство. Образец состоял из организаций, представляющих разные уровни зрелости рисков; поэтому подход был достаточно всеобъемлющим, чтобы уловить различные перспективы и выявить элементы, которые, насколько это возможно, представляют различные анализируемые контексты. В каждом вопроснике основное внимание уделялось четырем основным темам:

I. Структура управления рисками

II. Процесс управления рисками

III. Обширные процессы

IV. Зрелость риска в организации

По каждой теме респондентам задавали вопрос:

- ЧТО БЫЛО САМЫМ УСПЕШНЫМ ?»: что было самым эффективным для организации, в результате внедрения управления рисками;
- «ЧТО БЫЛО САМЫМ ТРУДНЫМ?»: какие основные препятствия были при разработке управления рисками;
- «ЧЕГО НЕ НАДО ДЕЛАТЬ?»: согласно опыту НСО, участвующим в ОПРОСЕ, какие ошибки лучше не повторять при внедрении управления рисками.

Результаты были проанализированы с целью прослеживания каждого элемента относительно трех категорий, которые стимулировали весь процесс: эксперты по вопросам рациональности, проблематичности и технологий. Исходя из данного различия, , были сопоставлены основные функции, которые могут способствовать успеху или неудаче при внедрении систем управления рисками в НСО.

back to top

4. Краткий обзор содержания руководящих принципов

Руководящие принципы структурированы в соответствии со стандартами МОС (Международная Организация по Стандартизации) - 31000: 2009; этот стандарт широко используется в международном практике, а также большинством общественных организаций при внедрении систем управления рисками.

Структура, заложенная в основе руководства, начинается с опыта, стандартов и / или других методологических ссылок. Она соответствует информации для анализа практики, собранной в ходе трех опросов. Затем приводятся направления внедрения системы управления рисками, которые можно осуществить в статистических организациях. В некоторых случаях в руководстве приводятся выдержки из вопросников вместе с соответствующими ответами, с целью трансформации содержания в контекст.

Более подробно, два основных раздела Руководства расположены следующим образом:

1. **. Создание системы управления рисками.** Этот раздел начинается с наблюдения за стратегическими компонентами: от общих определений риска и управления рисками до описания мандата и политики управления рисками,которые включают выбранную схему принятия решений, а также выбранный подход к интеграции технологий и процессов управления. Затем в разделе рассматриваются активы и управление персоналом, в частности, обучение, сопоставление компетенций, назначение ролей и ответственности, а также возможность создания специального офиса / подразделения. Эта часть руководства даёт подсказку на процесс управления рисками (тема разработана во втором разделе), в то время как особое внимание уделяется созданию информационных потоков, а также мониторингу самой системы управления риском, а также через систему отчетности на разных уровнях.
2. **Разработка процесса управления рисками.** Путем балансирования источников информации и практики, как в первой части руководства, в этом разделе описываются все этапы процесса управления рисками: от сквозных консультаций и общения с заинтересованными сторонами до контекстного анализа, включая картографирование процессов, идентификацию, определение приоритетов, обработку риска и (подхода). Кроме того, существуют направления, относящиеся к системам управления и внутреннему аудиту, а также к индикаторам, измеряющим как эффективность, так и состояние рисков. В данной части руководства также содержится описание некоторых контекстных функций, связанных с реализацией системы управления рисками, то есть требований к вспомогательным информационным системам, моделей для оценки уровня зрелости систем управления рисками и «извлеченных уроков» при разработке таких систем. К «урокам» относятся, в частности, то, что было наиболее успешным, что было самым трудным и чего не следует делать. Второй раздел заканчивается абзацем по гибкому подходу по отношению к управлению рисками, подготовленному целевой группой ЕЭК ООН по этой теме.

Наконец, руководящие принципы включают еще три элемента:

- **Приложения**, которые показывают более практический подход к различным областям управления рисками, описывая две категории примеров:

- Концентрация внимание на основные вопросы управления рисками, разработанных в руководящих принципах;

- Тематические исследования, описывающие весомый опыт некоторых НСО в отношении конкретных особенностей систем управления рисками;

- **Ссылки**, связанные с основными источниками руководящих принципов: стандарты и международные руководящие принципы, специальная литература, углубленный анализ и конкретный опыт;
- **Глоссарий,** содержащий основные термины и фразы, соответствующие тематике руководства.

РАЗДЕЛ 1: Структура управления рисками

Резюме | РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ» | РАЗДЕЛ 2: Процесс управления рисками

1. Организация системы управления рисками

РАЗДЕЛ 1: Структура управления рисками | 2. Ресурсы для управления рисками

Структура (система) управления рисками[1] предусматривает инфраструктуру для проведения, сопровождения и контроля процесса управления рисками по всей организации. В рамках такой инфраструктуры организация должна предусмотреть:

а) Мандат на управление рисками – заявление совета о направлении и приоритетах в управлении рисками, а также создание структуры «кто что делает», после чего выдается соответствующее разрешение и необходимые ресурсы. Является основным выражением управления риском, посредством которого совет организации привлекает заинтересованные стороны в процесс определения разных ответственностей за управление рисками.

б) Стратегия риска, указывает, как управление рисками дополняет общую стратегию организации и связанные задачи. При этом учитывается внешний и внутренний контекст, и особое внимание уделяется потребностям ключевых заинтересованных сторон.

в) Политика рисков предусматривает четкое и краткое содержание требований организации к управлению рисками в рамках общего подхода организации к управлению. Включает заявление о готовности к принятию риска, программу подготовки человеческих ресурсов для поддержки процесса управления рисками, а также определение критериев оценки риска.

г) Комплексный риск-ориентированный подход дополняет процесс управления качеством в совершенствовании целостности и качества статистических данных через определение, анализ и обработку рисков, присущих статистическим и всеохватывающим процессам.

[1] В стандарте AS/NZS 4360:2004 используется следующее определение структуры управления рисками: «*набор элементов системы управления организации, относящихся к управлению риском*». В рамках настоящего проекта, пункты «структура УР» и система «УР» применяются в качестве синонимов.

1.1 Определение риска и управления рисками

1. Организация системы управления рисками	1.2 Мандат и стратегия управления рисками	

Управление рисками - это организационная модель, направленная на развитие качества процессов управления. Она выявляется путем анализа событий, которые никогда по сути не возникали внутри организации.

В отличие от большинства управленческих систем, управление рисками не пересекается с другими внутренними средствами контроля, поскольку оно представляет собой другую перспективу, которая включает в себя планирование и контроль, систему оценки эффективности, аудита, качества и т. д.

Поэтому управление рисками помогает организациям повышать качество услуг и продуктов, поскольку оно поддерживает процессы принятия решений, готовит к трудностям, которые могут помешать достижению стратегических целей.

В общих чертах, главная задача управления рисками это защита и укрепление и касается следующего:

- Ценности, этика и ощущение сопричастности
- Материальные и нематериальные активы субъектов
- Рост организационной культуры
- Лидерство и отношения
- Эффективность и производительность процессов
- Ресурсы для стратегических приоритетов
- Заинтересованность патрнёров

Это означает, что управление рисками можно рассматривать как инструмент эффективного управления организацией. Фактически, оно касается рисков и возможностей, влияющих на создание или сохранение ценности предприятия. По определению Комитета спонсорских организаций Комиссии Тредуэя управление рисками это - *«процесс, осуществляемый советом директоров, руководством и другим персоналом организации, применяемый в стратегии и на предприятии, предназначенный для выявления потенциальных событий, которые могут повлиять на организацию, и управлять рисками на протяжении нарастания риска , с целью обеспечения достаточной гарантии в отношении достижениия целей организации».*

Определение отражает некоторые основные концепции; в частности, управление рисками:

-
    - Текущий процесс, происходящий в организации
    - Воздействие людей на всех уровнях организации
    - Применение при разработке стратегии
    - Применение всецело, на каждом уровне и подразделении предприятия и включает в себя анализ портфеля уровней рисков предприятия
    - Предназначение в выявлении потенциальных событий, которые, в случае, если они произойдут, повлияют на сущность; и управление риском в пределах приемлемых параметров готовности
    - Способность предоставлять достаточную гарантию руководству и совету директоров
- Ориентирование на достижение целей в одной или нескольких отдельных, но пересекающихся категориях

Это определение целенаправленно распространенное. Оно охватывает ключевые концепции, основанные на том, как компании и другие организации управляют рисками, обеспечивая фундамент для применения в разных организациях, отраслях и секторах. Основное внимание в нем уделяется достижению целей, установленных конкретной организацией, и обеспечивает основу для определения эффективности управления рисками на предприятиях.

Управление рисками рассматривает события, которые оказывают негативное воздействие; они представляют собой риски, которые могут препятствовать созданию ценности или разрушать существующее значение.
В литературе и в стандартах, наиболее признанных на международном уровне, существует множество определений рисков; стандарт Международной организации по стандартизации (МОС) 31000: 2009 определяет риск как: «влияние неопределенности на цели», где «влияние является отклонением от ожидаемого (положительного и / или отрицательного), часто выражаемого с точки зрения сочетания последствий событие (включая изменения обстоятельств) и связанную с ним вероятность возникновения », а неопределенность это – «отсутствие информации о понимании или знании события, его последствиях и вероятности”.

На самом деле концепция риска более сложна, чем сочетание вероятности и эффекта; он включает в себя некоторые вопросы, рассматриваемые когнитивным анализом, имеющим отношение к организации, в том числе:

- Профиль риска: набор рисков, которые могут повлиять на всю или часть организации;
- Готовность к принятию риска: общая сумма и тип рисков, которые организация решает принять на себя, управлять или внедрять
- Восприятие риска, в котором описывается, как люди воспринимают риски в соответствии с их ценностями и интересами
- Отношение к риску (Существующая характеристика рисков). Если организация особенно эффективна в управлении определенными типами рисков, она может быть склонна к большему риску в этой категории, и наоборот, она может быть не готова в данной области.
- Принятие риска, касающееся максимального потенциального воздействия риска, которое может выдержать организация. Часто уровень готовности к риску буде гораздо ниже принятого.
- Потенциал несения рисков это максимальный уровень риска, который может принять организация, не нарушая регулятивное бремя;
- Способность удержания рисков, в котором учитываются ориентировочные показатели прибыли заинтересованных сторон и очень низкую готовность к принятию риска.

- Толерантность к риску, что представляет собой уровень вариативных решений, которые компания готова принять по конкретным целям.

Все эти вопросы следует рассматривать для оценки общего уровня риска организации.

Таким образом, определение «факторов стимулирования» и «причин», связанных с риском, может в значительной степени способствовать определению контекста, в котором может возникнуть риск, позволяющего лицам ответственным за риски принимать необходимые превентивные меры.

Хотя стимулирующий фактор представляет собой организационное / социальное / экологическое обстоятельство, которое способствует поведению и может привести к риску, первопричиной является обстоятельство, в связи с которым было предпринято действие. Поэтому анализ основных причин может помочь организациям различать риски, которые можно эффективно преодолеть из тех, которые можно преодолеть лишь частично.

Что касается определения риска, то следует учитывать некоторые вопросы[2]:

- Отчет о рисках должен быть ясным, содержательным и кратким заявлением, в котором описывается риск. Например: *Возрастающие сложности в установлении контакта с респондентами исследования домашних хозяйств могут негативно повлиять на качество наших данных.*
- В заявлении должно быть описано событие и возможное влияние этого события на достижение целей организации. Например: *существует риск того, что (событие) .... и последствия (воздействие)* ...
  Перед тем, как будет оказано какое-либо воздействие на риск, мероприятие включает «неотъемлемый риск», онтологически связанный с деятельностью, которая может определять само событие. После того, как были предприняты меры по смягчению последствий, все, что осталось, - это «остаточный риск», значение которого может быть равно, больше или меньше «неотъемлемого риска".
- Хороший отчет о рисках должен также включать возможные причины (стимулирующие факторы). Например: *существует риск того, что (событие) ... из-за (причины) ... и последствия будут (воздействие) ...; Учитывая, что ... существует риск того, что ... с потенциальным воздействием ....*

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) - Internal Control - Integrated Framework, 1992,2004,2013

[2] Источник: “Усовершенствованное мероприятие2014 года Статистического управления Канады по операционным рискам ” –Статистическое управление Канады file:///C:/Users/KOLOMI~1/AppData/Local/Temp/notes256C9A/01%20Unece%20Guidelines%204.5%20DRAFT%20FINAL.docx#_ftnref2

1.2 Мандат и стратегия управления рисками

1.1 Определение риска и управления рисками	1. Организация системы управления рисками	1.3 Выработка политики управления рисками

ТЕГИ: Философия, мандат, объем, план.

Стратегия управления рисками включает определение объема и плана управления рисками, а также обсуждение философии управления рисками.

I. Философия риска

Философия управления рисками – это набор общих убеждений и установок, которые описывают то, как риск учитывается в деятельности организации. Влияет на способы

применения компонентов управления рисками, в том числе на способы выявления рисков, виды принятых рисков, а также на методы их управления.

Если философия управления рисками не сформирована, не изучена или недостаточно понимается персоналом, существует вероятность того, что процесс управления рисками в хозяйственных единицах, формированиях или департаментах будет применяться неравномерно. Даже если философия имеет хорошо разработанную структуру, могут по-прежнему обнаруживаться культурные различия в единицах, вызывая разное применение процесса общеорганизационного управления рисками.

Поэтому философия риска, готовность к принятию риска и стратегия риска должны всегда соответствовать друг другу, поскольку одно отражает другое. Для этой цели необходимо «измерить» восприятие риска руководящим персоналом (некоторые руководители могут быть готовы к принятию дополнительного риска, тогда как остальные относятся к этому осторожнее), а также зрелость риска в контексте организации, поскольку последнее может носить более-менее устойчивый характер в случае риска.

II. Мандат

Мандат на управление рисками выражается через официальное заявление/документ, который четко определяет стратегию и задачи управления рисками, людей, ответственных за них на всех уровнях, и уполномочивает таких людей на использование соответствующих ресурсов для достижения поставленных перед ними задач.

Определение и сообщение о таком заявлении подтверждает приверженность организации внедрению системы управления рисками.

Box 1 - Пример мандата среди НСИ

“*Минимизация существенных рисков, возникающих во время работы и оказания услуг, путем применения эффективных принципов и практик управления рисками. Организация принимает допустимый уровень риска, но только после оценки вероятности, последствий и стоимости возникновения неблагоприятного события относительно имеющихся ресурсов для устранения или управления риском».*

Источник: Австралийское бюро статистики – инструкции для ответственного органа

III. Объем управления рисками

Определение объема стратегии управления рисками означает, что весь персонал знает об актуальности риска при достижении своих задач, а также для такого персонала предусматривается специальная подготовка. Кроме того, это означает, что в организации совместно применяется единый подход к управлению рисками, в том числе единый язык рисков.

IV. План рисков

Для внедрения системы управления рисками, необходим план рисков, который должен включать следующее:

· Задачи управления рисками (стратегические и оперативные);

· Деятельность по управлению рисками, предпринимаемая в соответствующие временные рамки, содействующая организации в достижении стратегических задач;

· Необходимые ресурсы, в том числе люди, знание и бюджет;

· Решения по информированию о рисках, внутренний и внешний уровень.

В плане описываются варианты мониторинга, анализа и отчетности о результатах стратегии управления рисками.

Что касается предпринимаемой деятельности, некоторые действия носят критически важный характер, будь то в результате расширенной программы или в результате «быстрой» программы на основе «опытного выпуска» системы управления рисками. Ресурсы, которые организация будет инвестировать во внедрение такой системы, также критичны. Они позволяют определить качество и достижение результатов.

1.3 Выработка политики управления рисками

1.2 Мандат и стратегия управления рисками	1. Организация системы управления рисками	1.4 Подход по управлению рисками	

ТЕГИ: Готовность к принятию риска, профиль риска, старшее руководство, обязательство, заинтересованные стороны.

Для обеспечения согласованности в действиях по управлению рисками в организации, политика управления рисками должна содержать высокоуровневый анализ и описывать процесс управления рисками.

Основные особенности политики:

· Определение готовности к принятию корпоративного риска: совет и старшие менеджеры устанавливают уровень склонности к риску путем определения общих границ с учетом нежеланной подверженности риску. Готовность к принятию корпоративного риска затем применяется для формирования допустимых уровней в организации по принципу сверху вниз (см. ниже);

· Внедрение стандартного процесса по управлению рисками на всех уровнях, тем самым гарантируя, что управление рисками – это неотъемлемая часть управления основным предприятием (см. Главу 4);

· Участие старшего руководства в разработке структуры управления проектами (см. ниже);

· Предоставление возможностей заинтересованным сторонам (см. ниже и см. также Раздел 2, Глава 1);

· Определение критериев риска (см. Раздел 2, Глава 3);

· Определение иерархии рисков (см. Раздел 2, Глава 3);

· Внедрение группы/отдела по управлению рисками (см. Главу 2);

· Определение политики подготовки человеческих ресурсов для поддержки процесса управления рисками (см. Главу 2);

· Создание системы коммуникаций (см. Раздел 2, Глава 1);

· Создание системы отчетности (см. Главу 4).

I. Готовность к принятию риска и профиль риска

Организация, собирающаяся внедрить соответствующую систему управления рисками, должна определить Структуру готовности к принятию риска (СГР), которая представляет собой структуру, увязывающую риски с миссией и стратегическими задачами, и, таким образом, стратегия переводится в качественно-количественные переменные. С учетом профиля риска («набор рисков, которые могут влиять на организацию полностью или частично») и последовательного выполнения общего стратегического плана, такая структура определяет предрасположенность к риску (склонность к риску), пороги чувствительности, пределы риска, управление риском, а также любые процессы, которые необходимо обозначить и устранить.

Организация не может учитывать риск, просто как риск, образующийся в результате воздействия от вероятности, чтобы его обработать: его управление зависит от составляющих переменных, участвующих в определении готовности к принятию риска, или от «суммы риска, которую организация готова принять, выдержать или которой готова подвергнуться в любой момент времени». Уровень готовности к принятию риска во многом зависит от рода выполняемой деятельности, предлагаемых товаров и услуг, а также от нормативного и окружающего контекста, в котором работает организация.

Переменные, выражающие соотношение профиля риска к готовности к принятию риска, следующие:

· Восприятие риска, которое описывает то, как люди воспринимают риски с учетом своих ценностей и интересов;

· Отношение к риску (существующий профиль риска): Если организация особенно эффективна в управлении определенными видами рисков, она может быть готова принять дополнительный риск в этой категории, или наоборот, может не захотеть этого;

· Принятие риска, относится к максимально возможному воздействию рискового события, которое организация сможет выдержать. Зачастую готовность будет намного ниже уровня принятия;

· Допустимая степень риска, представляет собой максимальный уровень, который организация сможет принять, не нарушая при этом бремя регулирования;

· Удержание риска – консервативные ожидания возврата заинтересованных сторон и очень низкая готовность к принятию риска;

· Склонность к риску – уровень вариации, который организация готова принять в отношении определенных задач.

Несмотря на то, что готовность к принятию риска связана со стратегическими задачами, склонность к риску, главным образом, относится к операционному риску, поскольку благодаря последнему руководящий орган устанавливает максимальное отклонение, допустимое готовностью к принятию риска.

Рисунок 1: От определения «профиль риска» к определению «готовность к принятию риска»

Структура готовности к принятию риска (СГР) – это методологическая схема, направленная на определение уровня готовности организации принять риск через развитие, представляющее собой итеративный процесс, помогающий организации обозначить сумму риска, которую она готова принять, что позволит достичь задач в соответствии с бизнес-стратегией.

При обозначении готовности к принятию риска, все стратегические действия (планирование, выявление финансовых и людских ресурсов, выбор проектов из портфеля и т.д.) определяются в соответствии с риск-ориентированным мышлением и критериями. Руководящий орган должен составить СГР на основе заявления (ЗГР – Заявление о готовности к принятию риска), состоящего из официального документа, в котором излагаются связанные с риском цели, а также способы контроля их достижения и последовательного включения в течение оперативных процессов организации.

В частности, в ЗГР должно заявляться следующее:

Ø Типы рисков, которые организация намеревается принять;

Ø Что касается каждого вида риска, то указывается возможный порог чувствительности и эксплуатационный предел, как при нормальных, так и при критических (на организационном/финансовом уровне) обстоятельствах;

Ø Любые начинаемые процедуры и/или действия, которые становятся необходимыми, чтобы привести риск к обратному уровню или же к установленной задаче или границам, особенно если уровень риска достигает порог чувствительности;

Ø Роль сторон, участвующих в определении и внедрении СГР (совет, руководители, аудиторы, структурные единицы);

Ø Сроки и процедуры контроля и обновления СГР;

Ø Правила обмена контентом СГР со всеми внутренними и внешними сторонами, участвующими в определении и внедрении.

Те организации, которые по существу принимают Структуру готовности к принятию риска, могут интегрировать ее с собственными процессами принятия решения, и прилагать все усилия по обеспечению внутренней коммуникации и распространению ее контента, начиная со старшего руководства.

При определении собственного уровня готовности к принятию риска, организация должна создать шаблон, который поможет определить пороги чувствительности по какой-либо деятельности. Например, шаблон будет показывать наличие по определенной деятельности в определенной области низкого, среднего или высокого уровня риска, и, соответственно, высокого, среднего или низкого допустимого уровня.

СГР должна содержать любые компоненты, учитываемые при определении склонности к риску, например, путем составления матрицы, позволяющей оценить уровень склонности к риску по каждой деятельности, проводимой соответствующими владельцами рисков.

Поэтому для главных стратегических рисков может обозначаться другой уровень готовности к принятию риска, а также определенные стили поведения, соответствующие заранее определенному уровню склонности к риску. Для этого может быть составлена матрица, дополняющая процессы принятия решения, которая позволит привести индивидуальный подход в соответствие с политиками риска, сформулированными старшим руководством: пагубное воздействие риска, минимизация рисков, осторожность, подверженность риску или принятие риска.

II.Обязательство по управлению рисками

Старшее руководство при поддержке среднего/младшего руководящего и технического персонала (например, через смешанные рабочие группы) должны содействовать работе по разработке структуры управления рисками. В частности, на фазе запуска проекта должен учитываться каждый организационный уровень, способствующий сбору входных данных и информации о потребностях (например, через *специальные* интервью). Сотрудники хорошо знают о наиболее типичных и повторяющихся рисках в своих областях работы, и необходимо способствовать и призывать их к регулярному представлению информации о таких рисках.

Цели по управлению рисками должны быть не только хорошо определены и доведены до сведения старшего руководство, но и обсуждаться с каждым из отделов НСБ. В каждом отделе должно предусматриваться контактное лицо, которое имеет право координировать всю деятельность по управлению рисками при взаимодействии со своими коллегами, в том числе с руководителем отдела.

III. Полномочия заинтересованных сторон

Крайне важно создать и поддерживать соответствующие структуры риска, которые обеспечивают сотрудничество с заинтересованными сторонами, направленное на достижение общих задач (например, доверие общественности к качеству официальной статистики, защита конфиденциальности по отношению к сведениям респондентов и т.д.). Организация должна регулярно распространять информацию, а также поддерживать диалог с внутренними и внешними заинтересованными сторонами по вопросу управления рисками, что позволит обеспечить понимание всеми участниками основ принятия решения и причин выполнения определенных действий.

С этой целью организация должна:

· Периодически пересматривать области взаимодействия;

· Проверять на предмет того, правильно ли понимается коммуникация и все ли коммуникационные каналы эффективны;

· Создавать надежные протоколы связи для обеспечения общего понимания соответствующих ответственностей;

· Внедрять консультативный групповой подход, содействующий правильному определению внутреннего и внешнего контекста, а также эффективному выявлению рисок, объединять разные области компетенции при анализе рисков, учитывать разные точки зрения при оценке рисков и эффективно управлять изменениями при обработке риска;

· Составить план коммуникации для внутренних и внешних заинтересованных сторон на начальном этапе процесса управления рисками;

· Способствовать, признавать и учитывать представленные по собственной инициативе точки зрения;

· Периодически давать комментарии о том, насколько хорошо и фактически выполнено обещанное или запланированное.

См.дополнительную информацию в Разделе 2, Глава 1.

.

Back to top

1.4 Подход по управлению рисками

	1.3 Выработка политики управления рисками	1. Организация системы управления рисками	1.5 Принятие комплексного риск-ориентированного подхода, связанного с управлением качеством статистических данных

Координация процесса управления рисками должна носить централизованный характер: отдел рисков анализирует и вырабатывает информацию по каждой фазе процесса, а затем приступает к стратегическому планированию по согласованию с советом организации.

Комитет по рискам и менеджер по рискам, выполняющий функцию координатора, вырабатывают критерии отбора наиболее актуальной информации, поступающей от информационной системы управления рисками (выборочный подход). О существенных рисках с точки зрения воздействия или стратегического уровня сообщает отдел, поддерживающий менеджера по рискам, на регулярной, специальной и исключительной основе. Менеджер по рискам дает распоряжения по переводу стратегий в задачи по управлению рисками, и контролирует их достижение подразделениями/отделами и менеджерами в рамках своих компетенций. Соответственно, менеджер по рискам дорабатывает полученную информацию, адаптируя ее к контексту организации (вплоть до уровня какого-либо одного отдела), что позволит устранить возможные отклонения от стратегических приоритетов.

Создание регистра рисков подразумевает подробное описание организационных рисков (корпоративные, проектные и операционные) и создание регистров специфических рисков по определенным темам (охрана здоровья и безопасность, мошенничество, IT-безопасность, среда и т.д.).

Существуют три вида подхода по вовлечению руководства и заинтересованных сторон в процесс выявления рисков:

- **Нисходящий подход**: процесс принятия решения сосредотачивается на уровне руководства. Этот подход может демонстрировать два режима: а) Полный нисходящий режим, при котором риски хозяйствующих единиц перечисляются на ведомственном уровне, то есть руководители отдела не могут добавлять риски сами на уровне отделов. Нет необходимости эскалации риска, кроме как на ведомственном уровне. б) Преобладающий нисходящий режим, при котором регистр корпоративных рисков создается непосредственно на основе детального регистра операционных рисков.
- **Восходящий подход**: процесс принятия решения осуществляется на уровне управления. Операционные риски выявляются каким-либо штатным сотрудником во время выполнения своей повседневной работы (например, чтобы мотивировать персонал проявлять большую активность в выявлении несоответствий, предусматривается возможность их регистрации он-лайн).
- **Смешанный подход:** совет заявляет о критериях (нисходящий подход), на основании которых руководители отдела выявляют и управляют рисками

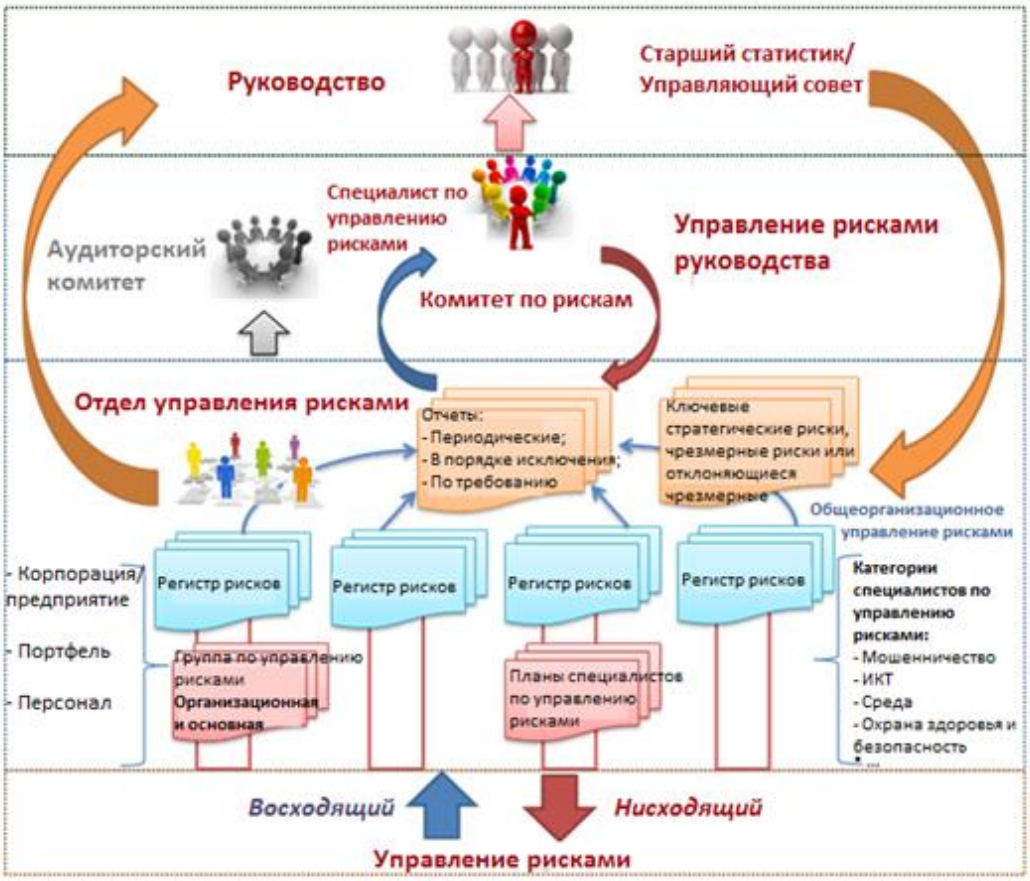
(восходящий принцип). Риски могут проверяться и оцениваться по всей организации на любом уровне (например, группа, программа, отдел, проект и т.д.). Чтобы создать структуру, иерархия рисков, которой будет уделяться внимание, должна соответствовать уровням предприятия, оперативным и проектным уровням.

Такие подходы не являются взаимоисключающими, и сочетание подходов по управлению процессами желательно направить на достижение эффективной интеграции управления рисками на любом уровне в организации.

Эти подходы по управлению рисками также представляют собой способ включения иерархии организации и преодоления организационных барьеров.

Рисунок ниже показывает процесс управления рисками в соответствии с нисходящей перспективой, и также выделяет потоки информации, связанные с процессами принятия решения в зависимости от различных ролей.

Рисунок 2: Управление рисками в соответствии со смешанным (нисходящим и восходящим) подходом



Источник: По материалам Австралийского бюро статистики, структура управления рисками

Чтобы выявить риски необходимо принять соответствующий инструмент или метод. Ниже представлены два из широко распространенных методов:

· Проведение анализа риска: Специальная команда (внутрифирменная или сторонняя) учитывает все операции и действия, связанные с организационными задачами, и выявляет сопутствующие риски. Такая команда должна проводить интервью с ведущим персоналом на всех организационных уровнях, что позволит создать профиль риска по целому ряду деятельности. (Тем не менее, важно, чтобы этот подход не сказывался негативно на осведомленности линейного руководства о своих ответственностях в управлении рисками, которые относятся к их задачам);

Самооценка риска: Каждому уровню и части организации предлагается оценить деятельность, а также провести диагностику рисков, с которыми они сталкиваются. Такая работа может проводиться на бумажной основе (такая диагностика проводится с помощью вопросников), но зачастую проведение семинара является наиболее эффективным подходом, при котором координаторы помогают группам отрабатывать риски, влияющие на их задачи. Особым преимуществом данного подхода является то, что при этом ответственность за риск устанавливается лучше, когда владельцы выявляют риски самостоятельно.

Вопросы и ответы

Вопрос. Ссылаясь на принятый подход, расскажите подробно о методологии, используемой при определении функций, ответственностей и связей с другими фазами процесса:

Ответ. Процесс начинается с того, что всем директорам предлагается заполнить вопросник по рискам, что позволит выявить главные три/пять рисков с точки зрения программы подразделения. Для этой цели были пересмотрены регистры риска на уровне программы, и утверждены соответствующими Отраслевыми советами по планированию, чтобы обеспечить согласованность между пониманием и относительной важностью рисков, выявленных на уровне подразделения или программы. Результаты данного упражнения предоставляются совету старшего руководства, который потом предложит собственный взгляд на корпоративные риски, с которыми сталкивается организация.

Источник: Статистическая служба Канады, Подробный обзор практики управления рисками

Вопросы и ответы

Вопрос. Отобранные заинтересованные стороны организации вовлечены в:

Ответ. Все заинтересованные стороны должны выявить риски: каждый штатный сотрудник может сообщить менеджерам процесса о препятствиях и рисках, выявленных в ходе процесса (Статистическое управление Литвы).

Ответ. Выявление и анализ риска необходимо распространять в организации и проводить департаментами, группами, территориальными статистическими управлениями, командами и проектами (Статистическое бюро Финляндии)

Источник: Обзор практики управления рисками

1.5 Принятие комплексного риск-ориентированного подхода, связанного с управлением качеством статистических данных

1.4 Подход по управлению рисками | 1. Организация системы управления рисками

ТЕГИ: Подход, статистический риск, структура качества.

Управление рисками имеет важное значение для достижения стратегического результата организации, и такая возможность может обеспечиваться только путем включения риска в качестве рутинного в весь процесс принятия решения. Это означает, что управление рисками должно являться частью культуры организации, внедренной в каждый организационный процесс, включая производственные и вспомогательные процессы.

Для этого требуется согласованный подход, объединенный с корпоративной стратегией, который подчеркивает нестабильность, вопросы и потенциальные проблемные области: комплексное управление риском должно вылиться в систему, являющуюся частью постоянного анализа эффективности организации. При этом организация не только обращает внимание на работу и события, но и систематически выявляет важные пробелы, вариации и нестабильность, что позволит опередить (смягчить) их возможное влияние.

С практической точки зрения:

а. Управление рисками не должно рассматриваться, как отдельная система, существующая независимо от того, как организация самостоятельно осуществляет управление, принимает решения, распределяет ресурсы и возлагает ответственность на людей.

б. Управление рисками не может проводиться на некоторых уровнях, если это означает исключение других.

Управление рисками не может проводиться только в нескольких частях организации.

Согласно целостному подходу, риски должны рассматриваться и оцениваться на любом уровне организации. Они должны являться основным фактором при утверждении предложений на инвестирование, и включаться в средства управления проектом и мониторинга эффективности. Следовательно, их необходимо включать в ключевые подотчетные документы и внутреннее стратегическое и проектное планирование.

Наиболее современные статистические организации разработали интегрированные модели, основанные на перспективе риска в масштабе предприятия, принимая стандартизированные термины и понятия для содействия эффективной реализации в организации.

В этих системах все аспекты внутреннего контроля разрабатываются через риск-ориентированный подход, построенный на следующих критериях:

а. Позиции политики отражают готовность старшего руководства к принятию риска, и разрабатываются, чтобы направлять поведение уполномоченного персонала в сторону управления рисками, с которыми они сталкиваются при выполнении своих заданий.

б. Механизмы руководства обеспечивают прозрачность и подотчетность в процессе принятия решения путем продвижения таких принципов, как уверенное лидерство, рациональное управление, эффективное планирование и анализ.

в. Планирование и отчетность предусматривают большие возможности для документального оформления целей и сопутствующих рисков.

г. Деятельность по предоставлению гарантий является частью внутренней проверки, в процессе которой выполняется проверка на предмет того, что управление рисками в организации проводится в соответствии с международными стандартами и установленной практикой[1], в то же время учитывается важность задач организации.

д. Организации должны выверять риски в соответствии с мерами внутреннего контроля, что позволит по мере возможности обеспечить наличие мер контроля по каждому риску, и при этом каждая такая мера содействует устранению таких рисков.

Такие НСБ приняли комплексную структуру управления рисками путем определения (дополнительно к общему управлению рисками) специального управления рисками, при котором рассматриваются устойчивые риски (например, мошенничество, охрана здоровья и безопасность, безопасность информационно-коммуникационных технологий (ИКТ) и риск раскрытия информации)[2]. Они также делают значительный упор на управление статистическим риском, которое определяется как возможность несоответствия одного или нескольких компонентов производственного процесса установленному стандарту качества, что приводит к более низкому качеству или целостности статистических выходных данных. Учитывая, что статистические риски неизбежно управляются на всех уровнях (стратегический, оперативный и проектный) в НСБ, стоит отметить, что даже если они и управляются по отдельности, то их, в конечном счете, необходимо интегрировать в организационную структуру риска.

Учитывая сильную связь между качеством и риском[3], риски могут обрабатываться путем проведения управления качеством, особенно на оперативном уровне.

В действительности, управление риском и управление качеством похожи в следующем:

- Управление качеством обычно определяет требования, и определяет то, выполняются ли они, и в каких случаях выполняются (через анализ, проверку и т.д.). Если требования не выполняются, проводятся корректирующие действия;
- Управление рисками позволяет выявить угрозы (источники рисков), которые могут повлиять на задачи. Если уровень риска слишком высок, проводятся меры по смягчению.

Несмотря на наличие множества общих структур качества в литературе, применение подходов по непрерывному улучшению качества среди НСБ по-прежнему ограничено.

При внедрении структуры улучшения качества статистического бизнес-процесса, НСБ должны уделять особое внимание следующим аспектам:

- Извлечение ключевых элементов и возможных отношений общей структуры качества статистических процессов из этих существующих моделей;
- Принятие общего словаря по управлению качеством и риском.

Первый шаг внедрения структуры качества, независимо от принятого стандарта, заключается в разработке карты технологического процесса, что позволит определить точки, на которых можно измерить качество продукта и процесса.

Картирование процесса может помочь понять принцип работы системы, а также определяет то, как система взаимодействует с другими системами и процессами.

Другой ключевой шаг заключается в выявлении требований пользователей к качеству статистических данных по отношению к рассматриваемому процессу[4]. Требования к качеству должны охватывать как критерии качества, так и требования, связанные с риском. Процесс находится под контролем, если критерии качества соблюдены, а риски являются приемлемыми.

НСБ могут использовать Типовую модель производства статистической информации (ТМПСИ) в качестве руководства по картированию деятельности статистических процессов. Это гарантирует включение всех шагов статистического процесса в целях мониторинга. Например, фаза «Сбора» ТМПСИ включает любую деятельность, относящуюся к получению данных. Учитывая недавнее принятие Типовой модели работы статистических организаций (ТМРСО), которая расширяет и дополняет ТМПСИ путем добавления других видов деятельности, которые необходимы для поддержки статистического производства, было бы желательно ввести этот стандарт, который бы дополнял внедрение всей системы управления рисками

В частности, согласно модели ТМРСО:

- Система руководства при управлении рисками и корпоративное управление рисками (т.е. общие риски, которые могут влиять на стратегические задачи НСБ) может находиться в рамках деятельности «Стратегия и лидерство» под заголовком «Руководить и управлять»;
- Управление статистическими рисками, связанное с фазами выявления и мониторинга, может находиться в рамках деятельности по управлению потенциалом под названием «Планировать/контролировать потенциал». Такие виды рисков, которые могут повлиять на качество данных, зачастую связаны с правильным применением статистических методологий и производственных стандартов;
- Что касается выявления и обработки организационных рисков, управление операционными рисками, связанными с вспомогательной деятельностью (например, финансы, человеческие ресурсы, ИКТ), может предусматриваться в каждой подобласти «Корпоративной поддержки». В этой области деятельности существуют специальные типы рисков (т.е. риски потерь от мошенничества);
- Управление операционными статистическими рисками на бизнес-уровне – это деятельность, находящаяся под ответственностью владельца риска, с учетом фазы выявления и обработки, что позволит обеспечить статистическое качество и успешное осуществление

[1] Внутренний аудит должен проводиться независимой организационной единицей, осуществляющей консультативную функцию и предусматривающей независимую гарантию и содействие Главному статистику (см. Раздел 2, Глава 5)

[2] Одно учреждение, которое управляет всеми этими устойчивыми рисками – это Австралийское бюро статистики (АБС), которое также разработало структуру повышения качества статистической цепочки на основе управления рисками (см. Приложение).

[3] A) Качество определяется как степень соответствия характеристик объекта требованиям (ISO 9001:2015). Риск определяется как влияние неопределенности на цели (ISO 31000). Цели могут рассматриваться как требования высокого уровня. B) Традиционно, качество концентрируется на качестве продукта и удовлетворенности заказчиков (ISO 9001). Однако определение качества может применяться к таким другим объектам, как процессы, входные данные, а также учреждение в целом.

[4] Проекты BLUE-ETS: SP1-Проект взаимодействия и сотрудничества /Исследовательский проект, направленный на малые или средние предприятия/FP7-SSH-2009-A/Номер соглашения о гранте 244767/ Пакет документов 7.3

2. Ресурсы для управления рисками

⇦	1. Организация системы управления рисками	⇧РАЗДЕЛ 1: Структура управления рисками	3. Процесс управления рисками (см. Раздел 2) ⇨

ТЕГИ: Выделение человеческих ресурсов, внутренние заинтересованные стороны, организационные изменения, климат организации, культура организации, обучение управлению рисками, навыки и компетенции.

2.1 Культура организации по отношению к риску

⇧2. Ресурсы для управления рисками	2.2 Обучение ⇨

Инициативы по управлению рисками могут вырабатывать у сотрудников чувство принадлежности к группе, а также чувство их собственного значения в организации. (Люди могут объединиться, чтобы создать систему управления рисками, управления активами, что позволит определить организационные меры и т.д.). Кроме того, управление рисками предусматривает систематический стандартный механизм внутреннего контроля, который обязывает весь персонал из разных областей объединяться, чтобы обсудить и выявить вопросы, а также решить проблемы. Эта деятельность также содействует повышению качества культуры работы, и позволяет персоналу чувствовать свое значение и участие в процессе достижения более широкой задачи организации.

Человеческие ресурсы считаются одним из ключевых элементов успешности организации[1] и некоторых неопределенностей, вызывающих риск, которые могут появляться фактически в результате внутренней среды организации.[2] Например, то, как старшее руководство реагирует на результаты мониторинга, может влиять на поведение сотрудников. Организация должна обладать достаточно четким представлением о неопределенности, возникающей в случаях, когда полагаются лишь на одного человека, чтобы выполнить значительную модификацию риска, и должна надлежащим образом вознаграждать усилия. При составлении структуры и внедрении процесса управления рисками, требуются определенные действия по интеграции таких человеческих и культурных факторов.

Изменение и, в частности, культурные изменения, являются слабой стороной управления рисками: процесс – это, скорее, не проблема, а ее восприятие людьми. Два важных урока, полученные в результате внедрения системы управления риском: внедрение четкого риск-ориентированного мышления на наивысшем уровне организации, при этом обеспечивается последовательное включение вплоть до руководства младшего звена и сотрудников, и представление риск-ориентированного мышления не как что-то совершенно новое (чтобы уменьшить сопротивление), а как важная особенность процесса изменений.

Профили работы (обозначение роли, ожидаемых результатов работы и задач развития) должны определяться для персонала, ответственного за вопросы, связанные с управлением рисками, а конкретное описание определенных вопросов должно включаться в профили работы менеджера по управлению общими рисками и специалистов по рискам.
Организация должна создать **профилактические меры контроля человеческих ресурсов** для сокращения вероятности и/или влияния неблагоприятных и критических событий, например, невыполнение и нарушение дисциплины[3]. Следовательно, организация должна усилить и/или пересмотреть матрицу приоритетных рисков и, по мере необходимости, план оптимизации рисков, который должен отражать реализованные инициативы по человеческим ресурсам в соответствии с текущим анализом остаточного риска и эффективностью относительно запланированного анализа остаточного риска

[1] См. Портер М.Е., 1990 г.

[2] В ISO/TR 31004:2013(E) говорится об общих типах ошибок, связанных с человеческими и культурными особенностями: а) неспособность обнаружить и отреагировать на раннее предупреждение; б) безразличие к мнению других или к недостатку знаний; в) систематическая ошибка из-за упрощенных стратегий обработки информации для изучения сложных вопросов; г) неспособность признать сложность.

[3] Для этого в качестве примера потенциальных дополнительных практик, организация также может: определять, какие обязанности необходимо отделить, чтобы предупредить критические события; разработать системы вознаграждений и других поощрений для лиц или единиц, которые показывают сниженные остаточные результаты или степень несоблюдения, а также принудительные действия или другие позитивные задачи для организации.

Вопрсы и ответы

Вопрос. Определены ли профили работы для персонала, ответственного за вопросы управления рисками?

Ответ 1. «Конкретное описание вопросов, связанных с управлением рисками, представлено в должностных инструкциях специалистов по рискам и руководителей отделов»

Источник: Румыния, *Подробный обзор практики управления рисками*

Ответ 2. «Да, определены. Существует должностная инструкция для менеджера по управлению общими рисками. Менеджер по управлению общими рисками Бюро статистики Австрии имеет сертификат старшего менеджера по управлению рисками в области ÖNORM EN ISO 31000 и ONR 49003 (Австрийская экономическая палата, WIFI- орган сертификации)»

Австрия, *Подробный обзор практики управления рисками*

Ответ 3. «Весь персонал имеет Соглашение о развитии и деятельности (СРД), в котором определена их роль, ожидаемые результаты деятельности и задачи развития. Роли, связанные с риском, будут составлены в ходе расширенного планирования и в отдельных СРД, но могут не отражаться в названии. Кроме того, роли, связанные с управлением специфичными рисками, определены в документации по управлению рисками»

Австралия, Подробный обзор практики управления рисками

2.2 Обучение

2.1 Культура организации по отношению к риску | 2. Ресурсы для управления рисками

Для эффективного внедрения системы управления рисками, организация должна выделить **соответствующие ресурсы, подходящий человеческий капитал,** а также обеспечить, что подотчетный персонал может выполнять свои функции, предусматривая для него необходимое **обучение и навыки**. Весь персонал должен знать об актуальности риска, что позволит достичь поставленных задач, и необходимо предусматривать обучение, содействующее персоналу в управлении рисками. Информированность и постоянная поддержка позволяет знать об ожидаемых результатах, и сокращает вероятность ошибок.

Для работы с угрозами и возможностями организация должна определить наличие и эффективность текущих действий и мер контроля. Это включает применение образовательных и ознакомительных программ. Организация также должна провести структурированную оценку потребностей, выявить риски и потребности в обучении (например, общая система контроля, специфическая подготовка в области систем управления рисками, стандарты внутреннего контроля, специальные инструменты, модули статистического качества и т.д.), а также предусмотреть соответствующую подготовку и поддержку для ответственного персонала. И, наконец, организации

определяют практику информирования, образования и поддержки, которую они должны внедрить **в рамках каждой политике и целевой аудитории**.

Рекомендуется начать обучение с программы, предназначенной для менеджеров и сотрудников, ответственных за вопросы управления рисками на разных уровнях. Было бы лучше, если бы стартовая учебная деятельность сначала фокусировалась на областях повышенного риска. Также важно регулярно проводить учебные инициативы в соответствии с разработкой системы управления рисками, а также одновременно со значимыми изменениями в организации.

Обучение УР необходимо включить в существующую систему профессионального обучения, если управление рисками рассматривается как средство для совершенствования и в целях экономической эффективности. В целях образования и информированности рекомендуется применять технологии соответствующего уровня и выработать инструменты электронного образования для охвата более широкой целевой аудитории. Организации также должны распланировать *специальные* сессии, на которых рассматриваются темы и вопросы, конкретное касающиеся управления качеством и рисками, а также связанные с широкими процессами изменений в организации, при которых требуется тщательное и эффективное управление переходной фазой. Они должны предусматривать инициативы по специфической подготовке и/или *специальные* мероприятия, описывающие то, как управление рисками представляет собой стратегический рычаг изменений.

Вопросы и ответы

Вопрос. Пожалуйста, укажите частоту инициатив по специфическому обучению, проводимых с начала внедрения системы управления рисками, независимо от вида:

Ответ. «Ежегодное обучение управлению рисками и системе внутреннего контроля (СВК) в рамках семинаров (УР, СВК) с участием приглашенного эксперта. Система управления рисками представляется всем новым штатным сотрудникам в рамках системы общей подготовки Бюро статистики Австрии».

Источник: Австрия, *Подробный обзор практики управления рисками*

2.3 Функции и ответственности

	2.2 Обучение	Sec 2: 1. Communication and consultation	

ТЕГИ: Функции, ответственности, обязанности

Управление рисками должно осуществляться на любом организационном уровне, а также при участии всего персонала в соответствии с их функциями и ответственностями.

Управляющий совет несет ответственность за создание эффективной системы управления рисками во всей организации;

Комитет по управлению рисками/совет – это наблюдающий субъект, контролирующий систему управления рисками и другие статистические вопросы. Комитет/совет устанавливает готовность к принятию риска совместно со старшим руководством, и сообщает всей организации. Комитет/совет несет ответственность за контроль соблюдения политики по организационному риску, мониторинг соответствия мер контроля, мониторинг изменений в профиле риска организации, что рассматривается как часть организационной стратегии и процессы планирования, содействует старшему руководству в отборе ключевых рисков, периодически проводит анализ системы отчетности по управлению рисками, а также достаточности ресурсов по управлению

рисками, несет ответственность за эскалацию и передачу вопросов по существенным рискам старшему статистику на рассмотрение.

Менеджер по рискам работает под руководством комитета/совета, обладает квалификацией (или даже сертификацией) в области управления рисками, имеет поддержку со стороны персонала, соответствующего размеру организации (см. ниже группа управления рисками). Менеджер по рискам несет ответственность за сотрудничество со старшим руководством в выявлении областей высокого риска, связанного со стратегическими или бизнес-процессами; сотрудничество со старшим руководством в определении действий по обработке и контролю процесса управления рисками. Его функция также заключается в следующем: содействие согласованному управлению рисками и владению риском на всех уровнях в пределах организации, формирование культуры оповещения о рисках в пределах организации, включая надлежащее образование и обучение, разработка, внедрение и анализ структуры управления рисками, согласование других консультативных функций по определенным аспектам управления рисками, согласование мер реагирования в случаях, когда риску подвержены несколько областей, управление качеством в рамках управления рисками, представление отчетности, эскалация и сообщение о вопросах, связанных с управлением рисками, ключевым заинтересованным сторонам.

Старшее руководство несет ответственность за наличие соответствующей целевому назначению и современной структуры управления рисками, принятие процессов и наличие соответствующих ресурсов и финансов для управления рисками, при этом предусматривается стратегическая направленность на соответствующий учет рисков при принятии решений, устанавливается степень готовности к принятию риска и соответствующий орган, утверждается политика рисков, распространяется культура управления рисками, обеспечивается надлежащая оценка и управление ключевыми рисками, с которыми сталкивается организация, предусматривается направление и получается отзыв об эффективности управления рисками и соответствии политики управления рисками.

Руководитель департамента/подразделений/групп должен активно заниматься управлением рисками, что является частью ежедневной работы, при этом соблюдая структуру управления организационными рисками. В частности, такие отделы устанавливают задачи по управлению рисками и формулируют ключевые показатели рисков, разъясняют своему персоналу стратегию управления рисками и готовность к принятию риска, осуществляют процессы управления рисками, управляют рисками, которые подпадают в их сферу ответственности, сотрудничают в выявлении ключевых рисков, контролируют программы действий по управлению рисками, регулярно отчитываются перед старшим руководством о каких-либо новостях или изменениях в существующих рисках, или неудачных существующих мерах контроля.

Весь персонал должен учитывать риски при принятии решений, и нести ответственность за эффективное управление рисками, включая за их выявление. Весь персонал ответственен за понимание и осуществление политик и процессов управления рисками.

Внутренняя проверка (см.подробную информацию в Разделе 2, Глава 5) обуславливает отчетность перед советом по соответствию процессов управления рисками в организации, гарантируя их структуру и принцип работы, эффективность мер контроля и ответных действий на ключевые риски, надежность и соответствие оценки риска. Осуществление мандата по внутренней проверке выполняется независимым отделом, который отчитывается непосредственно перед старшим статистиком.

Группа управления рисками координируется менеджером по рискам и ответственна за сбор формы выявления риска, которая заполняется теми структурами (директоратами, подразделениями, группами), которые находятся под ответственностью соответствующего владельца риска. Также ответственна за анализ этих форм и предложение действий по предварительной обработке, эскалацию риска, если он превышает уровень полномочий группы, подтверждение конечного решения, постановку задач, показателей риска, целей и сроков по предлагаемым действиям, подготовку документации по эскалационным рискам и представление ее на соответствующем уровне управления (в частности, для комплексных действий), мониторинг исполнения действий по контролю для оценки результатов, предложение корректирующий действий. Кроме

того, группа ответственна за заполнение регистра рисков, заполнение документов по рискам, подготовку документации по рискам и представление ее менеджеру по рискам, подготовку собраний по вопросам управления рисками.

Описание задач, сроков и ответственностей по всем участникам процессов управления рисками должно включаться в процедуру, доводимую до сведения каждого в организации.

.

3. Процесс управления рисками (см. Раздел 2)

2. Ресурсы для управления рисками	РАЗДЕЛ 1: Структура управления рисками	4. Мониторинг и отчетность	

Процесс управления рисками – это компонент структуры, разрабатывается на основе введенной в действие политики управления рисками.

Процесс управления рисками – это систематическое применение политик, процедур и практик управления по отношению к задачам коммуникации, создания контекста, оценки, мониторинга и анализа рисков.

Включает следующую деятельность:

1) Коммуникация и консультация;

2) Контекстуальный анализ;

3) Оценка рисков:

а. Выявление;

б. Анализ и измерение;

в. Взвешивание;

4) Обработка рисков;

5) Мониторинг и анализ.

Процесс также должен учитывать риск-ориентированную проверку и поддержку информационной системы на всех фазах

Раздел 2 в настоящем документе содержит анализ каждой фазы процесса.

4. Мониторинг и отчетность

3. Процесс управления рисками (см. Раздел 2)	РАЗДЕЛ 1: Структура управления рисками	

4. Мониторинг и отчетность

4.1 Мониторинг и анализ структуры

4. Мониторинг и отчетность	4.2 Создание механизмов отчетности	

ТЕГИ: Отклонения в системе, план управления рисками, изменение контекста, отзывы.

Для того чтобы гарантировать, что система управления рисками является эффективной и продолжает поддерживать деятельность организации, организация должна:

1. *Периодически измерять прогресс и отклонение от политики и плана управления рисками*: структура и процесс должны соответствовать целевому назначению, задачам/приоритетам организации, а соответствующие заинтересованные стороны должны получать соответствующие отчеты, позволяющие им выполнять свои обязанности и нести свою ответственность в структуре руководства;

2. *Периодически проверять адекватность структуры, политики и плана управления рисками, учитывая внешний и внутренний контекст организации:* организация должна гарантировать, что изменения контекста или изменения других факторов, влияющих на соответствие или стоимость управления рисками, выявляются и рассматриваются;

3. *Периодически пересматривать процесс управления рисками:* ресурсов по управлению рисками должно быть достаточно, а персонал, работающий в организации, должен обладать достаточными навыками, знаниями и компетенциями управления рисками в соответствии со своими функциями по управлению рисками, необходимыми для выполнения ежедневной работы;

4. *Периодически пересматривать уровень зрелости управления рисками*: В целях обеспечения непрерывного совершенствования, организация должна самостоятельно оценивать уровень своего развития в области управления рисками, выделять сильные и слабые стороны, и создавать и/или пересматривать длительный путь развития самой системы управления рисками;

5. Периодически докладывать о результатах мониторинга совету: исходя из результатов мониторинга и анализа, необходимо принимать решения для совершенствования процесса управления рисками организации и ее культуры, обеспечивая при этом способность организации получить опыт на основе рисковых событий.

4.2 Создание механизмов отчетности

⇦	4.1 Мониторинг и анализ структуры	⇧4. Мониторинг и отчетность

ТЕГИ: Система отчетности, исполнительная и оперативная отчетность, отчет заинтересованных сторон, подотчетность.

Организация должна гарантировать, что информация о рисках, полученная в процессе управления рисками, надлежащим образом сообщается и используется в качестве основы для принятия решений на всех соответствующих уровнях. Для этого должны быть созданы четкие механизмы отчетности и надежный межведомственный процесс обмена знаниями в целях подотчетности по рискам и гарантии предоставления точных, согласованных и своевременных отчетов. Кроме того, в политике управления рисками (см. Главу 1) должен четко заявляться способ представления отчетов по показателям управления рисками.

Несоответствующая требованиям отчетность по рискам[1] может привести к неспособности полностью интегрировать выявленные риски в стратегические и оперативные решения. Организация должна сообщать о прогрессе, достигнутом по плану управления рисками, доказывая, насколько хорошо соблюдается политика управления рисками, что позволяет гарантировать, что управление рисками является эффективным процессом и продолжает поддерживать показатели организации. В частности:

1. Результаты мониторинга и анализа риска должны регистрироваться и сообщаться на внутреннем и внешнем уровнях, если это целесообразно;

2. Разработки по реализации планов обработки рисков должны включаться в деятельность по управлению общими показателями работы организации, измерение, а также внутреннюю и внешнюю отчетность в качестве показателя эффективности;

3. Расширенное управление рисками включает в себя постоянные коммуникации с внешними и внутренними заинтересованными сторонами (см. Раздел 2, Глава 1), включая всестороннюю и частую отчетность по показателям управления рисками как часть эффективного управления.

Качество и успех отчетности по рискам зависит от следующих факторов:

- Целевая аудитория;

- Входные ресурсы и процессы;

- Частота;

- Содержание;

- Формат;

- Каналы распространения.

Определение **целевой аудитории** важно, так как оно влияет на другие решения, связанные с отчетностью по рискам. Всякий раз, когда раскрытие необходимо согласно нормативным требованиям, организация должна соблюдать и предусматривать соответствующее раскрытие. С другой стороны, добровольное раскрытие должно регулироваться анализом затрат и выгод потребностей аудитории и видом раскрытия (тип и подробная информация по рискам). Отчетность по организационным рискам должна осуществляться на нескольких уровнях, что позволит удовлетворить потребности разной аудитории, имеющей своим специфические потребности, требования, ожидания, повестки и уровни компетентности. При этом существуют два направления отчетности по рискам:

a) Отчетность перед **внутренней аудиторией**.

b) Отчетность перед **внешней аудиторией.**

Отчетность по рискам является неотъемлемым условием для лиц, принимающих решения на внутреннем уровне, что позволяет интегрировать оценку риска в свою операционную и инвестиционную стратегию, проанализировать эффективность и проверить решения по компенсации/вознаграждению. Внешняя отчетность по рискам за последние годы прошла быстрое развитие: отчеты по корпоративному управлению также фокусируются на внутреннем контроле, и анализ риска, как правило, включается в ежегодные отчеты. Внутренняя и внешняя аудитории могут в дальнейшем делиться на две подгруппы: с одной стороны некоторая аудитория (например, совет директоров и регулирующие органы из числа внешней аудитории) должна быть проинформирована об организационных рисках и процессах управления рисками через положения или рекомендации. Рекомендуется добровольное раскрытие другой внутренней аудитории (например, сотрудники) и внешним заинтересованным сторонам (например, СМИ, гражданские ассоциации), исходя из ожидаемых выгод благодаря улучшенному процессу принятия решения.

«**Входные ресурсы»** и «**процессы»** также играют критически важную роль. Наиболее важные **входные ресурсы** представлены:

I. Различными рисками, с которыми организация сталкивается;

II. Требованиями к отчетности по рискам заинтересованных сторон и ожиданиями;

III. Существующим руководством по управлению рисками организации, которое предусматривает контекст для создания процессов отчетности по рискам;

Организационными ресурсами (например, физические лица с необходимыми навыками и опытом, финансовые ресурсы и доступ к необходимой информации).

Необходимо принять решение о том, по каким рискам будет представлена отчетность, степень детализации и **частота отчетности**.

а) Внутренняя отчетность

Организация должна создать механизмы внутренней отчетности, что позволит поддерживать и содействовать подотчетности и владению риском. Эти механизмы должны гарантировать соответствующее распространение информации о ключевых компонентах структуры управления рисками, их эффективности и результатах, а также данные о последующих модификациях. Необходимая информация, полученная в процессе управления рисками, доступна на соответствующих уровнях и в соответствующее время, при этом существуют процессы, позволяющие консультироваться с внутренними заинтересованными сторонами (см. Раздел 2, Глава 1). Эти механизмы должны в соответствующих случаях включать процессы по объединению информации о рисках из разных источников, при этом необходимо учитывать чувствительность информации. Внутренние отчеты по рискам могут составляться в режиме реального времени или носить периодический характер.

Основная цель **периодических внутренних отчетов по рискам** заключается в представлении обобщенной информации о различных соответствующих организационных рисках с показателями тенденции и периодическими сравнениями, выделяющими изменениями в рисках. Периодическая внутренняя отчетность по рискам содействует стратегическому контролю и процессу принятия решения, а также улучшенным оперативным бизнес-решениям. Информация о риске может систематизироваться вокруг определенных категорий ключевого риска, а не вокруг фаз процесса управления рисками. Отчетность по остаточным рискам включает сравнение валового риска (оценка риска до принятия мер контроля или реагирования на риски) и чистого риска (оценка риска с учетом принятия каких-либо мер контроля или реагирования на риски), что позволяет проверять эффективность реагирования на риски и альтернативные варианты управления. Отчетность по рискам перед советом и комитетами должна выполняться хотя бы раз в квартал.

Внутренняя аудитория будет не только заинтересована в раскрытии информации о специфических рисках, но и в процессе управления рисками. Общепринятый и должным образом управляемый процесс заверит внутреннюю аудиторию о надежности отчетов по рискам: поэтому организации должны включать информацию о качестве их процесса управления рисками, в частности, в свои периодические отчеты по рискам.

Комплексная и частая внутренняя отчетность по существенным рискам, показатели управления рисками и процесс значительно содействуют эффективному руководству. В связи с этим, разные уровни организации, нуждающиеся в разной информации в результате процесса управления рисками, требуют разные виды отчетов:

- ***Исполнительная отчетность***. Совет директоров обладает максимальной контрольной ответственностью за разработку и реализацию миссии организации, ценностей и стратегии, и должен тщательно анализировать корпоративные процессы по выявлению рисков, мониторингу и управлению. Совет также устанавливает философию риска, готовность к принятию риска и склонность к риску. Специальный анализ финансовых целей, планов и других существенных сделок, как правило, также подпадает в рамки ответственности совета. Эти ответственности требуют широкой и прозрачной отчетности по различным организационным рискам (стратегические, операционные, отчетные и правовые риски). Соответствующая коммуникация **с советом** подразумевает следующую отчетность:

  - Прогресс относительно целей и сопутствующих рисков организации;

  - Эффективность непрерывного мониторинга по вопросам риска и контроля, включая отчетность по существенным ошибкам или слабым сторонам.

  Риски могут быстро принимать определенную форму, и совет должен гарантировать наличие четких процессов, которые позволяют быстро привлекать внимание к

существенным вопросам, когда это необходимо, и согласовывать вызывающие факторы для достижения этого. Совет также должен определить характер, источник, формат и частоту информации, которая ему необходима, и отслеживать получаемую информацию, гарантируя, что качество информации достаточное для принятия эффективного решения.

- ***Оперативная отчетность*.** Система управления рисками включает процедуры немедленной отчетности перед **соответствующими уровнями руководства** по выявляемым существенным **ошибкам** контроля или слабым сторонам, а также подробным сведениям о предпринимаемых корректирующих действиях. Физические лица должны систематически и оперативно отчитываться перед руководством младшего и среднего звена о любых воспринимаемых новых рисках или невозможности осуществить меры контроля. Руководство среднего звена должно систематически и оперативно отчитываться перед старшим руководством о любых воспринимаемых новых рисках или невозможности осуществить меры контроля. Без надлежащей внутренней отчетности по организационным рискам, менеджеры не смогут принять оптимальные тактические решения. Старшее руководство нуждается в соответствующих и надежных отчетах по рискам, составляемых в режиме реального времени и на периодической основе, для обеспечения эффективного контроля: пример представлен матрицей рисков. Это таблица, в строках которой отображаются риски, а в столбцах – вероятность возникновения и их воздействие.
- ***Экспертный/проверочный отчет***. Не каждый риск обладает мерой внутреннего контроля, но каждой мерой внутреннего контроля должен рассматриваться риск. Внутренние проверочные отчеты являются ключевым источником информации об эффективности организации и контрольной среде, которые позволяют согласовать меры внутреннего контроля и риски. Результат анализа или проверки будет представлен в виде отчета, в котором суммируются все полученные данные и приводятся выводы по оценке относительно предварительно определенных критериев. В этом отчете могут предлагаться рекомендации по совершенствованию системы на основе наблюдений экспертов. Также будет представлен ежегодный отчет по общему состоянию мер внутреннего контроля организации (см. Раздел 2, Глава 5).

back to top

Вопросы и ответы

Вопрос. В вашей организации отчетность по управлению рисками включает:

Ответ. «Цели управления, результаты семинара, посвященного вопросам риска, выявление и измерение рисков с высоким приоритетом, мониторинг действий по обработке рисков. Мониторинг выполнения стратегических целей также входит в отчетность по управлению рисками. Отчеты по управлению рисками представляются руководству, владельцам риска, участвующему персоналу и Экономическому Совету».

Источник: Австрия, Подробный обзор практики управления рисками

б) Внешняя отчетность

Организации все больше испытывают давление, обусловленное повышенной прозрачностью, будь то вынужденного или добровольного характера,

и **повышенным согласованием информации, сообщаемой на внешнем уровне, с той, которая сообщается на внутреннем уровне**. Заинтересованные стороны надеются на интенсивное распространение информации о риске на корпоративном уровне, а также на информированность о критической роли надлежащего управления рисками. Ввиду этого, организация должна представлять точные, своевременные и качественные отчеты, что позволит удовлетворить потребности внешних заинтересованных сторон. В частности, она должна периодически пересматривать эффективность системы управления рисками и сообщать заинтересованным сторонам об этом, а также проводить надежную оценку принципиальных рисков, описывая и объясняя способы их управления или смягчения.

Организации могут подготавливать разные, специальные отчеты по рискам для разных внешних заинтересованных сторон. В то время как внутренние отчеты по рискам направлены исключительно на внутреннюю аудиторию, внешняя отчетность по рискам, включая корпоративные ежегодные отчеты, может включать как внешних пользователей, так и внутренних заинтересованных групп.

Вопросы и ответы

Вопрос. Если предусматривается отчет по управлению специальными рисками с внешними заинтересованными сторонами, опишите содержание:

Ответ. «Общее описание системы управления рисками (с точки зрения инициатив с SSE и ЕЭК ООН); Задачи, связанные с процессами управления рисками; Основные выявленные риски, действия по обработке; Результаты мониторинга, выходные данные; Эскалационные риски, предложенный план действий; Совершенствование системы управления рисками, следующие шаги».

Источник: Румыния, Подробный обзор практики управления рисками

Вопрос. Пожалуйста, укажите частоту составления отчета по управлению рисками, который адресован внешним заинтересованным сторонам:

Ответ 1. «По запросу».

Источник: Канада, Подробный обзор практики управления рисками

Ответ 2. «Ежегодно».

Источник: Румыния, Австралия, Подробный обзор практики управления рисками

Ответ 3. «Ежеквартально, ежегодно».

Источник: Литва, Подробный обзор практики управления рисками..

[1] Руководство по ISO 73:2009 определяет отчетность по риску как вид коммуникации, призванный информировать определенных внутренних или внешних заинтересованных сторон путем предоставления информации о текущем состоянии риска и его управлении.

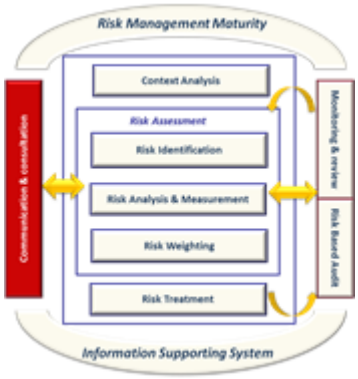
РАЗДЕЛ 2: Процесс управления рисками

РАЗДЕЛ 1: Структура управления рисками	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов

1. Коммуникация и консультирование

РАЗДЕЛ 2: Процесс управления рисками	2. Анализ деловой среды

ТЕГИ: участие заинтересованных сторон; внутренняя коммуникация; внешняя коммуникация; информационный поток; инструменты коммуникации.



Организация должна обеспечить информированность каждого сотрудника в соответствии с должностью о стратегии управления рисками организации, приоритете рисков и подобных учетах. В обязанности Совета, помимо прочих, входит предоставление достоверной внутренней информации и процессов коммуникации, а также ответственность за внешнее распространение информации об управлении рисками и внутреннем контроле. «Коммуникация и консультирование» - это не отдельный этап управления рисками, он идет параллельно всему процессу. Коммуникация и консультирование важны в виду того, что заинтересованные стороны также делают собственные выводы касательно рисков на основании своих представлений, которые необходимо определить, зафиксировать[1] и интегрировать в процесс принятия решений.

Консультирование с заинтересованными сторонами требует тщательного планирования, поскольку может как построить, так и разрушить доверительные отношения. Для усиления доверия к результатам процесса и получения одобрения плана обработки заинтересованные стороны должны участвовать во всех аспектах управления рисками, включая разработку процесса коммуникации и консультирования (См. разделы: Пункт 1.1, Пункт 1.2).

План распространения и отчетности по управлению рисками должен включать:

- Привлечение внутренних и необходимых заинтересованных сторон для обеспечения правильного, точного и эффективного обмена информацией с учетом аспектов конфиденциальности и неприкосновенности личности;

- Внешнюю отчетность для соблюдения законных, нормативных требований и требований органов управления (См. РАЗДЕЛ 1, Гл.4);

- Обеспечение обратной связи по механизмам коммуникации, консультирования и отчетности.

Вопросы и ответы

Вопрос. Какие наиболее важные уроки получены при внедрении системы управления рисками в вашей организации, которые другие организации должны принять во внимание при разработке собственных процессов управления рисками?

Ответ. «При разработке собственных процессов управления рисками Национальные статистические бюро должны учитывать то, что важно уметь слушать и пользоваться обратной связью»

Источник: Соединенное Королевство, *Опрос по практикам управления рисками*

Вопрос. Каковы сильные стороны системы управления рисками в вашей организации?

Ответ. «Все сотрудники и необходимые заинтересованные стороны консультируются в процессе управления рисками»

Источник: Южная Африка, *Обзор практики управления рисками*

[1] Записи по коммуникации и консультированию будут зависеть от таких факторов, как масштаб и восприимчивость деятельности.

1.1 Внутренняя коммуникация

1. Коммуникация и консультирование | 1.2 Внешняя коммуникация

Двусторонняя коммуникация с внутренней аудиторией (например, советом директоров, организационным комитетом аудиторского/внутреннего контроля при его наличии, менеджерами всех уровней, сотрудниками, партнерами цепи комплексных поставок/другими партнерами в соответствии с открытым видением организации) должна рассматриваться как путь к улучшению процесса управления рисками. Содействие внедрению политики управления рисками и общего участия в различных фазах процесса имеет большую важность для эффективности всей системы. Открытая коммуникация помогает в процессе принятия решений использовать информацию об управлении рисками. Более того, она помогает идентифицировать *корпоративные риски[1]* и приводит к выполнению общеорганизационных действий при сотрудничестве разных отделов.Организация должна наладить потоки внутренней коммуникации в целях поддержания отчетности и владения риском вместе с широкомасштабным участием. Эти механизмы гарантируют, что ключевые компоненты структуры управления рисками, а также любые последующие изменения должным образом сообщаются и передаются для консультирования. Механизмы внутренней коммуникации и консультирования включают методы и инструменты, за счет которых организация обеспечивает понимание каждым внутри организации в соответствии с его/ее должностью следующих вопросов:

- Из чего состоит стратегия управления рисками;
- Каковы приоритеты риска;
- Как распределяется ответственность, как соответствующие обязанности вписываются в рамки риска (кто что делает).

Выявление новых рисков (или изменений в уже оцененных рисках) зависит от поддержания хорошей сети коммуникаций через соответствующие контакты и обеспечение информацией. Если этого не достигнуто, на приоритеты риска отреагировать последовательно нельзя. Комплексный консультационный подход поэтому может быть полезен в определении контекста для обеспечения эффективного выявления рисков, в объединении различных областей знаний для анализа рисков, в **обеспечении должного внимания различным взглядам**, в должном управлении изменениями при обработке рисков.

Цели управления рисками должны обсуждаться в каждом подразделении организации или проекта[1] и четко сообщаться (например, через заявление о готовности к принятию риска). Всему персоналу – руководящему и не руководящему (а также необходимым внутренним заинтересованным сторонам) – в процессе управления рисками должны

предоставляться консультации. Выявление рисков и работа с ними должны исходить из совместной работы, включающей ключевые элементы каждого проекта или процесса, а также обратную связь от руководства касательно интегрированного процесса[2] управления рисками. Более того, в конкретных областях статистики важную роль могут сыграть межинституциональные комиссии и рабочие группы.

В итоге внутренняя коммуникация:

· Помогает внедрить желаемое поведение в организации;

· Привлекает персонал к деятельности по управлению рисками;

· Повышает прозрачность процесса управления рисками, поощряет ответственность и владение рисками;

· Улучшает сотрудничество между отделами/подразделениями в вопросе определения сквозных инициатив, общее понимание идей, правил для осуществления действии и интеграции управления рисками в статистические процессы, как основы установления очередности регулирующих действий, направленных на непрерывное совершенствование.

Следовательно, **план управления рисками**, как план внутренней коммуникации, должен включать:

- Создание группы, ответственной за сообщение по управлению рисками;
- Повышение осведомленности об управлении рисками и процессе управления рисками во всей организации.

Документы, касающиеся планов/политики, методические документы, информация, связанная с системой управления рисками, должны распространяться и быть доступны всем сотрудникам. Специальные **каналы** коммуникации могут включать: внутренние события (например, тренинги, семинары)[1], рассылку электронных сообщений, голосовых сообщений, базы данных, поддерживающие конкретные вопросы касательно рисков, письма от имени совета, группы обсуждения электронных сообщений, внутренние сайты по управлению рисками предприятия, информационные веб-сессии, селекторные совещания, постеры или плакаты, подкрепляющие ключевые аспекты управления рисками предприятия, очные обсуждения, информационные рассылки от старшего специалиста по рискам, итоговые совещания, системы обмена знаниями (например, вики).

Вопросы и ответы

Вопрос. Цели управления рисками четко сообщаются в вашей организации.

Ответ. «Полностью согласен. Процедуры и иные документы по процессу управления рисками распространяются по органу, ответственному за мониторинг, координирование и методическое руководство разработки системы внутреннего/административного управления НИС. Он должен состоять из высшего руководства всех областей статистики“.

Источник: Румыния, *Подробный обзор практики управления рисками*

[1] Риски/критичность, распределенные по категориям в соответствии с их стратегической важностью и контролируемые и обрабатываемые как приоритет.

[2] Для примера можно разработать матрицу риска в качестве задачи для групповой работы – под руководством ответственных за крупные статистические и/или

организационные проекты – и результаты должны сообщаться каждому из участников проекта, чтобы им были известны их обязанности.

[3] Обычно на ежегодной основе.

[4] Особенно в фазе запуска, собрания со всеми участвующими подразделениями организации должны проводиться с целью более подробного обсуждения различных актуальных вопросов, а также предоставления каждому сотруднику возможности выразить мнение и принять участие в процессе принятия решения. Презентации старших руководителей должны демонстрировать поддержку и ожидания от сотрудников в отношении риска, положительно обосновывая культуру рисков.

1.2 Внешняя коммуникация

⇦	1.1 Внутренняя коммуникация	⇧1. Коммуникация и консультирование

Организация должна периодически информировать и консультировать внешние заинтересованные стороны:

а. О том, как обрабатываются риски;

б. С целью проведения работы с ожиданиями заинтересованных сторон касательно того, что фактически может выполнить организация;

в. С целью убеждения их в том, что организация удовлетворит их ожидания.

Эффективная внешняя коммуникация и консультирование обеспечивают понимание заинтересованных сторон основы принятия решений.

«Структура рисков» разрабатывается в ходе всестороннего процесса, включая анализ информации о рисках и отражение рекомендаций от различных источников. Важно, чтобы организации учитывали все важные отношения с партнерами, подрядчиками и третьими сторонами и способствовали достижению соответствующей коммуникации и пониманию относительных приоритетов рисков. Коммуникация с внешними заинтересованными сторонами по вопросам рисков необходима: непонимание относительных приоритетов рисков может вызвать серьезные проблемы.

Правильный и тщательно составленный план отношений с заинтересованными сторонами по вопросам рисков должен учитывать и устанавливать наиболее существенные компоненты: стратегию и каналы распространения. Что касается первого элемента, для своевременного внешнего сообщения касательно рисков особенно удобен корпоративный сайт. Что касается периодического внешнего сообщения касательно рисков, части ежегодных или квартальных отчетов (на электронных и/или бумажных носителях) рассматриваются, в целом, как основные каналы. Ниже перечислены возможные инструменты коммуникации для обмена информацией с внешними заинтересованными сторонами и поддержания диалога:

1. Корпоративный сайт;

2. Публикации и газеты;

3. Ежегодные собрания;

4. Другие внешние события (например, конференции, научные встречи, семинары и проч.);

5. Корпоративные газеты;

6. Сообщения, являющиеся частью постоянной корпоративной коммуникации.

Вне зависимости от того, какой метод практикуется, целью коммуникации должно быть обеспечение внешней аудитории прочной основы для проведения всесторонней оценки сообщенных данных (см. Раздел 1, Гл.8).

Прежде всего, модель информирования о рисках должна объединять информацию, касающуюся рисков, которую организация сообщает вовне. Задачей является информирование среднего члена внешней аудитории, сохраняя справедливость и равновесие при распространении всех существенно важных перспектив.

Вопросы и ответы

Вопрос. Если риски ассоциируются с внутренними и/или внешними заинтересованными сторонами, укажите, какого вида консультации используются.

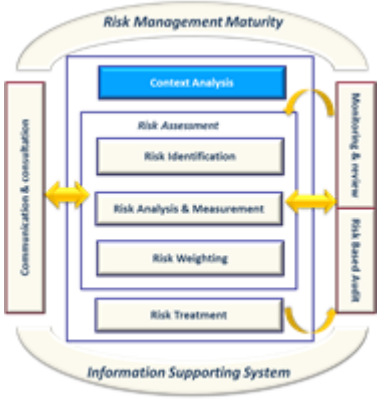
Ответ. «Пользователи статистики, респонденты и другие национальные производители официальной статистики должны иметь возможность вносить предложения, комментировать, подавать жалобы. Устанавливается единственная точка контакта»

Источник: Литва, *Обзор практики управления рисками*

2. Анализ деловой среды

⇦	1. Коммуникация и консультирование	⇧РАЗДЕЛ 2: Процесс управления рисками	3. Оценка риска ⇨

ТЕГИ: Среда; анализ; процесс; картирование.



2.1 Создание среды

⇧2. Анализ деловой среды	2.2 Картирование процесса ⇨

При разработке системы управления рисками следует учитывать различный уровень зрелости НСБ. Состояние проектов, программ и уровень зрелости портфолио НСБ следует оценивать до начала процесса управления рисками. В частности, важно установить, классифицировать (общий, специальный) и оценить риски, связанные с внедрением стратегии организации (так называемый «риск управления рисками»)[1].

Для обеспечения должной точности и качества следует тщательно изучить среду, в которой происходит процесс управления рисками.

Создание внешней среды гарантирует, что при разработке критериев управления рисками учитываются заинтересованные стороны и их цели, а возможности и угрозы извне должным образом принимаются в расчет.

Оценка внешней среды организации может включать, но не ограничиваясь:

- Юридическую, нормативно-правовую среду (международную, национальную, региональную или местную);
- Финансовую, технологическую и экономическую среду;
- Анализ конкурентной среды;
- Ключевые движущие силы и тенденции, влияющие на цели организации;
- Отношения, а также восприятие и ценность внешних заинтересованных сторон[2].

Поскольку управление рисками происходит в контексте целей и задач организации, необходимо понимать внутреннюю среду.

Организационный анализ и картирование процесса – это те два инструмента, которые способны поддерживать эту работу. Организационный анализ учитывает:

- Руководство, организационную структуру;
- Политики, цели, стратегии, которых следует достичь;
- Источники и знания (например, капитал, время, люди, процессы, системы и технологии);
- Информационные системы;
- Отношения, а также восприятие и ценность внутренних заинтересованных сторон и культуры организации;
- Стандарты, инструкции и модели, принятые организацией.

Через картирование все процессы разделяются, анализируются и представляются при параллельном определении исходных данных, информационных потоков, ролей и ответственности, а также результатов для каждого из них.

[1] Более подробно об управлении зрелостью риска смотрите в Главе 8, о практиках управления зрелостью риска – в Приложении.

[2] Лица или организации, которые могут повлиять, попасть под влияние или посчитать, что попали под влияние какого-либо решения или действия.

2.2 Картирование процесса

	2.1 Создание среды	2. Анализ деловой среды

Совершенствование системы управления рисками требует глубокого и документально подтвержденного анализа процесса, относящегося ко всей организации: он все больше должен включать мероприятия, отличая основную деятельность от комплексной, вплоть до детальной операционной деятельности. Картирование процесса позволит организации проводить «идентификацию риска» (см. Главу 3), описывая задачи, персонал, деятельность, ответственности, организационные единицы, результаты, сроки, последовательность и связи/взаимодействие подпроцессов и соответствующих документально подтвержденных процедур.

Следовательно, «анализ рисков» (см. Главу 3) является эффективным, если он включает идентификацию всех ключевых процессов, охватывающих потенциальную подверженность некоторым последствиям. Должен включать анализ процесса, обращая особое внимание ключевым общеорганизационным зависимостям и точкам

существенного контроля, например: где образуются данные, где они хранятся, как они превращаются в полезную информацию и кто пользуется такой информацией.

Картирование процесса включает ряд **шагов**:

- Идентификация всех рутинных мероприятий в рамках конкретного проанализированного процесса;
- Группирование мероприятий на ключевые подпроцессы;
- Определение последовательности событий и связей между подпроцессами.

Для гарантии того, что карты процесса точно отражают то, что происходит на самом деле, организации могут сочетать разные **методы** (см. приложение), поэтому организация должна выбрать **вид «Моделирования и картирования процесса»,** который подходит для ее определенных целей. Карта может представлять собой простую макроблок-схему, показывающую лишь ту информацию, которой достаточно для понимания потока общего процесса, или информация может быть достаточно детальной, отражая каждую деятельность и точку принятия решения.

Ниже описываются виды картирования.

- Карта процесса на макро-уровне. Представляет собой очень глубокий уровень, а также довольно редкое картирование, в котором представляются действующие маршруты организации.
- Карта процесса по принципу «сверху вниз» или высокого уровня. Показывает непрерывные процессы по вышеуказанным производственным областям. Быстро и легко составить, но может не предусматривать необходимых деталей для формирования понимания или выполнения улучшений. Хорошо показывает основные кластеры деятельности процесса.
- Универсальная карта процесса. Показывает функции, входные ресурсы, выходные данные и шаги, необходимые для выполнения определенного процесса в производственной области. Универсальное картирование процесса предусматривает достаточную информацию для проведения работ по совершенствованию, и использует блок-схемы для демонстрации отношения между бизнес-процессом и функциональными единицами (например, департаменты), ответственными за такой процесс. На этих схемах указывается, где люди или группы попадают в последовательность процесса, и как они относятся друг к другу на всем протяжении процесса. Универсальные схемы являются превосходным инструментом, показывающим протекание процесса через организационные границы.
- Детальная блок-схема процесса. Подробно описывает системы, инструкции и процедуры, необходимые для выполнения шагов процесса на третьем уровне (Универсальная карта процесса), и показывает входные ресурсы, выходные данные, связанные шаги и точки принятия решения. Из-за уровня детализации, создание такого картирования может являться ресурсоемким, но может предлагать максимальный потенциал совершенствования, поскольку показывает решения и последующую деятельность, предусматривая превосходные учебные и справочные материалы. Блок-схемы могут быть представлены в виде карт или в графическом виде.

Владелец процесса должен нести ответственность за картирование процесса, тогда как анализ процесса должен проводиться лицами, исполняющими другие функции (внутри организации или без участия организации), чтобы собственные рабочие методы не влияли друг на друга.

И, наконец, ссылки на карты, информация о порядке работы и сами карты необходимо хранить в последовательной структуре, которая называется «**библиотекой процессов»**. Ответственность за библиотеку процессов должна быть четкой, равно как и любой процесс, который нуждается во владельце.

Вопросы и ответы

Вопрос 1. Являются ли установленные риски в вашей организации результатом предыдущего картирования процесса?

Ответ. «Использовалась замещающая переменная, т.е. перечень действий, появляющихся в информационной системе планирования и управления».

Источник: Италия, *Исследование практик управления рисками*

Вопрос 2. Картирование процесса в вашей организации включает:

Ответ 1. «Что касается всех бизнес-направлений (чистая статистика или поддержка), интеграции специальных IT-(под)процессов, то был определен перечень типичной деятельности (начиная с начала 2000-х гг.), связывающей задачи, процессы, организационные единицы, ответственность, сроки и результаты. Теоретически, по каждому процессу и основной деятельности необходимо описать и документально подтвердить операционную (для вертикальных процессов) и системную (для пересекающихся процессов) процедуру в соответствии со стандартным шаблоном».

Источник: Румыния, *Подробный обзор практики управления рисками*

Ответ 2. «Модель бизнес-процесса Австралийского бюро статистики была внедрена в 2000 году, и охватывает 32 статистических основных процесса и примерно 35 комплексных процессов. По всем этим процессам предусматриваются и регулярно используются подробные описания операционной деятельности».

Источник: Австрия, *Подробный обзор практики управления рисками*

Вопрос 3. Программа подготовки к управлению рисками включает:

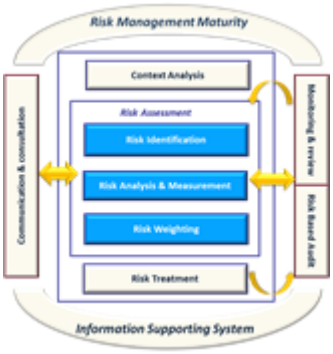
Ответ. «Ряд учебных модулей по статистическому качеству был только что разработан, и поддерживает картирование процесса, а также применение различных мер статистического контроля в бизнес-сферах»

Источник: Австралия, *Подробный обзор практики управления рисками*

3. Оценка риска

2. Анализ деловой среды	РАЗДЕЛ 2: Процесс управления рисками	4. Обработка риска	

ТЕГИ: идентификация риска, анализ риска, взвешивание риска, методы, функции и ответственности



Анализ организационного контекста влияет на методологию, используемую для оценки рисков, поскольку это влияет на выбор оценочных критериев. Первая деятельность в рамках процесса оценки рисков заключается в разработке общего набора оценочных критериев, которые будут развернуты по хозяйствующим единицам, корпоративных функций и крупных капитальных проектов. Риски и возможности, как правило, оцениваются по их воздействию и вероятности.

Некоторые риски являются динамичными, и требуют непрерывной оценки, другие более статичные, но их периодические повторные оценки учитываются при непрерывном мониторинге, который предупреждает об изменении обстоятельств.

Оценка риска включает три этапа:

1. Идентификация;

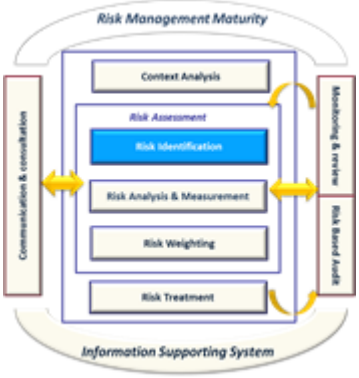
2. Анализ и измерение;

3. Взвешивание (ранжирование риска)

3.1 Идентификация риска

3. Оценка риска	3.2 Анализ и измерение риска	

ТЕГИ: Определение риска, критерии риска, идентификация риска, разные подходы, иерархия рисков, методы, участие заинтересованных сторон, функции и ответственности.



Риск, как правило, представляет собой неопределенность, по сути связанную с последствиями действий и событий, будь то положительные (например, возможность) или отрицательные (например, угроза). Риск измеряется путем комбинацией вероятности и воздействия, включая воспринимаемую актуальность. «Неотъемлемый риск» – это подверженность, вытекающая из специфического риска до выполнения какого-либо действия для управления им, тогда как «остаточный риск» – это подверженность, вытекающая из специфического риска после выполнения какого-либо действия для управления им, а также в случае если такое действие доказало свою эффективность.

Организация определяет критерии, используемые для оценки значимости риска. Такие критерии должны отражать восприятие риска заинтересованными сторонами (на основе

набора значений/опасений), а также ценности организации, задачи и ресурсы. Некоторые критерии могут задаваться или возникать на основе законодательных и нормативных требований. Критерии риска должны соответствовать политике организации по управлению рисками, определенной в структуре управления рисками.

Определение критериев риска включает выбор следующих элементов:

1. Характер и вид последствий, которые будут включены, а также то, как они будут измеряться;

2. Способ выражения вероятностей;

3. Как будет определяться уровень риска;

4. Критерии, определяющие то, когда необходимо выполнить обработку риска;

5. Критерии, определяющие то, когда риск является приемлемым и/или допустимым;

6. Будут ли комбинации рисков учитываться и как.

Идентификация риска требует анализ следующих вопросов:

- П*ервичное/коренное событие*: любая деятельность, которая может потенциально повысить специфический риск, вне зависимости от того, контролируется ли такая деятельность организацией или нет;
- *Области воздействия*: работа с классификацией/ранжированием последствий;
- *Ключевые факторы*: организационные свойства, которые помогают произойти рисковому событию;
- *События*: определенное стечение обстоятельств; и
- *Их возможные последствия*: потенциальный результат события. Необходимо учитывать широкий спектр последствий риска, включая каскадный и суммарный эффект.

Вышеуказанные вопросы могут создавать, решать, предупреждать, ухудшать, ускорять или сдерживать способность всей организации или ее части в достижении собственных задач.

I. Иерархия рисков и классификация рисков

Структура управления рисками включает иерархию рисков, включающую различные уровни рисков и приоритеты в стратегиях обработки рисков.

- **Общеорганизационные или так называемые «корпоративные» риски** являются стратегическими (т.е. могут существенно влиять на организацию). Их управление имеет существенное значение для обеспечения долгосрочной жизнеспособности организации, и должно выполняться под руководством комитета по рискам;

- **Риски управления портфелем** неотъемлемо относятся к портфелю проектов в целом, и управляются старшим руководством. Некоторые примеры портфельных рисков: доступность портфеля, отсутствие возможности/потенциала осуществить портфель, отсутствие своевременной доступности навыков и человеческих ресурсов;

- **Проектные риски** могут влиять на задачи и результаты проектов, и управляются менеджером по проектным рискам. В соответствующих случаях они будут рассматриваться в рамках структуры управления проектом. Некоторые примеры проектных рисков: недостаточно хорошо определен объем проекта, отсутствие ресурсов в случае необходимости, недостаточно хорошо определены требования качества.

***- Операционные риски** могут влиять на задачи и/или результаты программы (т.е. неподходящая профессиональная структура, сокращение ресурсов в результате сокращения бюджета, неполученные вовремя результаты, результаты плохого качества), и управляются руководителями программ.*

Несмотря на то, что каждый зарегистрированный риск может быть важен для управления на уровне функциональной и хозяйствующей единицы, перечень корпоративных рисков

требует ранжирование, чтобы привлечь внимание совета и старшего руководства к ключевым рискам.

Управление рисками на корпоративном, общеорганизационном и оперативном уровнях необходимо интегрировать, так чтобы уровни активности дополняли друг друга. Таким образом, стратегия организации по управлению рисками должна руководиться сверху, и включаться в нормальные рабочие процедуры и мероприятия.

Требуются специалисты по специфическим рискам, непосредственно относящиеся к соответствующему высшему руководству. Области специфического риска включают:

- Риски для здоровья и безопасности;

- Риски потерь от мошенничества (т.е., манипулирование какими-либо процедурами в мошеннических целях, несоблюдение процедур и/или правил внутреннего распорядка, изменение проверок исполнения работ или поставки товаров и т.д.);

- Риски, связанные с ИКТ (т.е., риски, связанные с системами безопасности, непрерывность бизнеса и т.д.)

Поэтому организации следует установить и документально зарегистрировать категории рисков, а также категории последствий рисков в соответствии с размером, целью, характером, сложностью и контекстом. Категории рисков, в том числе со стороны заинтересованных сторон, необходимо передавать по организации, что предусмотрит обмен взаимопониманием.

Группирование похожих видов рисков в категории рисков помогает:

1. Выполнить корректную оценку;

2. Профилировать и сообщать о последствиях фактических и потенциальных событий;

3. Содействовать сравнению в рамках всей организации;

4. Объединять и картировать одинаковые виды риска в рамках всей организации;

5. Распределять ответственности по управлению рисками;

6. Формировать внутренние навыки, знания и опыт в рамках всей организации.

Таблица ниже показывает категории и классы рисков для НСБ в соответствии с распределением, предложенным стандартом общеорганизационного управления рисками Co.S.O.

Стратегический	Статистическое производство, распространение статистических данных, системы и процессы управления, организация
Операционный	Отдел кадров, финансы, ИКТ, закупки
Соблюдение	Соблюдение закона, стандартов
Отчетность	Коммуникационные потоки

II. Средства идентификации рисков

Идентификация рисков может потребовать многосторонний подход, поскольку риски могут охватывать широкий ряд причин и последствий.

Методы идентификации риска:

а) Доказательные методы, например, листок самоконтроля и анализ архивных данных;

б) Системные командные подходы (команда, состоящая из экспертов, систематически идентифицирует риски посредством структурированного набора подсказок или вопросов (т.е. структурированные или полуструктурированные интервью, мозговой штурм[1], метод Дельфи[2]));

в) Способы индуктивного рассуждения (т.е. предварительный анализ опасности, анализ эксплуатационных опасностей, анализ рисков и критических контрольных точек);

г) Анализ сценариев (т.е. анализ основной причины, анализ сценариев как таковых, анализ причин и последствий);

д) Статистические методы (т.е. анализ по методу Монте-Карло, байесовский анализ).

При осуществлении этих методов, необходимо всегда учитывать зрелость системы управления рисками. Во время экспериментальной фазы по моделированию управления рисками, квалифицированный анализ всегда необходимо сочетать со структурированным или полуструктурированным интервью, или с заполнением листка самоконтроля, чтобы помочь владельцам риска в анализе рисков.

Квалифицированный анализ должен основываться на фактической информации путем проверки данных, полученных от различных систем (например, электронные системы управления документацией, система регистрации несоответствий и ИТ-инцидентов, система регистрации использования времени, а также специальная система регистрации признаков качества статистических обследований). После создания культуры управления рисками в рамках всей организации, мозговой штурм и метод Дельфи могут заменить интервью, анализ причин и последствий, листок самоконтроля или другой упрощенный вид анализа сценариев.

Факторы, влияющие на выбор метода:

1. Сложность проблемы и методы, необходимые для их анализа;

2. Характер и степень неуверенности оценки рисков, основывается на сумме доступной информации и требований по удовлетворению задач;

3. Объем ресурсов, необходимый с точки зрения времени и опыта, информационных потребностей или расходов;

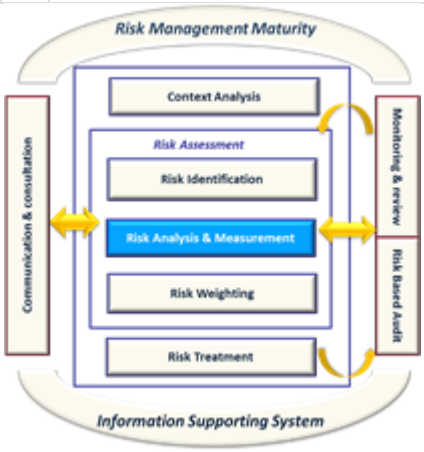
4. Может ли метод предусмотреть количественный результат.

[1] Мозговой штурм – это способ сбора широкого спектра идей и их оценка, а также упорядочение, выполняемое командой. Может предлагать подсказки или методы проведения личных и групповых интервью

[2] Способ объединить мнения экспертов, позволяющий дополнить процесс выявления источника и влияния, оценки вероятности и последствий, и также оценки рисков. Представляет собой кооперативный метод формирования консенсуса среди экспертов (ISO ISO31010 – Метод оценки рисков).

3.2 Анализ и измерение риска

3.1 Идентификация риска | 3. Оценка риска | 3.3 Взвешивание рисков



Анализ риска подразумевает учет причин и источников рисков, их положительные и отрицательные последствия, а также вероятность возникновения таких последствий.

Как правило, включает оценку ряда возможных последствий, которые могут возникнуть в результате события, ситуации или обстоятельства, и их соответствующую возможность, что позволяет измерить уровень риска. Однако в отдельных случаях (например, если последствия могут быть незначительными, или предполагается, что возможность будет крайне низкой) оценки одного параметра может быть достаточно для принятия решения.

В любом случае необходимо разработать некоторую структуру для оценки рисков. При оценке необходимо обратить внимание на беспристрастные независимые доказательства, следует рассмотреть вопрос о перспективах целого ряда заинтересованных сторон, пострадавших от риска, и предупредить путаницу, связанную со справедливой оценкой риска и суждением о приемлемости определенных рисков.

При оценке риска существуют три важных принципа:

1. Обеспечение наличия четко структурированного процесса, с помощью которого учитывается, как вероятность, так и воздействие;

2. Регистрация оценки риска способом, содействующим мониторингу и идентификации приоритетов риска;

3. Проведения различия между «неотъемлемым» и «остаточным» риском[1]. Уровень риска будет зависеть от достаточности и эффективности существующих мер контроля.

Методы, используемые при анализе рисков:

- Качественный метод: такие методы определяют последствие, возможность и уровень риска по описательным шкалам, могут сочетать последствие и возможность, и оценивать результирующий риск в соответствии с качественными критериями.
- Полуколичественный метод: в таких методах используются числовые оценочные шкалы последствия и возможности, и они могут сочетаться для формирования уровня риска, используя формулу. Шкалы могут быть линейными или логарифмическими, или иметь некоторое другое отношение. Используемая формула также может меняться.
- Количественный метод: такой вид анализа оценивает практические значения последствий и их возможностей, а также производит цифровые показатели воздействия, вероятности и уровня риска, используя данные из разных источников. Полный количественный анализ может не всегда быть возможен или желателен из-за скудной информации об анализируемом объекте, отсутствии данных, влияния человеческих факторов и т.д.

Качественный и количественный методы имеют свои преимущества и недостатки.

Качественный анализ относительно быстрый и легкий, предусматривает много информации о нефинансовых последствиях, и легко понимается большим количеством сотрудников.

С другой стороны, не проводит большой разницы между уровнями риска, не может численно агрегировать или изучить взаимодействие или соотношение риска, и предоставляет ограниченные возможности для выполнения анализа затрат и выгод.

Количественный анализ позволяет преодолеть множество недостатков количественного метода, несмотря на то, что он может занять много времени и средств, прежде всего, на этапе разработки метода.

Анализ причинно-следственных связей – это полукачественный, структурированный метод, позволяющий отследить первопричины потенциального события. Систематизирует возможные способствующие факторы в широкие категории, таким образом, могут учитываться все соответствующие гипотезы. Однако сам по себе анализ не указывает на фактические причины, поскольку они могут определяться только вещественными доказательствами и эмпирической проверкой гипотез. Анализ причинно-следственных связей предусматривает структурированную наглядную картину (схему) перечня причин специфического воздействия (положительное или отрицательное, в

зависимости от контекста). Применяется для формирования консенсуса по всем возможным сценариям, а также наиболее вероятным причинам, выявленным командой экспертов. Такие причины затем могут проверяться на эмпирическом уровне или путем оценки доступных данных.

При необходимости может составляться схема причинно-следственных связей:

- Выявить возможную коренную причину специфического воздействия, проблемы или условия;
- Выбрать и привести в соответствие некоторые взаимодействия между факторов, влияющих на определенный процесс;
- Провести анализ существующих проблем, таким образом, могут быть предприняты меры по совершенствованию.

Входные данные для анализа причинно-следственных связей могут образовываться в результате навыков и опыта участников или на основе ранее разработанной модели, которая использовалась в прошлом.

Анализ причинно-следственных связей должен проводиться командой экспертов, которые знают о проблеме, требующей разрешения.

Основные шаги выполнения анализа причинно-следственных связей:

1. Создание анализируемого эффекта и помещение в блоки;

2. Определение основных категорий причин (выбранных в соответствии с конкретным подтекстом) и представление их по блокам в диаграмме причинно-следственных связей;

3. Информирование о возможных причинах по каждой главной категории с секторами и подсекторами для описания взаимоотношения между ними;

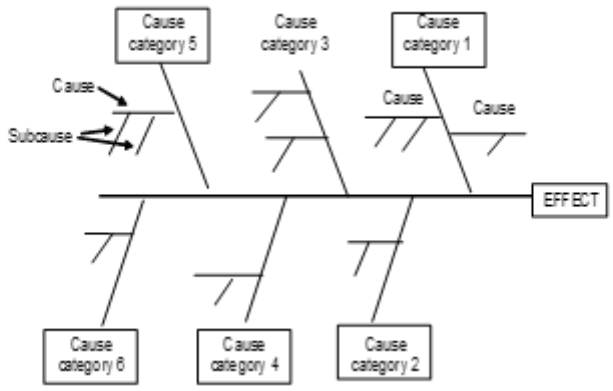
4. Продолжать спрашивать «почему?» или «какова причина?», чтобы увязать причины;

5. Обзор всех секторов для проверки согласованности и полноты, а также для обеспечения того, что причины распространяются на основное воздействие;

6. Выявление наиболее вероятных причин, исходя из мнения команды и имеющихся доказательств.

Результаты, как правило, отображаются на диаграмме причинно-следственных связей (или графике причинной зависимости) или на древовидной схеме. Диаграмма причинно-следственных связей структурируется путем подразделения причин на основные категории (представляется размеченными линиями диаграммы причинно-следственных связей), при этом секторы и подсекторы описывают более специфичные причины под вышеупомянутыми категориями.

Рисунок 3: Пример графика причинной зависимости или диаграммы причинно-следственных связей



Источник: IEC/FDIS 31010:2009, Методы управления рисками – оценки рисков

Как говорилось выше, уровень риска – это действие факторов, в частности, таких, как вероятность и воздействие.

Воздействие относится к степени влияния рискового события на организацию. Критерии оценки воздействия могут включать финансовые, репутационные, нормативные последствия, последствия для здоровья, сохранности, безопасности, окружающей среды, сотрудников, заказчиков и операционные последствия. Организации, как правило, определяют воздействие, используя сочетание таких последствий, учитывая, что определенные риски могут воздействовать на предприятие с финансовой точки зрения, тогда как другие риски могут больше сказываться на репутации или здоровье и безопасности.

Вероятность отражает слабую/сильную возможность фактического наступления определенного события. Вероятность может выражаться с качественной, процентной или частотной точки зрения. Иногда организации описывают вероятность с наиболее персональных и качественных перспектив, например «событие, которое, по предположению, возникнет несколько раз (или не возникнет) за профессиональную деятельность».

В Приложении представлены примеры показателей риска по воздействию и вероятности.

При использовании качественных или полукачественных методов (например, показатели риска), направленных на оценку уровня риска, вне зависимости от события (статистические, организационные или специфические), применение одного и того же числа параметров воздействия, а также вероятности является крайне важным условием. Чтобы сбалансировать субъективность оценки, требуется несколько специалистов, проводящих оценку по отдельному риску, при этом оценка должна максимально дополняться объективными данными.

Что касается функций и ответственностей, оценка факторов риска находится в рамках ответственности владельцев процесса. Измерение риска – это задача для рабочих групп, которая поддерживается отделом по управлению рисками и при участии персонала, работающего над рассматриваемыми процессами. Такой персонал представляет свои результаты старшему руководству на утверждение/проверку. Эксперты (например, в области IT, защиты данных/статистической конфиденциальности и т.д.) ответственны за измерение специфических рисков. Результаты оценки также всегда анализируются и подтверждаются менеджером по рискам.

Влпросы и ответы

Вопрос. С привязкой к фазе измерения риска, использует ли ваша организация разные методы по классификации рисков (IT, финансовые, риск, связанный с нарушением, и т.д.)?Ответ. Оценка риска (в статистических областях) учитывает ряд вопросов, связанных с циклом обработки статистических данных, который может влиять на качество данных, а также с управлением взаимоотношениями с заинтересованными сторонами.

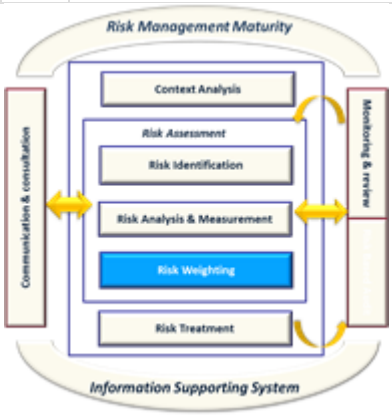
Источник: Австралийское бюро статистики, *Подробный обзор практики управления рисками*

Неотъемлемый риск: риск для субъекта при отсутствии какой-либо деятельности, которую руководство может осуществить для изменения вероятности или воздействия риска.

Остаточный риск: часть общего риска, оставшегося после обработки. Остаточный риск включает в себя допустимый риск и неустановленный риск.

3.3 Взвешивание рисков

	3.2 Анализ и измерение риска	3. Оценка риска



Взвешивание рисков подразумевает сравнение расчетных уровней риска с оценочными критериями, что позволяет определить наиболее существенные риски или исключить минимальные риски из дальнейшего анализа. Цель заключается в фокусировке используемых ресурсов на наиболее важных рисках. Необходимо проявлять осторожность, чтобы не упустить низкие риски, которые встречаются часто, и поэтому могут иметь большее значительное воздействие.

Предварительный анализ определяет один или несколько способов действия:

· Исключение незначительных рисков (так называемых допустимых рисков), которые не оправдывают обработку;

· Принятие решения для обработки неприемлемых рисков;

· Расстановка приоритетов для мер реагирования на риски.

Взвешивание рисков предусматривает входные данные по решению о необходимости обработки рисков, а также по наиболее подходящим стратегиям и методам обработки риска. Впоследствии, цель взвешивания рисков заключается в принятии решений (на основе результатов анализа риска) о том, какие риски нуждаются в обработке и какой приоритет необходимо назначить обработке. Риски связаны с задачами, поэтому им можно легко назначить приоритет с точки зрения ответных мер на такие задачи. Ранжирование и установление приоритетов по неприемлемым рискам выполняется в отношении других рисков. Поэтому решение о том, необходимо ли обрабатывать риск и как, может зависеть от затрат и выгод принятия риска, а также от затрат и выгод осуществления усовершенствованных мер контроля.

Общий подход по установлению приоритетов по рискам состоит в их подразделении на три группы:

· Верхняя группа, где уровень риска считается недопустимым вне зависимости от выгод, которые может предусматривать деятельность, а обработка риска является неотъемлемым условием вне зависимости от затрат;

· Средняя группа, где затраты и выгоды учитываются, а возможности уравновешиваются потенциальными последствиями;

· Нижняя группа, где уровень риска считается незначительным или настолько малым, что меры по обработке рисков не требуются.

Некоторые организации представляют этот портфель в виде иерархии, некоторые – в виде набора рисков, нанесенных на тепловую карту (а также карту рисков или матрицу рисков).

Во-первых, риски классифицируются по одному, двум или более критериям, например, оценка воздействия, умноженная на оценку вероятности.

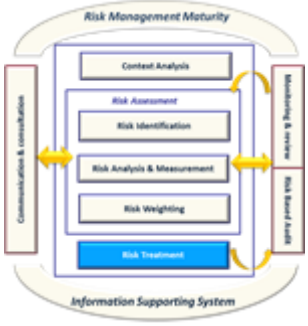
Во-вторых, порядок ранжированного риска анализируется в свете таких дополнительных аспектов, как воздействие само по себе или величина разрыва между текущим и желаемым уровнем риска (порог склонности к риску).

Если первоначальное ранжирование выполняется путем умножения финансового убытка на вероятность, то при итоговом установлении приоритетов необходимо учитывать другие качественные факторы (например, потеря репутации).

Наиболее распространенный метод установления приоритетов по рискам заключается в назначении уровня риска в каждой области графика: очень высокий, высокий, средний или низкий, при этом, чем выше общая оценка воздействия и вероятности, тем выше общий уровень риска. Границы среди уровней меняются от субъекта к субъекту, в зависимости от готовности к принятию риска. Например, границы организации с большой готовностью к принятию риска будут смещены вправо вверх, а границы организации с высокой неготовностью принятия риска будут смещены влево вниз. Кроме того, некоторые организации принимают асимметричные границы, делая несколько больший акцент на воздействии, нежели на вероятности. Например, риск с рейтингом «среднего» воздействия и «частой» вероятностью имеет назначенный уровень «высокого» риска, тогда как риск с рейтингом «крайнего» воздействия и «возможной» вероятностью имеет назначенный уровень «очень высокого риска».

4. Обработка риска

⇦	3. Оценка риска	⬘РАЗДЕЛ 2: Процесс управления рисками	5. Мониторинг и контроль	⇨



ТЕГИ: Приоритет обработки, ответные меры, смягчение риска, снижение риска.

Цель устранения (обработки) рисков заключается в превращении неопределенности в преимущество для организации, ограничивая угрозы и пользуясь возможностями.

После назначения рискам приоритетов, обработка риска должна определяться как по корпоративным, так и по операционным рискам, а также увязываться с процессами бизнес-планирования. Задача состоит в определении портфеля соответствующих ответных мер, которые формируют согласованную и комплексную стратегию, таким образом, остаточный риск попадает в пределы допустимого уровня подверженности. Стоит отметить, что нет правильной меры реагирования на риск. Выбранная мера зависит от таких вопросов, как «готовность организации к принятию риска»[1] (см. Раздел 1, Глава 1), воздействие и вероятность риска, а также затраты и выгоды планов смягчения.

Обработка риска должна соответствовать законодательным требованиям, а также правительственным и организационным политикам. Поэтому решения касательно того, требуется ли обработка риска, могут основываться на операционных, технических, финансовых, правовых, социальных, экологических или других **критериях**. Такие критерии должны отражать контекст организации, и зависят от ее внутренних политик,

целей и задач, а также потребностей заинтересованных сторон. В этой связи, командный подход может помочь правильно определить контекст и поспособствовать целенаправленному управлению изменениями во время обработки риска

[1]До разработки ответных мер по каждому выявленному риску, необходимо выяснить отношение организации к риску или «готовность к принятию риска» под влиянием размера и типа организации, ее культуры и потенциала выдерживать отрицательные воздействия.

4.1 Действия по обработке риска

4. Обработка риска	4.2 Процесс обработки риска	

Существуют разные **категории ответных мер,** которые соответствуют **ключевым общим подходам по обработке риска.** Такие категории ответных мер представлены ниже:

1. ДОПУСКАТЬ. Подверженность может быть приемлемой без каких-либо принимаемых дополнительных мер, или если она неприемлема, то может ограничиваться способность что-либо делать (или затраты на принятие каких-либо мер могут быть несоразмерны потенциальной выгоде). В таких случаях ответная мера может допускать существующий уровень риска. Такой вариант, конечно, может дополняться планированием на случай чрезвычайных обстоятельств для обработки воздействия, которое может возникнуть в случае, если риск вызовет фактические события.

Действия, связанные с таким подходом:

- Принятие риска: не предпринимается никакое действие, влияющее на вероятность или воздействие.
- Сохранение: после изменения или распределения рисков, будут наблюдаться остаточные риски, которые сохраняются. Риск может сохраняться посредством обоснованного решения: принятие бремени убытков или выгоды от доходов в результате определенного риска, включая принятие рисков, которые не были определены. Риски также могут сохраняться по умолчанию, например, при неспособности их идентифицировать или надлежащим образом распределить, или же обработать. Кроме того, после изменения или распределения возможностей, могут наблюдаться остаточные возможности, которые сохраняются без необходимости принятия какой-либо конкретной безотлагательной меры (сохранение остаточной возможности).

2. ОБРАБАТЫВАТЬ. Как правило, большая часть рисков устраняется таким способом. Цель обработки заключается в том, что во время продолжения деятельности, которая вызывает риск, предпринимаются конкретные действия, способные сдерживать такой риск до допустимого уровня.

Действия, связанные с таким подходом:

- Устранение: устранение источника риска.
- Снижение риска, действия предпринимаются для:

o Изменения вероятности (смягчающие действия): действие, выполняемое для снижения вероятности отрицательных результатов и/или повышения возможности, что позволит увеличить хорошие результаты.

o Изменения последствий (действия в непредвиденных ситуациях): действие, выполняемое для снижения степени убытков и/или повышения степени доходов с учетом соответствующих возможностей. Включает в себя создание мер, осуществляемых до событий, и ответных мер после событий, например, планы обеспечения непрерывности.

С точки зрения управления рисками, первый тип действия (изменение вероятности) должен быть предпочтительным, поскольку он предупреждает риск, а не ждет последствий.

3. ПЕРЕДАВАТЬ. Лучшей ответной мерой в отношении некоторых рисков может являться их передача[1]. Передача рисков может учитываться, как для снижения подверженности организации, или в результате того, что другая организация (которая может являться другой государственной организацией), судя по оценкам, более способна эффективно управлять такими рисками. Следует отметить, что некоторые риски не являются (полностью) передаваемыми: в частности, едва ли репутационный риск можно передать. Необходимо тщательно управлять взаимоотношениями с третьей стороной, которой передается риск, чтобы обеспечить успешную передачу.

Действия, связанные с таким подходом:

- Передача[2] риска или его части[3].
- Распределение[4]: другая сторона или стороны берут на себя или разделяют некоторую часть рисков, обычно предусматривая дополнительный потенциал или ресурсы, которые повышают вероятность возможностей или объем доходов. Распределение положительных результатов может включать распределение некоторых затрат, связанных с получением таких результатов. Меры по распределению зачастую могут вводить новые риски, в том смысле, что другая сторона или стороны фактически не могут предоставить необходимый потенциал или ресурсы.

4. ПРЕКРАЩАТЬ. Некоторые риски могут поддаваться обработке или снижению только при прекращении деятельности. Стоит отметить, что этот вариант может весьма ограничиваться в государственном секторе по сравнению с частным. Такой фактор может быть особенно важным при управлении проектом.

- Избежание: действие предпринимается для прекращения деятельности, вызывающей риск, или избежание риска, при котором такая деятельность не начинается (если такой вариант может осуществляться на практике). Избежание риска не может происходить надлежащим образом, если лица или организации неоправданно избегают риски. Нецелесообразное избежание риска может или повысить значимость других рисков, или привести к утрате возможностей.

5. ВОСПОЛЬЗОВАТЬСЯ ВОЗМОЖНОСТЬЮ. Такой вариант не является альтернативным вышеуказанным. Скорее, это вариант, который следует рассматривать каждый раз при допущении, передаче или обработке риска. Это может происходить двумя способами: первый, когда появляется возможность использовать положительное воздействие вне зависимости от того, предпринято ли одновременно действие по смягчению угроз или нет. Второй, когда появляются обстоятельства, которые, не образуя угрозы, предлагают положительные возможности.

- Принятие/повышение: принятие или повышение риска, чтобы воспользоваться возможностью.

Варианты обработки риска необязательно являются взаимоисключающими или могут подходить во всех обстоятельствах. Часто мера реагирования на риск может сочетать две или несколько стратегий, что позволяет достичь желаемых результатов. Если организация использует несколько вариантов обработки, то это может на нее положительно сказаться. Осуществление выбранных ответных мер подразумевает разработку плана рисков, где выделяются процессы управления, которые будут применяться для управления рисками или возможностями до уровня, установленного «готовностью организации к принятию риска» и культурой.

Обработка риска включает выбор одного или нескольких вариантов изменения рисков, и осуществление таких вариантов. После выполнения обработка предлагает или изменяет меры контроля: любое действие, предпринятое для устранения риска, формирует часть того, что известно как «меры внутреннего контроля».

[1] Может выполняться путем традиционного страхования или путем выплаты третьей стороне за принятие на себя риска. Такой вариант особенно эффективен для смягчения финансовых рисков или рисков для активов.

[2] Стандарт ISO 73:2009 рассматривает «передачу рисков» как вид распределения рисков.

[3] Например, через страхование или аутсорсинг.

[4] Стандарт ISO 73:2009 подчеркивает, что распределение рисков включает согласованное распределение риска с другими сторонами, отмечая, что правовые или нормативные требования могут ограничивать, запрещать или требовать принятия части риска. Кроме того, степень распределения риска может зависеть от надежности и прозрачности мер распределения.

4.2 Процесс обработки риска

Обработка риска включает **циклический процесс**:

а) Оценка обработки риска: определение и оценка вариантов обработки риска;

б) Планирование обработки риска: подготовка графика обработки риска и плана действий;

в) Мониторинг эффективности такой обработки (см. Главу 5);

г) Измерение остаточного риска: принятие решения о том, является ли остаточный риск допустимым;

Обратная связь: если остаточный риск не является допустимым, выполнение новой обработки риска (обратно к шагу а) и повтор процесса.

a) Оценка обработки риска: организация должна выбрать наилучший имеющийся вариант. Такой вариант предполагает сбалансирование затрат на осуществление каждого варианта относительно выгод, получаемых в результате, с учетом правовых, нормативных и других требований, например, социальная ответственность. Как правило, затраты на управление рисками необходимо сбалансировать с полученными выгодами. При вынесении таких суждений о затратах относительно выгод, необходимо учитывать контекст. Важно учитывать все прямые и косвенные затраты и выгоды, будь то материального или нематериального характера, и измерять их с финансовой или другой перспективы.

b) План обработки риска: Обработка должна включать в себя на оперативном уровне подготовку и осуществление соответствующего плана. Он показывает, как будут реализованы выбранные варианты и как они должны интегрироваться с управленческими и бюджетными процессами. В частности, информация, представленная в плане обработки, должна включать следующее:

а. Причины выбора вариантов обработки, включая ожидаемые выгоды;

б. Сторона, несущая ответственность за утверждение плана, и сторона, ответственная за его реализацию;

в. Предложенные действия;

г. Требования к ресурсам, включая резервы на непредвиденные затраты;

д. Показатели работы и ограничивающие условия;

е. Требования к отчетности и мониторингу;

ж. Сроки и график.

И, наконец, ответственности, связанные с фазой обработки, должны устанавливаться четким образом, при этом, необходимо указать сторону, ответственную за управление определенными рисками (или категориями рисков), за реализацию стратегий обработки, а также за осуществление мер контроля рисков. Для этого, совет должен гарантировать, что руководство учитывает и осуществляет соответствующие меры реагирования на

риски: ответственность за обработку, как правило, несет руководство (генеральные директоры, руководители подразделений, руководители проектов) и в соответствующих случаях персонал. Руководство должно определить и записать в «регистре рисков» те действия, которые выбраны в качестве обработки, и показать совету, как такие ответные меры на риски повышают эффективность организации. Для создания планов обработки риска указываются владельцы риска в соответствии со своими функциями в проекте или процессе, даже если на этом этапе ответственности варьируются по виду рисков (корпоративные или операционные). Например, старшие менеджеры ответственны за корпоративные риски, стратегии их смягчения и планы действий. Ответственность за операционные риски возлагается на уровне подразделений, за которым закреплена программа.

c) Мониторинг обработки риска: при разработке ответных мер, важно, чтобы введенные в действие меры **контроля** были пропорциональны рискам. Анализ рисков помогает такому процессу, определяя те риски, которые требуют внимания со стороны руководства. Приоритетность действий по контролю риска будет назначаться в соответствии с их потенциалом представления выгод для организации. Эффективность внутреннего контроля определяется тем, насколько риск будет устранен или снижен с помощью предлагаемых мер контроля. Если действие не предпринимается, такие меры необходимо измерять с точки зрения потенциального экономического эффекта относительно затрат на предложенные меры, и такие меры неизменно требуют более подробной информации и допущений, доступных в кратчайшие сроки. Каждая ответная мера предполагает соответствующие затраты, и важно, чтобы обработка предлагала качество по разумной цене по отношению к контролируемому риску. В этой связи, варианты устранения риска («ОБРАБАТЫВАТЬ») могут в дальнейшем анализироваться с точки зрения четырех разных видов **соответствующих/сопутствующих мер контроля**:

- МЕРЫ ПРОФИЛАКТИЧЕСКОГО КОНТРОЛЯ. Предназначаются для ограничения нежелательных результатов. Чем больше следует избегать нежелательного результата, тем больше соответствующих мер профилактического контроля необходимо выполнять[1]. Большинство мер контроля, внедренные в организации, принадлежат этой категории.
- МЕРЫ КОРРЕКТИРУЮЩЕГО КОНТРОЛЯ. Предназначаются для корректировки возникших нежелательных результатов, и предусматривают способ восстановления от потерь или ущерба[2]. Планирование на случай чрезвычайных обстоятельств является важным компонентом меры корректирующего контроля.
- МЕРЫ ДИРЕКТИВНОГО КОНТРОЛЯ. Предназначаются для достижения определенного результата, особенно важны при избегании нежелательного события, как правило, связанного с охраной здоровья и труда или безопасностью, что является критически важным условием[3].
- МЕРЫ КОНТРОЛЯ ОБНАРУЖЕНИЯ. Предназначаются для выявления нежелательных результатов. Их эффект, по определению, возникает «после события», поэтому они подходят только в случаях, когда могут признаваться результирующие потери или убытки[4].

г) Измерение остаточного риска: Если остаточный риск сохраняется даже после обработки, необходимо принять решение о том, следует ли сохранить этот риск или лучше повторить процесс обработки риска. Для остаточных рисков, которые считаются высокими, необходимо собрать информацию о затратах на реализацию стратегий по дальнейшему смягчению.

ПРИМЕР ПЛАНИРОВАНИЯ ОБРАБОТКИ РИСКА

ОБРАБОТКА РИСКА – ГРАФИК
ПРЕДЛАГАЮЩИЙ ДЕПАРТАМЕНТ _____ УТВЕРЖДАЮЩИЙ ДЕПАРТАМЕНТ _____ ОТВЕТСТВЕННОСТЬ _____

ВИД ОБРАБОТКИ _____	
ОПИСАНИЕ РИСКА	……
ПРОЦЕСС	……
ФАЗА	……
ПРИЧИНА	……
ДВИЖУЩИЕ ФАКТОРЫ	……
ГРАФИК	……

ОБРАБОТКА РИСКА – МОНИТОРИНГ		
ЗАДАЧИ	……	
ПОКАЗАТЕЛИ РЕЗУЛЬТАТА	……	
ПРОЦЕДУРА КОНТРОЛЯ	……	
ОБРАБОТКА РИСКА – ПЛАН ДЕЙСТВИЙ		
ФАЗА	ЕДИНИЦА	ВРЕМЯ
1. ……	……	……
2. ……	……	……
3. ……	……	……

Вопроы и ответы

Вопрос 1. Применяется ли обработка рисков в вашей организации после идентификации и оценки риска?

Ответ 1. «Да. Обработку наиболее существенных рисков выполняют менеджеры, после чего проводится последующий контроль (ежегодно или дважды в год советом директоров). Менее существенные риски обрабатываются в рамках стандартных процедур. Обработка средних или повышенных рисков передается управленческой группе департамента на утверждение. Обработка выполняется лицом, ответственным за выполнение обработки в рамках стандартных операций, а при невозможности этого необходимо подготовить отдельный план реализации».

Источник: Финляндия, *Обзор практики управления рисками*

Ответ 2. «Да. Риск взвешивается, а владельцам активов приходится создавать план по сокращению рисков, которые измеряются выше определенного уровня»

Источник: Исландия, *Обзор практики управления рисками*

Ответ 3. «Да. Обработка определяется как часть процесса

идентификации риска – шаблон заполняется руководителями подразделений дважды в год, и создаются регистры рисков отдельных директоратов и регистр корпоративных рисков. Устанавливается право владения риском, а процесс пересматривается дважды в год комитетом старшего руководства совместно с отдельным руководителем подразделения. Система управления проектом также содействует идентификации и управлению рисками, и команда проекта регулярно проводит анализ проекта. Обработка управления рисками может включать решения, связанные с человеческими ресурсами».

Источник: Ирландия, *Обзор практики управления рисками*

Ответ 4. «Да. Обработка рисков является основным результатом анализа риска. Результаты известны как меры контроля. В некоторых случаях меры контроля создаются на основе предыдущего опыта, задолго до формального анализа риска. Однако только полный анализ может достаточно широко гарантировать учет всех аспектов и готовность учреждений столкнуться с последствиями.

Источник: Мексика, *Обзор практики управления рисками*

Ответ 5. «Да, в соответствии с процедурой системы по управлению рисками, утвержденной Президентом НИС (Решение № 1038/2011). Учитываются проверочные отчеты по управлению рисками, что позволяет предложить меры по обработке».

Источник: Румыния, *Обзор практики управления рисками*

Вопрос 2. Пожалуйста, укажите, какими видами рисков происходит управление в процессе управления рисками, указывая связи и различия в обработке:

Вопрос 1. «Подход по обработке зависит от повышенного или пониженного влияния ЦСБ в сокращении риска до приемлемого уровня. Что касается обработки риска, большинство выявленных и оцененных рисков классифицируются на две категории: сокращение риска и избегание риска, или же сочетание обоих вариантов».

Источник: Хорватия, *Подробный обзор практики управления рисками*

Вопрос 3. Пожалуйста, опишите методологию, используемую в выявлении и мониторинге обработки риска, указывая функции участвующей организации:

Ответ 1. «Методология, используемая НИСГ, основана, главным образом, на международном стандарте ISO 31000 об управлении рисками, ISO/IEC 27000 об информационной безопасности, некоторых компонентах COSO ERM (общеорганизационное управление рисками),

а также на основе стандарта Европейской федерации рисков (FERMA). Первая версия методологии была выпущена в 2010 году, а настоящая версия является результатом институционального опыта использования».

Источник: Мексика, *Подробный обзор практики управления рисками*

Вопрос 4. Ссылаясь на управления рисками, внутренний контроль и систему внутренней проверки в вашей организации, опишите связь/интеграцию между ними более подробно, указывая следующее: как отслеживаются работы по обработке риска, функции, роли и ответственности, применяемые в мониторинге работ по обработке рисков …»

Ответ 1. «Что касается рисков, каждый руководитель административной единицы несет ответственность за установление, анализ, оценку и определение работ по обработке».

Источник: Мексика*, Подробный обзор практики управления рисками*

Вопрос 5. Пожалуйста, опишите, кто устанавливает приоритеты работ по обработке рисков и как:

Ответ 1. «На корпоративном уровне совет директоров устанавливает приоритеты». На уровне процесса приоритеты устанавливает владелец процесса».

Источник: Нидерланды, *Подробный обзор практики управления рисками*

Вопрос 6. Применяется ли обработка рисков в вашей организации после идентификации и оценки риска?

Ответ 1. «Да. Директоры/руководители подразделений (владельцы риска) предлагают ответные меры, утвержденные менеджером по рискам/менеджером по предупреждению мошенничества и коррупции. Эти меры отбираются на основе приоритетов (стратегическая область рисков, значение риска, обоснованность), а затем вверяются исполнителям. Менеджеры предлагают ответные меры, правительство выбирает меры после установления их значимости (установление приоритета). Структура заполняется внутренней репрезентативной сетью. Утвержденные и выбранные ответные меры разрабатываются, осуществляются и контролируются под ответственностью менеджеров (директоры/руководители подразделений). Структура заполняется контрольной информацией репрезентативной сетью».

Источник: Италия, *Обзор практики управления рисками*

[1] Примеры мер профилактического контроля включают только ограниченное количество уполномоченных лиц, например, только тем, кто имеет соответствующую подготовку и разрешение позволяется обрабатывать запросы СМИ, предупреждая выход несоответствующих комментариев в прессу.

[2] Например, составление пунктов договора, допускающих взыскание излишне выплаченных сумм. Страхование также может рассматриваться, как вид

корректирующего контроля, поскольку оно способствует финансовому восстановлению относительно актуализации риска.

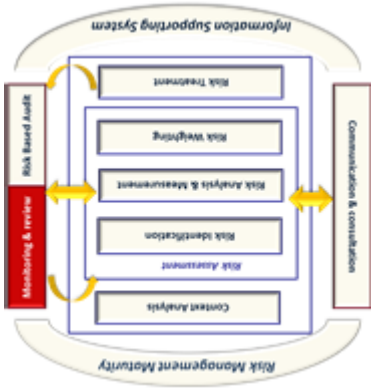
[3] Например, требуется, чтобы персонал был подготовлен в части получения определенных навыков, прежде чем им будет разрешено работать без контроля.

[4]Примеры контроля обнаружения включают «Анализы после реализации», которые демонстрируют уроки, полученные на основе проектов, и которые можно применить в будущей работе, а также мониторинг деятельности, направленной на обнаружение изменений, в отношении которых применяются ответные меры.

5. Мониторинг и контроль

⇦	4. Обработка риска	РАЗДЕЛ 2: Процесс управления рисками	6. Контроль и проверка с учетом уровня рисков ⇨

ТЕГИ: Мониторинг, анализ, функции и ответственности, ключевые показатели риска; проверка с учетом уровня рисков; цикл внутренней проверки.



5.1 Мониторинг и анализ

5. Мониторинг и контроль	5.2 Ключевые показатели риска ⇨

Управление рисками носит динамический, итеративный и чувствительный к изменениям характер. По мере изменения рисков и приоритетов, обработка риска должна контролироваться в рамках процесса управления рисками.

Процессы мониторинга организации должны охватывать все свойства управления рисками, чтобы:

· Обеспечить эффективность и действенность мер контроля;

· Обнаружить изменения в имеющихся рисках, которые требуют пересмотра в части обработки рисков и приоритетов;

· Выявить появляющиеся риски.

Мониторинг и анализ – это два разных и взаимодополняющих вида деятельности. Мониторинг включает рутинный контроль фактических показателей относительно ожидаемых (или требуемых) показателей, тогда как анализ подразумевает

периодическую (минимум раз в год) проверку текущей ситуации на изменения во внутреннем/внешнем контексте.

Общая ответственность за мониторинг и анализ лежит на совете и старшем руководстве: способ реагирования старшим руководством на результаты программы мониторинга влияет на деятельность сотрудников.

Мониторинг должен являться неотъемлемой частью управления, а риск и меры контроля относятся на счет владельцев, которые в силу этого несут ответственность за их мониторинг. Стандартный подход к мониторингу включает:

· Сканирование окружающей среды владельцами риска для контроля изменений в рисках или в контексте;

· Мониторинг плана по обработке риска, выполняемый владельцами риска;

· Мониторинг мер контроля владельцами мер контроля и специалистами по риску посредством показателей эффективности и ключевых показателей риска, в соответствии с количественным порогом, описанным в заявлении о готовности к принятию риска (см. ниже).

Работы по мониторингу и анализу также должны рассматриваться с точки зрения иерархии. Ответственность может меняться в зависимости от вида контролируемых рисков (корпоративный, операционный, проектный): операционные риски контролируются на уровне хозяйствующей единицы, проектные риски контролируются в рамках системы управления проектами, а корпоративные риски контролируются старшими менеджерами (т.е. генеральные директоры или руководители департаментов).

5.2 Ключевые показатели риска

	5.1 Мониторинг и анализ	5. Мониторинг и контроль

Ключевые показатели риска (КПР) применяются для мониторинга работ по обработке рисков.

Ключевые показатели риска – это количественные показатели, используемые для раннего обнаружения роста подверженности риску в разных областях в пределах организации. В некоторых случаях они могут представлять ключевой коэффициент, который отслеживается руководством по всей организации в качестве показателей развивающихся рисков и потенциальных возможностей, что говорит о необходимости принятия мер. Другие могут носить более сложный характер, и объединять несколько показателей индивидуальных рисков в многомерный балл по появляющимся событиям, что может привести к новым рискам или возможностям.

КПР, как правило, образуются в результате определенных событий или коренных причин на внутреннем или внешнем уровнях, которые могут помешать в достижении целей работы. Связь основных рисков с основными стратегиями помогает точно определить наиболее актуальную информацию, которая может служить в качестве эффективного опережающего индикатора появляющегося риска.

Эффективный метод разработки КПР начинается с анализа рискового события, сказавшегося на организации в прошлом (или в настоящем), а затем проводится работа в обратном направлении по выделению промежуточных и коренных событий, которые привели к наибольшей потере или потерянной возможности. Чем ближе КПР к коренной причине рискового события, тем вероятнее, что КПР предусмотрит время на управление для принятия положительных действий, направленных на реагирование на такое событие.

Эффективные КПР часто разрабатываются командами, состоящими из персонала по управлению профессиональными рисками и руководителями хозяйствующих единиц, обладающими глубоким пониманием операционных процессов и потенциальных рисков. Теоретически, эти КПР разрабатываются на основе стратегических планов отдельных

хозяйствующих единиц, и затем могут внедрять допустимые отклонения плана, которые находятся в пределах общей готовности организации к принятию риска.

Разработка показателей КПР, которые могут предусматривать актуальную и своевременную информацию для совета и старшего руководства, представляет собой существенный компонент эффективного надзора за рисками. Также важно учитывать частоту отчетности по КПР. Соответствующий временной горизонт зависит от главного пользователя определенного КПР. Что касается оперативных руководителей, может потребоваться отчетность в режиме реального времени. Что касается старшего руководства, если целью является составление показателей КПР, которые выделяют потенциальные отклонения от целевых показателей на уровне организации, то отчетность о статусе может быть не такой частой (например, раз в неделю). На уровне совета, отчетность зачастую агрегируется, что позволяет провести расширенный анализ. Затем руководство может проводить такие анализы для определения информации, относящейся к коренному событию или промежуточному событию. Такая информация может служить в качестве ключевого показателя риска, относящегося к любому событию. Когда проводится мониторинг КПР по коренным и промежуточным событиям, руководство может наилучшим образом определить стратегии раннего смягчения, позволяющие сократить или устранить воздействие, вызываемое появляющимся рисковым событием.

Показатели КПР не управляют и не обрабатывают риск, и без надлежащей разработки могут привести к ложному чувству безопасности. Важной особенностью любого КПР является качество доступных данных, используемых для мониторинга специфического риска, при этом необходимо уделять внимание источнику информации, будь то внутренняя для организации информация или информация, поступающая от внешней стороны. Могут существовать источники информации, сообщающие о решениях, сделанных в пользу выбора КПР. Например, могут быть доступны внутренние данные в отношении предшествующих рисковых событий, которые могут содержать информацию о потенциальных будущих воздействиях. Тем не менее, по многим рискам внутренние данные часто отсутствуют, особенно если они ранее не встречались. Кроме того, риски могут зачастую оказывать существенное воздействие ввиду внешних источников, например, изменение экономических условий, смещение процентных ставок или новые нормативные требования/законодательство. Поэтому КПР могут основываться на внешних данных, учитывая, что коренные и промежуточные события могут возникнуть за пределами организации.

Хорошо разработанный КПР должен:

1) Основываться на установившихся практиках или сравнительных анализах;

2) Последовательно разрабатываться по всей организации;

3) Предусматривать однозначное и понятийное представление выделенного риска;

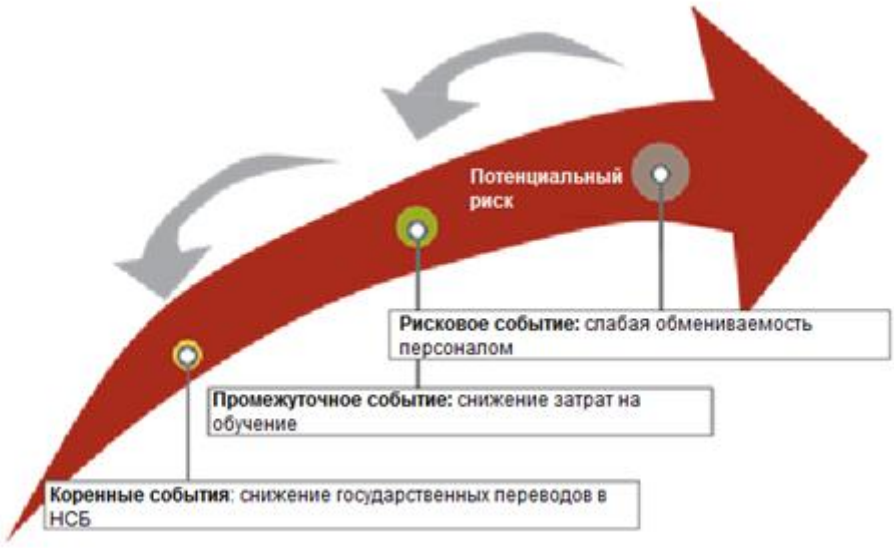
4) Предусматривать измеряемые сравнения по времени и хозяйствующим единицам;

5) Предусматривать возможности для регулярной оценки показателей владельцев риска;

6) Эффективно потреблять ресурсы.

На рисунке ниже представлена идентификация ключевого показателя риска, связанного с задачей «Повышение ротации работ», которая дополняется развитием причинно-следственной цепи между событием, которое может негативно сказаться на определенной задачей, и его коренной причиной.

Рисунок 4: Пример ключевого показатели риска: «Повышение ротации работ»



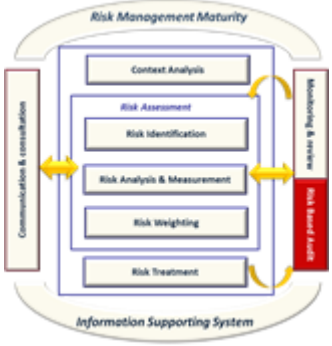
Формула:

Ключевой показатель эффективности (КПЭ)	**Ключевой показатель эффективности (КПЭ)**	**Ключевой показатель эффективности (КПЭ)**
% кадровых перестановок в год	*% трансфертов персонала в год*	*% затрат на обучение в год*

6. Контроль и проверка с учетом уровня рисков

5. Мониторинг и контроль	РАЗДЕЛ 2: Процесс управления рисками	7. Информационная система управления рисками	

ТЕГИ: ПУР, цикл внутренней проверки.



Структура внутреннего контроля, которая включает структуру управления рисками и структуру внутренней проверки, проводит различие между тремя уровнями контроля:

- Внутренний контроль (профилактически или последующий), развернутый в рамках структуры управления рисками, под ответственностью руководства (владельцы риска), направлен на предупреждение или сокращение последствий, связанных с возникновением риска;

- Уровень «соответствия» направлен на содействие и мониторинг управления фактическими рисками их владельцами. Такой уровень курирует процессы оценки и

контроля риска, обеспечивая их соответствие целям организации (группа управления рисками);

- «Проверка с учетом уровня рисков» обеспечивает эффективное развертывание ресурсов для оценки управления этими рисками, связанными с действиями организации путем анализа и оценки соответствия системы управления рисками и мер внутреннего контроля, процессов и руководства. Поэтому меры внутренней проверки направлены на контроль и демонстрацию хода реализации рекомендаций по проверке, а также на улучшение областей проверок.

Задачи проверки с учетом уровня рисков (ПУР):

Ø **Обеспечение стратегии управления рисками**: чтобы выяснить, в какой степени все линейные менеджеры анализируют риски/меры контроля в рамках объема своей ответственности, чтобы оценить соответствие политики и стратегии управления рисками для достижения задач;

Ø **Обеспечение управления рисками/мерами контроля**: чтобы охватить все ключевые риски, а также достаточное количество других рисков для поддержания доверия к достигнутому общему мнению; чтобы оценить соответствие процессов управления рисками, предназначенными для сдерживания остаточного риска до уровня готовности к принятию риска;

Ø **Обеспечение соответствия процесса анализа/гарантии**: качество, гарантированное для формирования доверия к процессу анализа, чтобы определить ограничения в представленных доказательствах или ограничения, связанные с глубиной/объемом предпринимаемых анализов, чтобы выявить пробелы в контроле и/или чрезмерный контроль, и предусмотреть возможности непрерывного улучшения, чтобы поддержать подготовку суммарного отчета по внутренней проверке для комитета по статистике/главного статистика.

Цикл управления ПУР выполняется в виде следующих шести шагов:

а) **Объект**: процедуры, процессы и внутренние услуги, риски, выбранные в соответствии с приоритетами, но: риски в пределах готовности к принятию риска, риски, не требующие проверку в краткосрочной перспективе, риски, проверенные иным способом, допустимые риски.

б) **План проверки**: внутренние проверки, проводимые в краткосрочной перспективе, осуществляются в соответствии с годовым планом, который заверяется советом и сообщается участвующим подразделениям организации. Такой план демонстрирует на основе какой-либо деятельности: i) продолжительность проверки, ii) состав команды, iii) ответственности, iv) задачи проверки (согласно процедурам, договорным требованиям и т.д.), v) требуемые документы, vi) период подготовки. Годовой план составляется на один год на основе стратегического плана в соответствии с оценкой риска. Поэтому при планировании проверки учитываются результаты предыдущих исследований, а также оценка руководством текущих уровней риска относительно специфических программ организации.

в) **Подготовка проверки**, состоит из некоторых работ, предшествующих фактической проверке, например: а) формальное распределение обязанностей; б) определение плана работ; в) определение документов, необходимых для установления диапазона проверки исходных документов и работ; г) сообщение о начале проверки; д) стартовое совещание с вовлеченным персоналом.

г) **Проведение проверки**, фактическая проверка, состоящая из следующих работ: i) производственные совещания; ii) предварительная оценка критических значений; iii) проверка пригодности и соответствия управлению рисками или системе качества; iv) составление рекомендаций и возможных смягчающих мер. Проверки могут помогать менеджерам по риску в оценке эффективности мер контроля по каждому риску. Оценка может выполняться вне зависимости от того, соответствуют ли меры контроля для снижения уровня риска (т.е. для снижения риска с крайне/высокого уровня до среднего или низкого), или требуются ли дополнительные меры обработки/контроля.

д) **Отчетность.** Проверка завершается совещанием, на котором происходит обмен полученными основными результатами. Отчет по проверке содержит следующее: i) результаты, ii) выполненные действия, iii) обнаруженные критические значения и предложения, iv) план возможных действий в сотрудничестве с вовлеченной единицей/подразделением. После оценки эффективности мер контроля по каждому риску, будут представлены предложения по стратегиям дополнительной обработки, направленным на сокращение уровня риска. Кроме того, некоторые стратегии обработки, предложенные во время этого процесса, могут быть включены в план внутренней проверки (отзывы).

Последующие действия направлены на проверку фактической реализации ответных мер, связанных с какими-либо комментариями или рекомендациями.

Вопросы и ответы

Вопрос. Ссылаясь на управление рисками, внутренний контроль и систему внутренних проверок в вашей организации, опишите связь/интеграцию между ними более подробно

Ответ. «Стратегический план внутренней проверки соответствует задачам, содержащимся в Стратегическом плане».

(Источник: Хорватское статистическое бюро, Подробный обзор практики управления рисками)

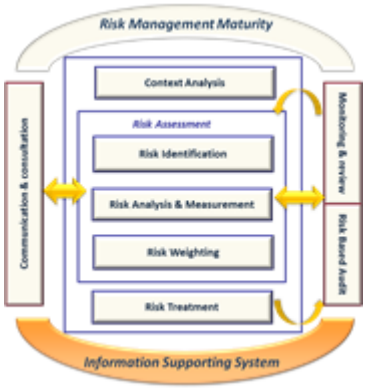
Ответ. «После анализа ключевых стратегических/операционных областей, программа внутренней проверки будет иметь приоритет по согласованной оценке и классификации рисков»

(Источник: Австралийское бюро статистики, Подробный обзор практики управления рисками)

7. Информационная система управления рисками

6. Контроль и проверка с учетом уровня рисков	РАЗДЕЛ 2: Процесс управления рисками	8. Модель зрелости управления риском	

ТЕГИ: Управление документооборотом, информационный менеджмент, комплексная и сетевая информационная система, программное обеспечение по управлению рисками, запись, веб-инструмент.



Организация должна документально записывать то, как управляет рисками. Информация о рисках и результаты процесса управления рисками должны **записываться** последовательным и надежным способом, формируя политику и процедуры, необходимые для получения доступа, использования и передачи информации в рамках плана информационного менеджмента. Информационные системы управления рисками должны:

- Регистрировать детали рисков, мер контроля и приоритетов, и демонстрировать любые изменения в них;
- Регистрировать обработку риска и соответствующие требования к ресурсам;
- Регистрировать детали инцидентов и случаев наступления убытка, а также полученные уроки;
- Отслеживать отчетность по рискам, мерам контроля и обработки;
- Отслеживать прогресс и регистрировать завершение работ по обработке рисков;
- Предусматривать проверку хода работ относительно плана управления рисками;
- Осуществлять мониторинг и обеспечивать гарантию.

  Организация должна определить достаточное количество ресурсов с точки зрения информационных систем и систем управления документооборотом, таким образом, информация о потенциале будет актуальной, надежной, своевременной и доступной. Для этого необходимо управлять соответствующими записями и процессами, которые формируют поток своевременной, соответствующей и надежной информации. Поэтому каждый этап процесса управления рисками должен соответствующим образом записываться. Управления записями – это важный аспект эффективного корпоративного управления: дополняет деятельность и решения, а также обеспечивает отчетность перед настоящими и будущими заинтересованными сторонами.

  Качество информационного менеджмента и управления документооборотом зависит от следующих **принципов**:

  - Информация по организации должна быть последовательна, предусматривать эффективный и точный поток;
  - Стандартизация определения терминов и описания гарантирует одинаковое понимание информации разными частями организации, или предупреждает работу с противоречащими наборами информации;
  - Нет необходимости в наличии единой системы управления записями по организации, поскольку руководство разрабатывает и использует множество систем, предусматривающих **эффективную консолидацию, обмен и интеграцию информации**.
  - На операционном уровне организация должна сначала установить определения, классификации и процедуры, необходимые для выявления и управления информацией о рисках в рамках плана информационного

менеджмента. Затем, в качестве основных субпрактик необходимо создать «записи по управлению рисками» на основе следующих шагов:

о Определение и поддержание схемы классификации и методологии управления рисками;

о Определение непрерывного процесса по инвентаризации и классификации информации об управлении рисками, включая такие характеристики, как: тип, требование по сохранению, требование по удержанию, требование по размещению, требование по доступности, оперативное/стратегическое значение, владелец данных, источник информации (база данных/применение, электронная почта, электронная таблица и т.д.), требование к конфиденциальности и сопутствующие процессы и политики организации.

- Организация должна периодически учитывать изменения в структуре классификации, а также в случае необходимости лежащие в основе определения и классификации.

Весь процесс управления рисками должен документально подтверждаться с помощью веб-инструмента, который позволяет передавать и осуществлять эскалацию рисков и мер обработки на организационном уровне, а также дает возможность увязать определенную цель или деятельность оперативного плана агентства (или собственных планов действий департаментов). Следовательно, организация должна определить требования к ресурсам, связанным с информационными системами и базами данных.

Основные особенности информационной системы управления рисками по каждой фазе процесса управления рисками: обмен данными/совместимость, интеграция данных, отслеживаемость, защита данных.

Идентификация, анализ и измерение риска должны выполняться с помощью специального средства в четыре этапа:

1. Качественная оценка (идентификация риска и анализ риска). Информационное средство по управлению рисками регистрирует результаты оценки риска так, чтобы это способствовало мониторингу и определению приоритетов риска. Оценка риска должна подтверждаться документально, при этом необходимо регистрировать эти фазы обработки. Документирование результатов оценки риска показывает профиль риска организации, который: содействует определению приоритетов риска (в частности, для выявления вопросов по наиболее существенным рискам, которые старшее руководство должно учесть); регистрирует причины решений, принятых в отношении допустимого и недопустимого воздействия, содействует регистрации процесса принятия решения по устранению риска, позволяет всем, кто занимается управлением рисками, наблюдать за профилем общего риска, а также за тем, какие области определенной ответственности соответствуют этому, кроме того, содействует анализу и мониторингу рисков.

2. Установление приоритета;

3. Измерение риска;
4. Мониторинг действий по обработке риска. Штатные сотрудники/менеджеры, ответственные за обработку рисков, должны составлять периодические отчеты (например, ежемесячно, ежеквартально, ежегодно) о реализации/выполнении работ с помощью средства.

Вопросы и ответы

Вопрос 1. Какие наиболее важные уроки, полученные в результате управления рисками в вашей организации, должны учесть другие организации при разработке собственных процессов по управлению рисками?

Ответ 1. «Эффективное IT-средство является очень важным»

Источник: Австрия, *Обзор практики управления рисками*

Вопрос 2. В вашей организации сумма финансовых ресурсов, направленная на запуск системы управления рисками, является соответствующей.

Ответ 2. «Было инвестировано достаточно ресурсов в информационную систему, дополняющую процесс управления рисками».

Источник: Италия, *Обзор практики управления рисками*

Вопрос 3: В вашей организации процесс управления рисками связан с:

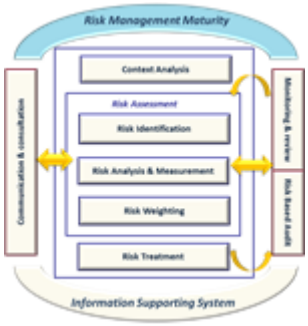
Ответ 3. «Оценкой эффективности организации: анализ риска полностью интегрируется в процесс планирования и последующий процесс контроля деятельности, и сообщается каждым департаментом с помощью единого веб-инструмента». Что касается стандартных методов по идентификации и оценке риска: «важным является правильная система регистрации результатов с помощью веб-инструмента».

Источник: Швеция, *Подробный обзор практики управления рисками*.

8. Модель зрелости управления риском

7. Информационная система управления рисками	РАЗДЕЛ 2: Процесс управления рисками	9. Полученные уроки	

ТЕГИ: Корпоративная зрелость по отношению к риску, этап разработки, эволюционный путь, уровень / степень сложности, шкала зрелости, показатели зрелости, модели зрелости, измерение прогресса, поэтапная реализация, потенциал управления риском.



Для обеспечения сравнительного анализа между уровнями внедрения управления рисками в организациях, исследователи, государственные учреждения, профессиональные ассоциации и органы стандартизации попытались определить свою собственную модель управления рисками[1]. Такой вид инструмента включает в себя основные элементы процессов эффективного управления рисками и отражает **эволюционную шкалу** от основного подхода к внедренному и целостному подходу. Он позволяет НСБ измерять прогресс в развитии необходимых способностей по управлению рисками, а также оценивать эффективность снижения риска и влияния на получение благоприятных результатов. Он также содействует развитию общего языка и понимания. Поэтапный подход позволяет НСБ: оценить то, чего оно уже добилось; установить цели в отношении будущего; обозначить пути достижения таких целей, фокусируя усилия на усовершенствовании областей с выявленными слабыми сторонами. Более того, модель зрелости может служить в качестве программы по признанию[2] в пределах организации: достижение уровня зрелости может рассматриваться в качестве показателя эффективности.

Более того, при условии, что:

- отсутствует оптимальный уровень зрелости, который рассматривался бы в качестве надлежащего для каждой организации (он зависит от внешнего контекста, размера, внутренней культуры, людей, истории, сложности деятельности организаций и т.д.)[3]; и

- один и тот же субъект может представлять различные уровни зрелости по отношению к разным организационным сферам (любые процессы и виды деятельности, связанные с управлением рисками, могут быть лучше развиты, чем другие);

- Для содействия более глубокому пониманию управления рисками, предлагается **сетка многомерного анализа и считывания** (Рисунок 5, полная версия представлена в Приложении). Она учитывает входные данные из различных источников: сбор данных по фактическим случаям внедрения систем управления рисками среди статистических организаций (*практики*); выборочные примеры, сообщающие определенные данные о достоверном опыте НСБ; существующие модели зрелости, отражаемые в научной и технической литературе, которые также входят в различные области.

- Сетка была разработана посредством извлечения принципов создания моделей зрелости возможностей, соблюдаемых в проанализированных практиках, а также посредством обзора литературы. Ее структура – это матрица, где каждая клетка заполняется данными о компетенции или возможности. Во-первых, были определены *некоторые ключевые области*/позиции, представляющие ряды значимых особенностей. В качестве второго шага были разработаны специальные дескрипторы с целью более подробного отображения различных тем, связанных с ключевыми областями. Дескрипторы позволяют распределять статьи среди четырех уровней зрелости, отличающихся на основании индикаторов атрибутов/деятельности, состоящих из возможных/типичных характеристик, которые отражают объем, в котором определены, узаконены или контролируются компетенция или возможности по управлению рисками. Многомерная сетка была спроектирована в качестве инструмента для диагностики вместо предписывающей модели для осуществления: ее подход основывается на утверждении, что качество процесса организации по управлению рисками должно повышаться с течением времени, предусматривая такое повышение при каждом шаге к повышенной зрелости.

- Сетка также делает акцент (для каждого дескриптора) на трех компонентах или ключах считывания, которые используются при проектировании обследования, а также на фазе обработки. Собранные данные анализируются в соответствии с теоритической парадигмой/протоколом под названием «Шаблон»[4]. Первый компонент – *рациональность риска (процессы)* – соответствует попыткам организации перевести неопределенность на поддающуюся управлению и передаче концептуализацию рисков, а также определение действий и задач для достижения таких целей. Он отражает главную цель, вокруг которой любая организация закладывает основу своей стратегии по управлению рисками (т.е. повышение соответствия, результативности, стоимости компании и т.д.). Второй компонент – *эксперты по неопределенности (роли)* – относится к участникам (их опыту, подготовке и взаимодействию), организационным подразделениям или структурам, которым организация назначает ответственность за

управление рисками. Третий компонент анализа – *технологии (поддержка)* – указывает на сложные наборы практик, процедур и инструментов, вводимых для осуществления управления и контроля рисков.

- Зрелость системы управления рисками организации может быть распределена по группам, которые варьируются от не сопровождающихся формальным процессом до полностью интегрированных во все аспекты предприятия. Возможности управления рисками представляют собой широкий спектр, варьирующийся от периодического неформального применения техник риска к конкретным проектам посредством штатных формальных процессов до культуры понимания рисков с превентивным управлением неопределенности. Учитывая это, основные сферы/предметы дифференцированы с использованием четырехточечной шкалы, разработанной с учетом того, что каждый уровень зрелости является определенной позицией в иерархии достижений, который определяет достижение определенных возможностей управления рисками. Эта иерархия основана на различных этапах прогрессивно зрелого поведения организации. Было определено, что наличие большего количества уровней повысит степень неопределенности и непонимания без достаточной дополнительной обработки в помощь пригодности и четкой структуры в отношении конкретной ситуации в НПО. В определении уровня зрелости целевого риска организации необходимо рассматривать модель в перспективе: там, где на предыдущем уровне достигается достаточная квалификация, она допускается и для следующего уровня. Границы определяются концами непрерывного множества между состоянием незрелости и зрелости организации. Многомерная сетка разработана масштабируемой, гибкой и адаптируемой для учета изменений в размерах организации, структурном или регулятивном контексте. Представляет собой живую карту, при необходимости обновляемую и интегрируемую, для отражения новых входных данных, стандартов, режимов управления и так далее.

На **УРОВНЕ 1**:

- Отсутствуют процессы управления рисками. Организация не ощущает необходимости в управлении рисками и не использует структурированные подходы для этих целей: не ведет деятельность по предварительному планированию, но реагирует на ситуации и вопросы риска после их появления без каких-либо предупреждающих соображений.
- Организация не способна разграничить положительный и отрицательный риск.
- Процессы управления повторяются, попытки извлечь урок из прошлого и подготовиться к будущим угрозам не предпринимаются.
- Может существовать уверенность в том, что наиболее важные риски известны.
- Воздействие рисковых событий может быть определено, но не связано с целями, а рисковые события не связаны с источниками их процессов.
- Попыток разработки планов ликвидации последствий не предпринимается.
- Отсутствует культура контроля, но наличествует культура сопротивления изменениям. Подчеркиваются защитные физические и финансовые активы.

Для перехода от Уровня 1 к Уровню 2 организации нужно признать ценность управления рисками и ознакомиться с его потенциальными выгодами. С этой целью деструктивные события или внешние факторы, такие как влияние заинтересованных сторон, давление правительства и т.д. могут запустить в большей степени превентивный подход к рискам и осведомленность о том, что необходимо задействовать некоторые формы структурированной системы для работы с неопределенностью.

На **УРОВНЕ 2**:

- Высшее руководство знает о необходимости управления неопределенностью и рисками и обеспечивает наличие необходимых для проведения улучшений ресурсов.
- Стратегия обработки рисков определена, политика управления рисками спланирована.

- Ключевые лица понимают необходимость оценки и управления рисками, понимают концепции и принципы рисков.
- Некоторые отдельные процессы определены, равно как и действия по ликвидации последствий рисков, которые, однако, выполняются нечасто.
- Управление рисками преимущественно сосредоточено на прошлых событиях.
- Корпоративная культура находится на невысоком уровне ответственности за управление рисками, при этом ответственные за процессы определены или представлены не четко.
- Культура работы с рисками осуществляется политикой, тем не менее, истолковывающейся как соблюдение.Внедряется пилотная программа подготовки, и ключевая группа лиц имеет навыки и знания в области управления рисками.
- Программы соответствия, управления качеством, совершенствования процессов и так далее все еще работают независимо и не имеют общей структуры, вызывая пересечение действий по оценке рисков и противоречия.
- Средства управления в основном сосредоточены в отделах и финансах.
- Отсутствует последовательное планирование и отслеживание активности. Качественная оценка риска не используется или используется неформально.

Если подвести итог, хотя организация и знает о потенциальных выгодах управления рисками, эффективных масштабных процессов его внедрения нет, и внедрение передовых наработок остается за заинтересованным отдельным руководителем. Существует весьма ограниченное подтверждение того, что управление рисками эффективно как минимум в наиболее значимых областях.

На **УРОВНЕ 3**:

- Определены организационные процессы, а ответственность за риск четко установлена и надлежащим образом сообщена всему персоналу.
- Определены полномочия, роли и компетенции, соответствующие ресурсы распределены.
- Существует договоренность о рамках рисков, имеется рабочее руководство.
- Старшие менеджеры берут на себя руководство в целях обеспечения разработки подходов и обработки рисков, а также их внедрения во всех ключевых и сопутствующих областях.
- События связаны с источниками их процессов.
- Подчеркивается разработка ряда планов превентивных действий для обработки событий, могущих повлиять на организацию и ее заинтересованные стороны, для лучшего реагирования на установленные вопросы, а также для учета мер, снижающих вероятность нежелательных событий и их последствий.
- Превентивному планированию уделяется больше внимания.
- Методы качественной оценки используются для определения более глубоких потребностей в использовании количественных методов, анализов, инструментов и моделей.

Эта фаза обеспечивает возможность повысить осведомленность большей части организации. Имеется четкое свидетельство того, что управление рисками эффективно во всех сопутствующих областях. К концу этой стадии культура управления рисками охватывает организацию, включая управление возможностями.

На **УРОВНЕ 4**:

- Управление рисками является ответственностью каждого, а система управления рисками исполняется на каждом уровне: она заключена во все процессы и стратегии организации и является формальной частью постановки и достижения целей.
- Ответственность внедрена во все процессы, поддерживающие функции, линии и места расположения как путь к достижению целей.
- Риск-ориентированный подход к достижению целей используется на всех уровнях.
- Терминология и классификация для сбора информации о рисках внедрены полностью.
- Информация о рисках и об активности собирается изо всех областей для определения зависимостей и частоты показателей основных причин, более того, активно используется для совершенствования всех организационных процессов.
- Меры по ликвидации последствий определены, имеется понимание метода количественной оценки эффективности.
- Ликвидация последствий рисков объединена с оценкой (проводится вместе с количественным анализом, инструментами и моделями, поддерживающими качественные методы) для контроля над эффективным использованием.
- Меры обеспечивают решительное управление положительными и отрицательными последствиями рисков и возможностями.
- Для определения очередности рисков и дальнейших действий используются стандартизованные критерии оценки влияния, вероятности и эффективности управления.
- Поддерживается участие передовых сотрудников и значимость вопросов или возможностей документальных рисков.
- Ответственные за процессы регулярно изучают и дают рекомендации по показателям риска, которые лучше всего измеряют риски в их областях.
- Результаты планирования внутренних неблагоприятных событий рассматриваются как стратегические возможности.
- Развитие карьеры и вознаграждение включают стимулы к эффективному управлению рисками.
- Организация измеряет эффективность управления неопределенностями и получения возможностей, вытекающих из рисков.
- Отклонения от планов или ожиданий измеряются в сравнении с целями.
- Четкий, конкретный и эффективный подход к мониторингу хода достижения целей управления рисками регулярно сообщается со сферами деятельности.

Уровень 4 рассматривается как фаза циклического непрерывного совершенствования, где цепи обратной связи системы управления рисками постоянно способствуют получению уроков из опыта для достижения совершенства. Экспертный уровень характеризуется особыми чертами: организационная приспособляемость и приверженность совершенствованию, управление рисками как неотделимая часть принятия решений и повседневных операций, управление рисками как цель всех соглашений об исполнении обязательств старшего руководства, допустимая степень риска постоянно укрепляется и поддерживается высшим руководством, лидеры рассматриваются как примеры для подражания, организация, выбранная образцом надлежащей практики другими организациями, хороший опыт нововведений, эффективные мероприятия по управлению рисков вместе со всеми партнерами.**Рисунок 5.** ***Выдержка из Многомерного анализа и сетки для чтения: зрелость управления рисками***

			МНОГОМЕРНЫЙ АНАЛИЗ И СЕТКА ДЛЯ ЧТЕНИЯ:

КЛЮЧИ СЧИТЫВАНИЯ	**СТАТЬИ / ОСНОВНЫЕ ОБЛАСТИ**	**ОПИСАНИЕ**	**ЗРЕЛОСТЬ УПРАВЛЕНИЯ РИСКАМИ**			
			Стадия (Уровень) 1	**Стадия (Уровень) 2**	**Стадия (Уровень) 3**	**Стадия (Уровень) 4**
			Свойства / Показатели эффективности	**Свойства / Показатели эффективности**	**Свойства / Показатели эффективности**	**Свойства / Показатели эффективности**
РАЗУМНОСТЬ РИСКА: СТРУКТУРА УПРАВЛЕНИЯ РИСКАМИ И ПРОЦЕССЫ	**Структура риска**	*Отношение к неопределенности (Философия риска)*	Не проактивный подход: организации реагируют на ситуации и вопросы риска после того, как они уже произошли и не могут различать положительные и отрицательные риски	Риск рассматривается в качестве статитческое явление вместо динамического. Подход к управлению рисками фокусируется, в основном, на прошлых событиях	Конъюнктурный подход: общее и согласованное определение риска существует и применяется по всей организации, однако подход к управлению рисками фокусируется на том, чтобы избежать непредвиденного крупного ущерба	Открытый и проактивный подход, учитывающий и угрозу, и возможность. Риск-ориентированный подход для достижения целей применяется на всех уровнях.
		Мандат	Совет не чувствует необходимости в управлении рисками	Наблюдение за внешним спросом (влияние законодательных или регулирующих органов, давление правительства, влияние заинтересованных сторон)	Со стороны административного или политического совета	Обширный мандат, как у административного, так и у политического советов
		Лидерство и обязательство по управлению	Руководство не выступает за создание системы управления рисками и не принимает роли лидера в ее	Некоторые инициативы по управлению рисками поддерживаются высшим руководством на несистематической основе по	Высшее руководство берет на себя инициативу по обеспечению создания и внедрения подходов по устранению рисков во всех основных и актуальных	Лидерство по управлению рисками внедрено на всех уровнях организации. Управление рисками – это обычная и

			создании	всей организации	областях	постоянная деятельность высшего руководства. Высшее руководство также обеспечивает контроль структуры управления рисками и принимает участие в деятельности и инициативах по управлению рисками
ЭКСПЕРТЫ ПО УРОВНЯМ НЕУВЕРЕННОСТИ: ЛЮДИ, РОЛИ, **СТРУКТУРЫ И ВЗАИМОСВЯЗЬ**	**Культура**	*Внутренняя культура управления рисками*	Основное внимание уделяется реагированию на кризисные ситуации, а подход является скорее реактивным, чем проактивным. Превалирует культура, устойчивая к изменениям с упором на защиту физических и финансовых активов	Люди обычно враждебны к рискам: используется подход, предусматривающий меры предосторожности в отношении всей системы управления рисками (избежание риска)	Распространяется культура управления и контроля рисков	Ожидания отдельных лиц и организации в отношении управления рисками синхронизированы. Внимание уделяется возможностям, а не только исключению рисков. Организация поощряет культуру постоянного обучения и участия, а технически прогрессивный персонал поощряется. Сотрудники активно придерживаются принципа успеха организации
			Отсутствуе	Организаци	Принципы/руко	Этика и

		Связь с этикой и ценностями	т политика или руководство по этическим нормам. Нет четких формулировок общих ценностей или принципов, а также внимания правовым вопросам	я может иметь формулировку этики, но философия отражает правовые и политические соображения (подход соответствия), а любые письменные политики применяются непоследовательно	водство по этике и ценностям и правовые/политические соображения поняты персоналом, а подход по управлению рисками связан с ними	ценности последовательно отражаются в деятельности и мероприятиях организации по управлению рисками. Регулярные обследования по данной теме учитывают риски. На всех уровнях организации создан климат взаимного доверия
ТЕХНОЛОГИИ: ПОДДЕРЖКА	**Информационная система управления рисками**	*Инструменты ИКТ*	Информационная система по управлению рисками не предусматривается	Особая пилотная информационная система по управлению рисками внедряется как часть других информационных систем	Комплексноепрограммное обеспечение может использоватьс я для поддержки руководства в отслеживании ключевых и соответствующих процессных областей	Каждая стадия процесса управления рисками отслеживается в веб-инструменте, тщательно интегрированном с другими корпоративными информационными системами
		Управление документами	Ведение документации, поддерживающее деятельность и процессы принятия решений, сфокусировано на физических	Система управления документами, в основном сфокусированная на прошлых событиях, может быть предусмотрена для: 1. соответстви	Организация определяет ресурсы касательно документальных информационных систем для поддержки руководства при регистрации ключевых и	Информация о рисках регистрируется последовательным и безопасным образом, создавая политики и процедуры для доступа,

			и финансовых активах. Организация не осуществляет документирование информации о рисках	я правовым, нормативным требованиям и требованиям по корпоративному управлению; 2. для регистрации информации со ссылкой на некоторые одиночные процессы, определенные и связанные мероприятия по смягчению последствий	соответствующих процессных областей	использования и передачи информации, как часть структурированного Плана управления информацией. Каждая стадия процесса управления рисками регистрируется соответствующим образом.

Вопросы и ответы

Вопрос. Со ссылкой на фазу измерения риска, использует ли ваша организация различные методики в отношении классификации риска (ИТ, финансовые, соответствие и т.д.)?

Ответ 1. «Да. Методики значительно меняются в зависимости от вида риска и **зрелости риска** сферы деятельности. Часто корпоративные области имеют более **зрелые риски**, обычно с связи с наличием многолетней ответственности для поддержания организации в процессе управления особым видом риска».

Источник: Австрия, *Подробный обзор практики управления рисками*

Вопрос. Комментарии или наблюдения:

Ответ 1. «Система управления рисками все еще разрабатывается, и мы ожидаем переход к **модели зрелости,** как только система будет доработана».

Источник: Ирландия, *Подробный обзор практики управления рисками*

Вопрос. Оценивался ли уровень информированности персонала о рисках и (или) управлении рисками во время осуществления процесса управления рисками в вашей организации?

Ответ 1. «Да, на начальной фазе. Обследование при участии руководства было проведено для оценки и измерения восприятия

риска и **зрелости** внутренних (в пределах отдельных организационных подразделений) и внешних (среди подразделений в пределах организации) систем контроля.

Источник: Италия, *Обзор практики управления рисками*

Ответ 2. «Обзор **зрелости риска** и ее понимание являются частью проекта рамок управления рисками, но они еще не разработаны».

Источник: Новая Зеландия, *Обзор практики управления рисками*

Вопрос. В вашей организации процесс управления рисками связан с:

Ответ 1. «Оценкой достижений и организации, и индивидуумов. Управление рисками – это цель во всех трудовых договорах с высшим руководством – Имеются соображения по установлению такой ответственности всем сотрудникам организации. Организация имеет политику в отношении рисков и руководство, в котором указывается процедуры, которым ежедневно придерживается вся организация. Уровень **зрелости риска** – это критерий, в сравнении с которым мы регистрируем наш прогресс, а также управленческую информацию, представленную в ежемесячном Исполнительном отчете Директорам».

Вопрос. В вашей организации информация, полученная от процесса управления рисками, используется для: Понимания причин низкой эффективности (организации и (или) индивидуума) и анализа процессов изменений:

Ответ 1. «В некоторой степени согласны. Это делается, но организация разрабатывает свои показатели **зрелости риска** и еще не совсем внедрила их, но группа по управлению рисками планирует обеспечить продолжение повышения их **зрелости** в течение следующих 12 месяцев».

Вопрос. На какой фазе развития в вашей организации находится процесс управления рисками в настоящий момент?

Ответ 1. «Некоторые области являются очень **зрелыми**, другие имеют возможность усовершенствования, хотя, в целом, это очень хороший стандарт».

Вопрос. Какие сильные стороны системы управления рисками в вашей организации?

Ответ 1. «Внедрение целей риска и переоценка готовности к принятию риска. Новая база данных по рискам и новая политика в отношении рисков помогают повышать **зрелость** и грамотность в области рисков».

Источник: Великобритания, *Обзор практики управления рисками*

[1] *Модель зрелости риска (МЗР)* от Хиллсона (1997 г.); Правительственный центр для информационной системы (1993 г.); Модель зрелости риска Хопкинсона для предприятий (2000 г.); *Инструмент для диагностики управления зрелостью риска* от Базиля Орсини (2002 г.); *Модель зрелости управления рисками (МЗУР)* от компании PMI Risk Significant

Interest Group - RiskSIG (2002 г.); *Модель зрелости управления предпринимательскими рисками (МПР)* от IACCM (Международная ассоциация по контрактному и коммерческому менеджменту) Рабочая группа по управлению предпринимательскими рисками (2002 г.); *Модель зрелости возможностей (МЗВ)* от Института по разработке программного обеспечения (SEI) (2002 г.); *Модель зрелости риска для Управления рисками предприятия* от Общества по вопросам управления риском и страхования (RIMS) и Логического менеджера (2008 г.); *Шкала уровня эффективности работы* от Министерства финансов Великобритании (2009 г.); *Национальная модель показателей деятельности для управления рисками в государственных службах* от организации «Alarm», Ассоциации по управлению рисками для населения – Великобритания (2010 г.); *Модель зрелости управления рисками* от Института внутреннего аудита (2010 г.); Модель зрелости управления операционными рисками (МЗУОР) от МакКонелла (2012 г.); *Модель зрелости управления рисками Комковера* от Правительства Австралии (2013 г.); МЗУР от Инвесторов при управлении рисками (IIRM) (2015 г.).

[2] Используя программу по признанию достижений сотрудника, организация может стимулировать своих заинтересованных сторон к постоянному повышению устойчивости и совершенствованию деятельности.

[3] Уитли (2007).

[4] *Шаблон,* используемый на *Семинаре Комитета Модернизации по организационной структуре и оценке*, проведенного в Женеве с 14 по 17 октября 2014 года, учитывает наиболее часто используемые и хорошо известные международные стандарты, такие как Концептуальная модель управления рисками предприятия (ERM): Внутренний контроль-общий контроль, разработанная Комитетом спонсорских организаций (Co.S.O.), а также ИСО 31000:2009 (Управление рисками – Принципы и основополагающие принципы).

).

9. Полученные уроки

8. Модель зрелости управления риском	РАЗДЕЛ 2: Процесс управления рисками

ТЕГИ: Что было самым успешным, что было особенно трудным, что не делать при внедрении Системы управления рисками в НСБ.

9.1 Сильные и слабые стороны при внедрении Системы управления рисками в НСБ

9. Полученные уроки	9.2 Кластер 1: Передача мандата по управлению рисками и политика в отношении рисков

Для подтверждения, а также обоснования Руководства было спланировано завершающее обследование для получения полной картины путей внедрения Систем управления рисками в статистических организациях.

Данное Обследование состоит из шести различных вопросников, направленных на шесть организационных сфер (*Управление рисками; Анализ статистического качества; Управление процессом статистического производства; Управление организационным процессом; Внутренний контроль и (или) внутренняя проверка; Службы, поддерживающие статистическое производство*). Выборка проводилась среди организаций, представляющих различные уровни *Зрелости риска.* Таким образом, подход был достаточно всеобъемлющим для получения разнообразных мнений и, таким образом, для помощи выявления элементов, которые максимально характерны для различных контекстов, подвергнутых анализу. Целевой раздел обследования, состоящий

не более чем из 6 (шести) вопросов, был предусмотрен для каждой области целевой аудитории.

Каждый вопросник сфокусирован на четырех основных предметных областях:

1. Структура управления рисками

2. процесс управления рисками

3. Всеохватывающие процессы

4. зрелость риска организации

Для каждой предметной области были определены несколько тем/вопросов, чтобы помочь респондентам описать их собственный опыт и высказать свои мнения и размышления.

Каждая ТЕМА рассматривается с открытыми вопросами, нацеленными на вышеуказанную аудиторию и обращающими особое внимание на:

Ø «ЧТО БЫЛО САМЫМ УСПЕШНЫМ»: Что было самым лучшим действием для организации от внедрения системы управления рисками;

Ø «ЧТО БЫЛО ОСОБЕННО ТРУДНЫМ»: Что было главными подводными камнями при разработке системы управления рисками;

Ø «ЧЕГО ДЕЛАТЬ НЕ СЛЕДУЕТ»: Согласно опыту, полученному НСБ, участвующими в Обследовании, ошибки, которые лучше не повторять при внедрении системы управления рисками.

Далее представлена выборка актуальных тем по «самым успешным», «особенно трудным» примерам и примерам того, «чего делать не следует» на основе третьего обследования, которая оказалась самой общедоступной (более всеобъемлющая и подробная выборка представлена в таблицах, предлагаемых в конце каждого раздела). Такие темы также были выбраны за их неотъемлемую последовательность, а также согласованность с Руководством по управлению рисками, на основе доказательств, связанных с практиками управления рисками, управления качеством и внутренней проверки среди НСБ.

Для этой цели результаты Обследования были сгруппированы по 5 кластерам, отслеживаемым по 4 предметным областям, указанным выше:

- Кластер 1: Мандат по управлению рисками и Политика в отношении рисков;

- Кластер 2: Процедура управления рисками и роль Отдела по управлению риском;

- Кластер 3: Интеграция управления рисками с другими функциями;

- Кластер 4: Процесс управления рисками;

- Кластер 5: Вспомогательный процесс по управлению рисками

В следующих пунктах проводится анализ ответов по каждому объекту обследования, которые были сгруппированы в следующие 5 схожих кластеров для упрощения процесса анализа:

Ø Кластер 1 – МАНДАТ И ПОЛИТИКА В ОТНОШЕНИИ РИСКОВ. Вопросы: *Мандат и обязательства по управлению рисками; Определение Политики в отношении рисков*

Ø Кластер 2 – ПРОЦЕДУРА УПРАВЛЕНИЯ РИСКАМИ И ОРГАНИЗАЦИОННАЯ СТРУКТУРА. Вопросы: *Процедура управления рисками; Создание Группы/отдела управления рисками*

Ø Кластер 3 – ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ. Вопросы: *Этап идентификации риска; Этап оценки риска; Этап обработки риска*

Ø Кластер 4 – ИНТЕГРАЦИЯ УПРАВЛЕНИЯ РИСКАМИ. Вопросы: *Интеграция управления рисками с другими организационными функциями; Интеграция управления*

рисками с управлением качеством; Интеграция управления рисками с внутренним контролем/внутренней проверкой;

Ø Кластер 5 – УПРАВЛЕНИЕ РИСКАМИ: ВСПОМОГАТЕЛЬНЫЕ УСЛУГИ. Вопросы: *Обучение; Система ИКТ, поддерживающая процесс управления рисками; Коммуникации и консультации*.

В пунктах 9.2 - 9.6 перечислены Кластеры и соответствующие вопросы посредством анализа самых репрезентативных ответов согласно структуре вопросника (что было самым успешным, что было особенно трудным, чего делать не следует).

В Сводной таблице в Приложении на 45-56 страницах представлены более подробные ответы.

И, наконец, в пункте 9.6 проводится анализ интеграции управления рисками в текущую деятельность среди НСБ, принимающих участие в третьем обследовании.

9.2 Кластер 1: Передача мандата по управлению рисками и политика в отношении рисков

	9.1 Сильные и слабые стороны при внедрении Системы управления рисками в НСБ	9. Полученные уроки	9.3 Кластер 2: Процедура управления рисками и роль отдела по управлению рисками	

Успешная процедура:

До начала внедрения системы по управлению рисками необходим четкий мандат, демонстрирующий область применения системы, цели и пределы, а также помещающий общую подотчетность на уровень совета (т.е. на Комитет по управлению рисками), и, последнее, но не менее важное, размещающий все необходимые вспомогательные ресурсы, такие как человеческие и финансовые.

Политика в отношении рисков непосредственно вытекает из мандата и ее успех предполагает, что руководители высшего и старшего уровней вовлечены в ее определении. Задачей политики в отношении рисков является постепенная интеграция управления рисками, как в статистическое производство и вспомогательные процессы, так и в статистическую деятельность. Такая интеграция может быть достигнута посредством:

- Подтверждения политики по отношению к рискам Советом и ее распространение среди персонала;

- Определения готовности к принятию риска и склонности к риску, устанавливаемых Советом, а также, на операционном уровне, их постепенное включение в ожидаемые результаты, пока не будут получены измеряемые показатели риска;

- Интеграции между системой управления рисками и стратегическим и операционным планированием;

- Назначения конкретных целей управления рисками для Высшего руководства, целей, учитываемых при оценке из работы;

- Привлечения людей, ответственных за … (стратегические направления, портфели проектов, проекты и направления деятельности) к идентификации рисков и их оценке, а также к планированию обработки рисков;

- Уравновешивания рабочей нагрузки и ресурсов, назначаемых для управления рисками в соответствии с определенной готовностью к принятию риска;

- Создания информационной системы по управлению рисками, интегрированной с остальными системами управления, для обоснования рабочей нагрузки на среднее руководство, укрепляя, таким образом, сотрудничество.

Сложная процедура:

Некоторые существенные трудности в данной Области касаются воздействия так называемых социальных навыков[1] на успех Системы.

Более того, необходимо пройти сквозь недоверие, смешанное с ложным доверием, с которым сталкиваются владельцы рисков, следуя одним и тем же рутинным операциям в отношении риск-ориентированного подхода. Неслучайно то, что намного проще фокусироваться на рисках, недоступных вам самим, поскольку в обратном случае будут требоваться прочно установившиеся рутинные процедуры, а затем и свой собственный способ управления процессами.

Другая проблема заключается в поддержании фокусирования Высшего руководства на цели по управлению рисками не только потому, что такие цели не представлены для измерения эффективности, но и также по указанным выше причинам, а именно потому, что даже руководители часто считают риски, в основном, исходят от процессов, вне их доступа.

Среди трудностей также можно найти определение готовности к принятию риска и склонности к риску, а также четкому взаимопониманию, также учитывая, что «слабая готовность к риску, в то время, как необходимо защищать целостность оценочных показателей, может подавлять внедрение технических новшеств».

Чего делать не стоит:

Некоторыми основными ошибками, которых следует избегать при внедрении системы управления рисками, являются:

а) Навязывание изменений Высшим руководством вместо осуществления руководства такими изменениями, т.е. вместо обмена данными о предполагаемых преимуществах с внешними заинтересованными сторонами, а также со всеми задействованными сотрудниками для того, чтобы учитывать все их предложения;

Начало внедрения системы управления рисками как без нормативной базы, четко устанавливающей подотчетность, так и без надежной стратегии в соответствии с приоритетами учреждения, и, в то же время, гарантируя отсутствие ограничений ответственности одного отдела или индивидуума в отношении разработки системы управления рисками.

[1] Социальные навыки – это сочетание навыков межличностного общения, навыков общения, способностей к коммуникации, личностные качества, жизненная позиция, профессиональные качества и коэффициент эмоционального интеллекта (ЭИ). Все эти качества не зависят от приобретенных технических знаний.

9.3 Кластер 2: Процедура управления рисками и роль отдела по управлению рисками

⇦	9.2 Кластер 1: Передача мандата по управлению рисками и политика в отношении рисков	⇧9. Полученные уроки	9.3 Кластер 3: Интеграция функции управления рисками с другими функциями ⇨

Успешная процедура

Процедура управления риском является успешной тогда, когда она инклюзивна, т.е., когда она подразумевает сотрудничество между группой/отделом управления рисками и остальными задействованными сотрудниками, среди которых владельцы риска играют важную роль. Более того, такая процедура должна четко выявлять и раскрывать различные функции и ответственность, предполагая также надлежащую эскалацию рисков[1], а также определение ответственности за обработку в случае воздействия риска на различные процессы (сквозные риски), и недопущение дублирования ролей/функций в пределах процесса управления риском. Сотрудничество со службами внутренней проверки и управления качеством – это подходящий ключ к успеху, поскольку они вносят значительный вклад в весь процесс (См. ниже Область 3 - Интеграция).

Качество процедуры управления риском может измеряться через отслеживание процесса (определение этапов, результатов, документов) и, прежде всего, через ее гибкость, определенную как способность к адаптации к организационному контексту и соответствующим изменениям. Фактически, если процедура слишком строгая, она может перекрыть деятельность организации, снижая, таким образом, ее потенциал.

Другой задачей для процедуры управления риском является определение роли группы/отдела управления риском согласно задачам и целям, составленным в соответствии с пределами компетенции и политикой в области рисков. Группа/отдел должна официально входить в организацию, а также с официальными полномочиями действовать независимо и получать соответствующую поддержку (с точки зрения человеческих и финансовых ресурсов). Создание централизованного отдела через сеть контактных лиц для поддержания координации кажется лучшим выбором. Группа/отдел управления рисками предлагает поддержку и консультации по управлению рисками владельцам рисков, осуществляющим деятельность по управлению рисками, будучи непосредственно ответственными за них.

Значение осуществления централизованной координации также связано с необходимостью наблюдения за сквозными рисками, оказывающими воздействие на различные проекты или процессы, хотя такой координации и сложно достичь.

Сложная процедура

Основной проблемой, связанной с процедурой управления рисками, является гибкость, т.е. способность к адаптации к организационному контексту, поскольку это непростая задача сбалансировать рекомендованные шаги и позволить людям адаптироваться к обстоятельствам.

Другая проблема заключается в принятии решения, какой этап процесса управления риском является правильным для согласования мнений высшего руководства и руководства по осуществлению программ, а также интеграции нисходящих и восходящих подходов. С одной стороны, топ-менеджеры объединяют восходящие риски и определяют приоритеты обработки. С другой стороны, руководители программ располагают мерами по обработке каскадом через детальное и целесообразное планирование.

Чего делать не стоит

При составлении проекта процедуры не рекомендуется:

а) Отказывать в консультировании потребителей по всей организации о том, какие выгоды дает процедура и не иметь четкого графика осуществления;

б) Завершать подготовку отдельных шаблонов, не связанных с другими документами (т.е., оперативное, финансовое планирование и планирование управления качеством);

в) Уделять чрезмерное внимание документам по управлению рисками, забывая о значении объединения подхода по управлению риском с выполнением программы ежедневной работы.

При создании отдела/функции по управлению рисками не рекомендуется:

а) Назначать ресурсы группе/отделу по управлению риском, которые являются недостаточными по качеству и (или) количеству на основании целей группы/отдела;

б) Дублировать группы/отделы, оказывающие поддержку владельцам риска и контролирующие процесс управления рисками;

Помещать группы/отделы управления рисками на второстепенные места в организационной структуре.

[1] Эскалация риска – это процесс отвода обработки рисков назад от низшего уровня ответственности к более высокому (т.е. от проекта к программе к портфолио)

9.3 Кластер 3: Интеграция функции управления рисками с другими функциями

9.3 Кластер 2: Процедура управления рисками и роль отдела по управлению рисками	9. Полученные уроки	9.4 Кластер 4: Процесс управления риском	

I) С другими организационными функциями

Интеграция функции управления рисками с остальными функциями и организационными сферами – это основной принцип реального внедрения системы в производственные процессы, и, таким образом, более эффективное ее функционирование. Более того, при использовании отдельных систем управления в разных сферах организации очень сложно представлять отчеты на корпоративном уровне. Такая интеграция происходит и на уровне области риска (т.е. стратегический риск, трансформационный риск, статистический риск, проектный риск, риск потерь от мошенничества), и на функциональном уровне (управление качеством, внутренняя проверка, двойной опцион, ИКТ, здравоохранение и безопасность и т.д.).

Однако эффективная интеграция Системы управления рисками подразумевает компромисс, т.е. отказ от создания лучшей системы управления рисками во время ее адаптации, в качестве альтернативы, к фактической организационной структуре, функциям, процессам и возможностям. Другим словами, именно Система должна адаптироваться к требованиям организации, а не наоборот.

II) С функциями внутренней проверки

Для того чтобы быть более эффективным, а также лучше всего демонстрировать свои возможности, управление рисками должно быть объединено с внутренней проверкой, при наличии такой возможности. Однако для этого необходимо четко прописать функции управления рисками и внутренней проверки во всей структуре, а также роли, ответственность и подотчетность. Одной из сильных сторон интеграции является циклическая гибридизация двух функций и соответствующих подходов, например, использование риск-ориентированного подхода в соответствии с рекомендациями после проведенной проверки для определения приоритетов обработки и одновременного обеспечения рассмотрения результатов мониторинга процесса обработки рисков службой внутренней проверки. Кроме того, при подготовке рекомендаций аудиторских проверок крайне важно периодически полагаться на оценку риска.

Что касается проблем, актуальной проблемой является поддержание пристального внимания руководителей к обеспечению внутренней проверки в отношении эффективности системы управления рисками.

III) С функциями управления качеством

Управление рисками должно быть объединено с управлением качеством по следующим причинам:

- эффективность обработки статистических рисков выше, если процессом руководит команда экспертов по качеству, поскольку выявленные ими слабые стороны статистических обследований во время анализа качества могут привести к обнаружению потенциальных рисков в пределах статистических процессов, а затем и к планированию мер по усовершенствованию;

- рекомендации Сектора качества по лучшей организации и приоритизации работы внутренних аудиторов, а затем и помощь по повышению общего качества статистики;

- интеграция между двумя системами предложена в стандарте ИСО 9001:2015, где риск-ориентированный подход рассматривается в качестве вспомогательного инструмента для повышения качества;

- определение готовности к принятию риска и склонности к риску зависит, помимо всего прочего, от вида статистических результатов.

Тем не менее, внедрение процесса надзора за руководящими принципами в отношении качества в процесс управления качеством не всегда является легким методом, поскольку зависит от способности склонить производственные области к тому, что разработка границ качества[1] в виде компонента системы качества не будет затруднительной и повысит эффективность текущих процессов качества.

Чего делать не стоит:

а) Попытки контролировать выполнение руководств по качеству на чересчур подробной основе, поскольку контроль качества должен осуществляться в целом, а не по отдельному продукту или процессу;

б) Неудача при внедрении Системы управления рисками или ее интеграции с системой управления качеством, а также осуществление такой процедуры без четкого понимания того, как делать нужно, или без разумного понимания и знания требований к обеим системам или требований соответствующих стандартов и их применения, а также, наконец, без назначения координатора с установлением четких обязанностей для процедуры.

в) Закрепление ответственности по управлению рисками и качеством за одним отделом или сотрудником.

[1] В соответствии с австралийским Статистическим бюро, границы качества являются стратегией смягчения последствий риска, созданной для совершенствования процесса раннего выявления ошибок или дефектов в процессах статистического производства.

9.4 Кластер 4: Процесс управления риском

9.3 Кластер 3: Интеграция функции управления рисками с другими функциями	9. Полученные уроки	9.5 Кластер 5: Вспомогательные процессы по управлению рисками	

Идентификация риска

Один из лучших способов успешной идентификации риска заключается в вовлечении всех владельцев риска, а также внутренних и внешних заинтересованных сторон, в первую очередь, из числа Высшего руководства, к участию в семинарах на регулярной основе. Задачей семинаров является определение основных тематических рамок и рисков в таких рамках. SWOT-анализ может стать надежным инструментом для изучения внутренней и внешней обстановки в НСБ, а затем и облегчения мозговой атаки, поскольку он помогает определить сильные и слабые стороны организации, а также любые возможные угрозы и возможности.

На стадии идентификации, роль качества группы по управлению крайне важна, поскольку на основе периодических проверок качества статистической продукции можно определить основные статистические риски. Фактически, риск-ориентированный подход, примененный к статистическому качеству, предполагает целостный подход, т.е. подход, вовлекающий все процессы, а не только производственные, а также мнение всех внутренних и внешних заинтересованных сторон. Таким образом, все люди, ответственные за все процессы, производственные и вспомогательные, должны посещать семинары.

Какие бы риски не были выявлены, процедура идентификации должна быть определена и сохранена на некоторое время для того, чтобы позволить участникам адаптировать и полностью применить все возможности от знания процесса управления риском.

Что касается методов идентификации, которые могут быть довольно сложными, будет лучше использовать предложения с «если…, то…», а также обеспечивать изучение источников рисковых событий за пределами организации. Методология определения риска должна быть объяснена всем участникам заблаговременно сотрудниками, которые должны быть экспертами и иметь навыки по управлению рисками.

Процесс управления риском должен быть связан со стратегическим, секторальным и оперативным планированием, а значит, ключевые/приоритетные риски должны быть связаны с краткосрочными и долгосрочными стратегическими целями организации. Будет лучше не определять слишком много стратегических рисков, они могут быть менее контролируемы. Операционные риски, в свою очередь, должны быть связаны со стратегическими.

Классификация рисков, несомненно, полезна, также как и объединение рисков в кластеры, которые достаточно малы для проведения их анализа, и использование структуры, которая учитывает регулярные циклические риски и долгосрочную программу преобразования рисков в качестве отдельных, но связанных групп.

Основные проблемы на стадии идентификации рисков касаются:

- Выбора методики идентификации и извещение персонала о ней;

- Признания взаимосвязи между рисками для того, чтобы прогнозировать ситуацию при их управлении, особенно тогда, когда они пересекают более одной сферы деятельности;

- Визуализации потенциальных рисков, а также рисков, которые еще не наступили.

Чего делать не стоит:

- Путать риски с критическими уровнями;

- Либо определять слишком много рисков, либо путать риски, недоступные для организации, с рисками в действительности поддающимися управлению.

Чем выше зрелость риска организации, тем более осуществимым будет ожидаемое поведение в отношении готовности к принятию риска для изменения культуры организации: фактически, если культура менее зрелая, риски рассматриваются лишь в качестве угроз, вместо возможностей.

Оценка риска

Для успешного проведения этапа оценки риска, данный процесс должен проходить под руководством группы по управлению рисками и при поддержке специальных инструментов. Ее методология должна быть заблаговременно распространена и правильно понята. Даже процесс оценки риска, а также критерии измерения риска должны быть адаптированы к организационному контексту, распространены и стандартизированы.

Матрица рисков в качестве техники оценки имеет преимущество, позволяющее проводить интуитивную оценку рисков, а также более простой анализ рисков.

Оценка рисков должна проводиться группой специалистов из разных отделов, особенно в случае применения метода оценки качества, для того, чтобы оценка не подвергалась чрезмерному влиянию отдельного лица или компетенции. Оценке должна предшествовать мозговая атака, задачей которой является обеспечение того, что все поняли два главных критерия измерения риска – воздействие и вероятность. Регулярный анализ оценки риска, т.е. не только одновременно с обновлением регистров рисков (посредством измерения и остаточного, и неотъемлемого риска) для поддержания их актуальности, является чрезвычайно важным.

Качественная оценка может быть объединена с количественной, при условии, что обновленную информацию можно будет легко найти. В некоторых случаях сбор данных может требовать крайне больших затрат.

Результаты оценки риска (перечень рисков и соответствующих результатов измерения) должны быть сообщены внутренним и внешним заинтересованным сторонам, а затем анализироваться в соответствии с их наблюдениями. В некоторых случаях будет полезно проанализировать воздействие от наступления риска также по определенным категориям заинтересованных сторон (пользователи, персонал, поставщики данных и т.д.). Такая оценка очень помогает последующей оценке эффективности действий по обработке рисков.

Для сопоставления восходящего и нисходящего подходов, крайне важно делиться данными, по крайней мере, об оценке риска при поддержке от группы по управлению риском – на уровне Совета старших руководителей.

Несмотря на сложность, полезно измерять воздействие от наступления риска, как на корпоративном уровне, так и на уровне отдела, согласно взаимосвязи рисков, если такая взаимосвязь определена заблаговременно.

Далее указаны некоторые ошибки, которых нужно избегать (**чего делать не стоит**):

- Преувеличение рисков, а также недостаточное или чрезмерное их освещение с целью скрыть или искусственно сделать акцент на определенных рисках;

- Определение приоритетов рисков только в соответствии с их верхними значениями (вероятность наступления);

Использование комплексных инструментов оценки, сложных для понимания менее квалифицированными сотрудниками в области управления рисками.

Обработка риска

Ответственность за планирование и осуществление обработки ключевых рисков должна быть делегирована высшему руководству. При этом они опираются на свои собственные отделы, как на производственный, так и на технический. Любая обработка должна соответствовать целям, индикаторам, крайним срокам, уровням рискоустойчивости, а также осуществление обработки должно контролироваться и, при необходимости, адаптироваться к различным обстоятельствам после тщательной переоценки рисков.

Эффективность обработки достигается через сопоставление различных действий, как превентивных, так и последующих, на разных стадиях процесса статистического производства.

Осуществимость по каждой обработке должна измеряться посредством анализа затрат и результатов, предпочитая такие мероприятия по обработке, которые легко могут быть включены в производственные процессы. Для этой цели важно согласовать оперативное планирование обработки с финансовым планированием.

Одна из важных проблем касается сложности назначения ресурсов для плана обработки, которая имеет межсекторальные последствия для обеспечения интегрированного организационного реагирования, а также определения обязанностей и обязательств для обработки рисков в тех случаях, когда риск относится более чем к одному процессу или ко всей организации в целом.

Далее указаны некоторые ошибки, которых нужно избегать (**чего делать не стоит**):

- Оставлять команду по управлению качеством в стороне от планирования процесса обработки;

- Неспособность провести анализ затрат и результатов;

Неспособность контролировать прогресс мероприятий по обработке.

9.5 Кластер 5: Вспомогательные процессы по управлению рисками

9.4 Кластер 4: Процесс управления риском	9. Полученные уроки	9.6 Интеграция процесса управления рисками в текущую деятельность

Обучение, информационное взаимодействие и ИКТ системы доказали, что являются соответствующими стратегическими функциями, поддерживающими внедрение системы управления рисками.

Что касается **обучения**, необходимо включать информацию по управлению рисками, как часть ознакомительной программы обучения человеческих ресурсов. Лучше всего, если

такое обучение будет повторяться, по крайней мере, раз в год – тогда такое обучение реально будет работать.

Проведение обучения может осуществляться, как посредством семинаров, так и посредством электронного обучения, в соответствии с потребностями целевого персонала, а также посредством организации курсов. Обучение методам управления рисками требует планирования специального бюджета. Лучше всего, если это будет жесткий бюджет.

Чего делать не следует: проведение общего обучения для всего персонала и (или) проведение обучения методам управления рисками время от времени, поскольку оба способа неэффективны.

Что касается **ИКТ систем**, большинство НСБ согласны с их значимостью для поддержания процесса внедрения систем управления рисками.

В случаях, когда уровень зрелости риска высок, необходимо разработать программное обеспечение для управления рисками Предприятия. Такое ПО должно быть объединено с другими системами управления информацией, а также согласовано со Стандартами управления рисками и с охватом всех этапов процесса. Такой выбор влечет за собой преимущество для лучшего управления межсекторальными рисками, а также для всей организации в целом.

НСБ, которые все еще внедряют систему управления рисками, предпочитают использовать простой инструмент, не требующий применения комплексных компьютерных знаний, т.е. применения таких программ, как Microsoft Excel, а также охватывающий все стадии процесса управления рисками.

Какое бы ПО не было выбрано, оно, скорее, будет иметь интуитивно-понятную структуру для обеспечения распространения и хорошие пользовательские характеристики для всех сотрудников.

Одной из главных проблем является попытка интегрировать систему управления рисками с остальными системами управления, применяемыми организацией (управление проектами, управление качеством, инструмент планирования и контроля и т.д.).

Чего делать не следует: полагать, что информационная система, независимо от того, как она была разработана, сможет заменить планирование, анализ и управление процессами.

Информационное взаимодействие и консультирование персонала должны осуществляться на разных уровнях и посредством совместных усилий всех сторон, вовлеченных в процессы внедрения системы управления рисками. Функции управления рисками, управления качеством и внутренней проверки будут играть важную роль при осуществлении таких усилий.

Участие Высшего и старшего руководства упрощается посредством проведения регулярных семинаров, связывающих темы управления рисками с темами, касающимися повышения эффективности. На среднем управленческом уровне важно обеспечить взаимодействие областей управления рисками, управления качеством и внутренней проверки, используя свои собственные технологии для каждой области, с деятельностью, направленной на оповещение всего руководства о преимуществах от внедрения системы управления рисками. Руководители, в свою очередь, будут распространять культуру риска и риск-ориентированный подход для управления процессами среди всего персонала.

Информационное взаимодействие поддерживает процесс постепенного внедрения системы через различные каналы (электронное обучение, семинары, инструменты внутренней связи, форумы, конференции) в соответствии с целью, что также подразумевает предоставление отчетов по исполнительным и (или) операционным моментам.

Одной из главных проблем является установление баланса между необходимостью привлекать и необходимостью информировать, избегая, таким образом, любого излишка информации, который может нагружать повседневное управление процессом в долгосрочной перспективе.

Чего делать не следует: ограничение информационного взаимодействия и консультирования персонала до лишь нескольких категорий персонала, поскольку долгосрочная задача требует вовлечение всего персонала.

9.6 Интеграция процесса управления рисками в текущую деятельность

9.5 Кластер 5: Вспомогательные процессы по управлению рисками	9. Полученные уроки

При закрытии Третьего обследования респондентов попросили предоставить информацию для того, чтобы понять фактический уровень интеграции процесса управления рисками в их собственной организации. Ответы были проанализированы и сравнены с некоторыми утверждениями в Комплексной сетке зрелости риска, которая описана в Главе 8 Руководства.

В частности, ответы сравнивались со следующими пунктами и *дескрипторами* из Комплексной сетки зрелости риска:

- Рамки риска (*Мандат, Стратегия и политика в области рисков, Подход к управлению рисками, Лидерство и обязательство по управлению*)
- Оценка риска (*Идентификация риска*)
- Средства контроля (*Контроль и проверка, основанная на оценке рисков*)
- Политика распространения рисков (*Результаты и представляемая документация, Преимущества для организации в целом*)
- Интеграция системы управления рисками (*Связь с корпоративным и оперативным планированием, интеграция системы управления рисками, Интеграция с рамками качества*)
- Функции и подотчетность при управлении рисками (*Функции и ответственность высшего руководства, ответственность сотрудников*)
- Человеческие ресурсы (*Компетентность человеческих ресурсов*)
- Информационная система по управлению рисками (*Инструменты ИКТ, Управление документами*)

Например, согласно полученным ответам были проанализированы следующие ключевые характеристики:

1) Согласованы ли процессы управления рисками и управления качеством между собой или полностью интегрированы;

2) Является ли управление рисками неотъемлемой частью стратегического и бизнес-планирования, как на корпоративном уровне, так и уровне осуществления деятельности;

3) Имеется ли доказательство того, что управление рисками обеспечивает достижение ключевых результатов во всех соответствующих и ключевых областях;

4) Берут ли топ-менеджеры на себя инициативу за обеспечение разработки и применения походов по урегулированию рисков во всех ключевых и соответствующих областях;

5) Постоянно ли учитывается распределение подходящих человеческих ресурсов для управления рисками при планировании бюджета и укомплектовании персоналом;

6) Указаны ли обязанности по управлению рисками официально в соглашениях об ответственности и (или) документах о корпоративном управлении, а также сообщаются, применяются и отслеживаются на всех уровнях;

7) Проводится ли независимый мониторинг планов обзора и контроля для определения достигнутого прогресса и результатов;

8) Отслеживается ли каждая стадия процесса управления риска тщательным образом с помощью сетевого инструмента, объединенного с другими корпоративными информационными системами.

Согласно этим характеристикам практической деятельности НСБ назначены Стадии зрелости рисков от 1 до 4.

В следующей таблице 5 представлена практическая деятельность в соответствии со стадией зрелости рисков, а также «возрастом» систем управления рисками (время, потраченное на их внедрение – такая информация поступает от первого обследования по методам управления рисками, проведенного в мае 2015 г.). В Таблице сообщается имеющееся количество методов в связи с двумя переменными.

Figure 5. Analysis of the practices - Risk management maturity model

Стадия зрелости риска*

Период осуществления **	СТАДИЯ 1	СТАДИЯ 2	СТАДИЯ 3	СТАДИЯ 4
Более четырех лет		**4**	**3**	**8**
Менее четырех лет		**2**		

* Согласно Комплексной сетке зрелости рисков

** Информация, полученная во время первого обследования по процессу управления рисками

РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов

РАЗДЕЛ 2: Процесс управления рисками	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	Выражение признательности	

Целевая группа ЕЭК ООН по управлению рисками в контексте гибкого развития

1. Сводная информация

РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов	2. Введение

Многие национальные статистические институты (НСИ), наряду с другими организациями государственного и частного секторов, создали подходы к управлению рисками, чтобы помочь им выполнять текущие инициативы и изменения в области бизнеса, хотя и на разных уровнях зрелости. Управление рисками является основной частью традиционного управления проектами и, как правило, хорошо понимается и хорошо внедряется. Однако все чаще НСИ обращаются к использованию гибких-проектов и процессов для достижения своих целей, в частности, но не ограничиваясь технологическими изменениями. В рамках работы Группы высокого уровня ЕЭК ООН по модернизации официальной статистики несколько НСИ отметили возникающую напряженность в своих организациях между традиционным управлением рисками и функционированием в в сфере гибкого управления.

Была создана целевая группа для разработки способов смягчения этих напряжений, в то же время, используя возможности, связанные с реализацией проекта гибкости.

Этот пункт дополняет руководство ЕЭК ООН по практике управления рисками в статистических организациях, излагая:

а) Как НСИ могут повысить эффективность их управления рисками за счет более широкого использования гибких методов и процессов и гибкой культуры.

б) Как гибкая рабочая среда / культура может способствовать более эффективному управлению риском, а не отклоняясь каким-либо образом от традиционного управления рисками.

ЕЭК ООН Комитету по модернизации организационной структуры и оценки предлагается рассмотреть и поддержать выводы целевой группы, и при необходимости, принять эти подходы.

2. Введение

1. Сводная информация	РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных	3. Предполагаемые противоречия между традиционными управления

		статистических организациях посредством использования гибких принципов	рисками и гибкими методами управления рисками	

I. Управление риском в НСО

Риск может быть определен как «влияние неопределенности на цели», где «влиянием является отклонение от ожидаемого (положительного и / или отрицательного), часто выражаемого с точки зрения сочетания последствий события (включая изменения в обстоятельствах) и связанное с этим вероятное возникновение».

НСО работают в условиях неотъемлемых угроз безопасности возможностей. И это могут быть угрозы безопасности относительно качества статистики, безопасности данных, возможностей или общей производительности. Поэтому многие НСО видят управление рисками как неотъемлемый вклад в достижение высоких результатов, а также создание платформы для инновационной работы. Благодаря управлению рисками, организации стремятся свести к минимуму, хотя и не обязательно и устранять, угрозы, и максимально увеличить возможности.

Эффективное управление рисками изначально основано на принятии соответствующих решений. Мы все принимаем решения каждый день; некоторые решения будут создавать угрозы или возможности, в то время как другие будут смягчать угрозы. Управление рисками помогает нам принимать решения, соответствующие уровню риска, который мы готовы принять.

Существует много факторов, которые способствуют успешному управлению рисками, например:

- поручительство высшего руководства для управления рисками и готовность инвестировать средства в управление рисками и создавать возможности управления рисками в соответствии с передовыми стандартами;
- наличие конкретной и сосредоточенной инфраструктуры для поддержки управления рисками, т. е. политика управления рисками, корпоративный регистр рисков, обучение управлению рисками и централизованная поддержка;
- наличие четких заявлений о готовности к риску (как объясняется далее в настоящем документе) или допущения, позволяющие принимать соответствующие решения в соответствии с планируемыми результатами организации;
- развитие положительной культуры управления рисками, которое внедряет и поддерживает активное управление рисками для обеспечения наилучшего принятия решений во всех статистических организациях
- принятие мер по прогнозированию, обработке или устойчивости по отношению к угрозе и использованию возможностей; в соответствии с согласованными уровнями готовности
- мониторинг и обзор прогресса с целью поиска возможностей для каких-либо дополнительных действий. Например – «сделали ли мы достаточно?»;
- рассмотрение рисков посредством использования планов действий (смягчения) или допущение (принятие) риска, когда риски неконтролируемые, и очевидны непредвиденные обстоятельства;
- установление надлежащих процессов эскалации, при которых неуправляемые угрозы представляются высшим руководителям стратегически оценивающим и принимающим окончательные решения относительно воздействия на угрозу или терпимости к угрозе, с учетом возможных последствий.
- эффективная идентификация ответственных и подотчётных лиц, которые принимают на себя ответственность за любые риски.
- обеспечение эффективных планов действий в чрезвычайных ситуациях для поддержки управления произошедшими рисками.

Гибкая методология в НСО

Осуществление гибких методов берёт своё начало из разработки программного обеспечения в качестве подхода, когда требования и решения развиваются благодаря сотрудничеству между самоорганизующимися, меж функциональными командами. Оно способствует адаптивному планированию, мощному / стратегическому развитию, постоянному совершенствованию и также быстрому и гибкому реагированию на изменения. Некоторые общие методы, связанные с гибкой методологией, включают использование Scrum, Kanban, непрерывной интеграции, графики ликвидации / понижения и т. д. Гибкая методология фокусируется на раннем и частом предоставлении соответствующих целевому назначению решений, тем самым определяя ценность при первой же возможности, и обучение в результате быстрой обратной связи для удовлетворения потребностей клиентов.

Гибкая практика по сути снижает риск. Например, отслеживание изменений и развития в серии «спринтов» помогает обеспечить постоянную обратную связь и согласование с ожиданиями клиентов. Это само по себе снижает риск, позволяет допустить более высокий уровень риска и управляет самым большим риском, с которым есть вероятность столкнуться при выполнении любой инициативы - риска невыполнения. Было также признано, что некоторые меры «процессии» гибкой методологии (ежедневная готовность и быстрое планирование и т. д.) необходимы для обеспечения эффективности, но они могут быть сосредоточены в командах без объемного участия заинтересованных сторон.

НСО - это организации, подкрепленные технологиями; поэтому мы наблюдаем растущее использование исполнения гибкой методологии, как с точки зрения систем и инструментов, так и с увеличением использования гибких технологий в более обширном осуществлении проектов. В быстро меняющемся мире НСИ претерпевают значительные изменения, особенно в области цифровой и технологической трансформации. Этот акцент на изменения и технологии позволил преобразовать гибкую методологию в культуру НСО.

3. Предполагаемые противоречия между традиционными управления рисками и гибкими методами управления рисками

⇦	2. Введение	⇧РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов	4. Будущий подход к планированию рисков в НСО в условиях исполнения гибкой методологии	⇨

Ряд организаций, у которых имеется зрелый опыт, как в области управления рисками, так и в использовании гибкой методологии, признали некоторые общие проблемы, которые возникают. Об этом говорится ниже. Проявление этих напряжений ни в коем случае не является универсальным, но полезно признать, что они могут существовать. Даже если организации не сталкиваются с этими проблемами в настоящее время, они могут возникнуть в будущем.

Сторонники гибких методов думают, что традиционные методы уже «не современны»

Некоторые практикующие представители гибкой методологии воспринимают явное управление рисками как ненужное, откладывая управление рисками, пока они не проявятся в проблемах, а затем управляют ими через естественную прогрессию «спринт». Более того, гибкая культура также поощряет доверие и расширение прав и возможностей команд, что регулярно определяет приоритетность деятельности и постоянное рассмотрение потока. Некоторые практикующие рассматривают этот подход как противоречащий традиционному управлению риском, который может быть

сфокусирован на предотвращении потенциальных проблем, а не на том, чтобы сосредоточиться на задаче.

Управление рисками может являться многоуровневым механизмом отчетности и обеспечения, что противоречит выполнению гибкой методологии. Например, модели управления рисками располагаются рядом с архивом данных рисков, классификацией и систематизацией и оценочной матрицей (обычно управляемой через электронную базу данных о рисках). Опыт всех организаций показал, что проекты с использованием гибкой методологии стремятся ограничить использование такой базы опыта и вместо этого, использовать информационное рабочее пространство и соответствующие форумы. Это ограничивает способность организации рассматривать весь спектр риска, влияние накопленных данных о рисках и корпоративную память, содержащуюся в хранилище данных рисков организации.

Однако гибкая методология учитывает баланс между затратами и преимуществами ведения риска. Это позволяет избежать совпадений циклов в процессах принятия решений и отчетности, если принимать решения относительно воздействия на риск по мере их возникновения.

Представители традиционных методов считают гибкие методы неубедительными

Существуют вопросы, вызывающие озабоченность и требующие решения в отношении достижения убедительности проектов с использованием гибкой методологии. Гибкий способ работы, сосредоточен на быстром, краткосрочном планировании. Вытекающие из всего этого изменения уровня доверия, могут увеличить озабоченность высших руководителей в отношении стратегического распределения и исполнения. Представители команды гибкой методологии будут делать акцент на преимущества права выполнения, смещения акцентов, перераспределения ресурсов, своевременного исполнения с целью обеспечения постепенного прогресса.

Однако, рассмотрим это на организационном уровне. В качестве НСО, мы сталкиваемся со многими рисками в современном мире, будь то обеспечение безопасности данных, доверенных нам, способность идти в ногу с быстрыми изменениями в технологии и обществе, или последствиями продолжающегося глобального давления со стороны государственных фондов. На макроуровне мы не можем игнорировать или не смягчать эти риски. Кроме того, на микроуровне мы сталкиваемся с рисками, связанными с возможностями наших людей, качеством наших статистических результатов и уязвимостью наших систем и процессов, и все они должны быть идентифицированы, поняты и смягчены для обеспечения успеха.

Иногда гибкую методологию не считают эффективным подходом к управлению рисками стратегического уровня из-за её краткосрочного горизонта и связи с операционным уровнем. Однако в гибкой среде можно извлечь уроки для эффективного управления наиболее стратегическими рисками, с которыми сталкиваются статистические организации.

Краткосрочное планирование против долгосрочного планирования

Организации государственного сектора должны планировать в более долгосрочной перспективе. Общественная организация должна учитывать использование государственных денег, стратегическое направление для организации и то, как она будет влиять на общество. Видимо, гибкие условия исполнения противостоят данному долгосрочному фокусу, при этом многие из их процессов и методов задействованы здесь и сейчас.

С другой стороны, традиционное управление рисками ассоциируется с слишком строгим акцентом на жестких сроках. Хотя это может помочь снизить риски для исполнения. Но для своевременного, качественного выполнения задач, традиционному управлению может не хватать гибкости, необходимой для быстро меняющейся ситуации. Характер гибкой среды означает сосредоточение на постепенном продвижении к общей цели, которая может помочь справиться со сложной средой, но также может противоречить необходимости иногда сосредотачиваться на срочной доставке. НСО разработали

способы преодоления напряженности, установив более длительные сроки (например, день переписи) и используя гибкую методологию на небольших дистанциях для достижения цели.

Следует также признать, что часто управление рисками в значительной степени рассматривается с учетом негативных характеристик, а не как более широкого спектра, связанного с возможностями, в особенности в организациях с менее развиты подходом к управлению рисками. Напротив, гибкая среда больше ориентирована на признание рисков как возможностей и способность адаптироваться к их использованию. Если управление рисками следует признать полезным инструментом принятия решений, его следует рассматривать как средство обеспечения успеха, а не препятствия для успеха.

4. Будущий подход к планированию рисков в НСО в условиях исполнения гибкой методологии

3. Предполагаемые противоречия между традиционными управления рисками и гибкими методами управления рисками	РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов	5. Принципы	

Очевидно, что всё чаще используется подход гибкой методологии в НСО и в некоторых случаях могут возникнуть сложности. Во время ускоренных изменений в технологиях и данных нам нужно найти способ решить проблему осуществления гибкой методологии, а также управлять в среде, наполненной рисками, и обеспечивать гарантию успешного исполнения.

Гибкую методологию нужно рассматривать не в ущерб управлении рисками, а скорее как вспомогательное средство для более эффективного управления рисками.

Взаимопонимание в НСО и осознание проблем, с которыми мы сталкиваемся в этой области, и тем, как мы с ними справимся, поможет нам всем добиться большего успеха. Очевидно, есть возможности для рассмотрения управления рисками в среде гибкой методологии. Для достижения таких преимуществ нам следует задаться такими вопросами, как:

• Как мы можем использовать гибкую методологию, сохраняя при этом правильный курс на гарантию и надёжность успешного исполнения?

• Как можно совместить традиционное управление рисками с гибкой методологией для обеспечения успешного исполнения?

• Как НСО могут повысить эффективность внедрения лучшей практики управления рисками таким образом, которая подходит для гибкой культуры?

• Можем ли мы определить принципы управления рисками в контексте гибкой среды, чтобы узнать о приоритетных действиях при осуществлении проекта гибкости?

Для решения вышеуказанных вопросов целевая группа по разработке подхода основывается на опыте НСО. Этот подход основан на ряде принципов, которые, если они будут приняты, помогут НСО повысить эффективность управления рисками, используя преимущества гибких методов работы и принципов. Основное внимание уделяется использованию управления рисками в гибкой среде, чтобы помочь организации исполнять и принять решения в соответствии с готовностью к риску.

5. Принципы

Диаграмма 6: Пирамида неопределённости

4. Будущий подход к планированию рисков в НСО в условиях исполнения гибкой методологии	РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов	6. Заключение	

ПРИНЦИП 1: Определи свою готовность к риску, претвори в жизнь

Основополагающим принципом гибкого исполнения является ориентация на удовлетворение потребностей клиентов, а фундаментальный принцип управления рисками - обеспечение уверенности в том, что организация понимает и смягчает угрозы для исполнения. Чтобы позволить организации понять потребности своих клиентов, а также обеспечить уверенность, когда это необходимо для управления рисками, необходимо определение и согласованность относительно использования уровней готовности к риску.

Традиционные подходы к определению готовности к риску ориентированы на простые описания готовности по разным бизнес-аспектам, или, даже, для всей организации в целом. Например, организация может заявить, что она «не склонна» рисковать в сфере информационной безопасности или «осторожна» в отношении финансового риска. Эти простые утверждения о готовности могут дать широкое указание, но открыты для интерпретации («осторожный» человек «активно ищет другого») и может оставаться статичным в течение определенного периода времени.

Альтернативный подход и подход, который больше подходит для управления рисками в гибкой среде, - это определение склонности к риску таким образом, чтобы обеспечить правильное и последовательное поведение в организации в соответствии с ожиданиями руководства заинтересованных сторон. Для достижения этой цели организация должна согласиться с поведением, ожидаемым на разных уровнях готовности к риску, и четко сформулировать его как основу для принятия решений.

Основное преимущество этого подхода заключается в том, что он устанавливает четкое поведение, которое ожидается на разных уровнях готовности к риску, а не ряд нечётких заявлений, открытых для интерпретации. Формулирование поведения таким образом даст ясность для планированных результатов организации и позволит готовности к риску приспосабливаться к нуждам организации. Управление рисками в гибкой среде, где риск сосредоточен на принятии решений, является ключевым фактором успеха.

На диаграмме 6 показан пример заявления о готовности к риску для конкретного типа риска, в данном случае «Безопасность данных», и как можно сформулировать ожидаемое поведение, чтобы обеспечить согласованность при принятии решений.

Диаграмма 6. Пример заявления о готовности к риску

Тип риска: Данные о безопасности				
Несклонный	**Минимальный**	**Осторожный**	**Открытый**	**В активном поиске**
Мы избегаем потери доверия наших респондентов в связи раскрытием данных, но признаем, что наш бизнес зависит от доступа к данным и обработки данных, которые несут в себе угрозу безопасности. У нас установлено четкое управление и процессы обеспечения безопасности данных. Совет регулярно обсуждает вопросы безопасности. Мы понимаем соответствующий уровень кибер безопасности во всех наборах данных и инвестируем в приоритетные области. Мы рассматриваем наши политики безопасности и признаём более низкий уровень риска в отношении систем и данных, но также мы признаем, что потеря данных может нанести				

значительный ущерб репутации организации.

Мы допускаем надлежащий доступ к данным для персонала, с тем чтобы организация могла выполнять свою программу исследований, разработок и анализа.

Мы готовы рассмотреть доступ для одобренных исследователей к соответственным данным администратора.

ПРИНЦИП 2: Определите угрозы и возможности

Управление рисками в гибкой среде остается важным как для выявления угроз, так и возможностей. Однако подход к этому определению должен быть четко связан с целями организации, решениями, которые необходимо принять, и ее определенной готовности к риску. Люди, работающие в организации, после определения риска возможно должны будут последовать следующим шагам:

• Бизнес-план или план проекта

• Принятие необходимого решения для обеспечения успешного исполнения(насколько можно эффективнее пересмотреть все варианты от А до Я)

• Сопоставить решение, которое вы принимаете с готовностью к риску, связанным с деятельностью

• Решения, которые создают угрозы или возможности за пределами готовности к риску, требуют от кого-либо взятия на себя ответственности, документирования в корпоративной системе рисков и управления

• Если вы принимаете решение об исполнении, которое создает угрозу выше уровня готовности к риску или в её пределах, вы должны выбрать либо воздействие на риск, либо принятие данного риска

• Если вы решили воздействовать на угрозу или возможность, вы должны предоставить доказательства того, что вы делаете, чтобы уменьшить угрозу на уровне готовности.

• Если вы решите терпеть(принять) угрозу, вы должны задокументировать угрозу в регистре риска.

Эти шаги должны способствовать интегрированию управления рисками в исполнение целостным процессом в повседневные операции организации. Они также полезны для определения «правильных» (истинных и правдивых) угроз или возможностей, поэтому усилия могут быть сфокусированы на истинных опасностях для исполнения, а не на документировании общих «не», угроз для обеспечения ложной гарантии. Диаграмма на рисунке 1 показывает, когда и как могут быть записаны или усилены угрозы / возможности (также связанные с Принципом 3).

Следует признать, что этот принцип может быть соблюден, независимо от того, работает ли организация с помощью гибкого подхода или нет. Тем не менее, это понимание рисков как возможностей, так и угроз, которые демонстрируют более зрелый подход к управлению рисками, и это особенно актуально в гибкой среде. Гибкая методология ориентирована на исполнение и поэтому использует риск возможностей для быстрого исполнения, для обеспечения дополнительных улучшений и удовлетворения потребностей клиентов. Смещение внимания от смягчения угроз (прекращение плохих событий) для использования возможностей (сделать так, чтобы происходили хорошие события) имеет основополагающее значение для управления рисками в гибкой среде.

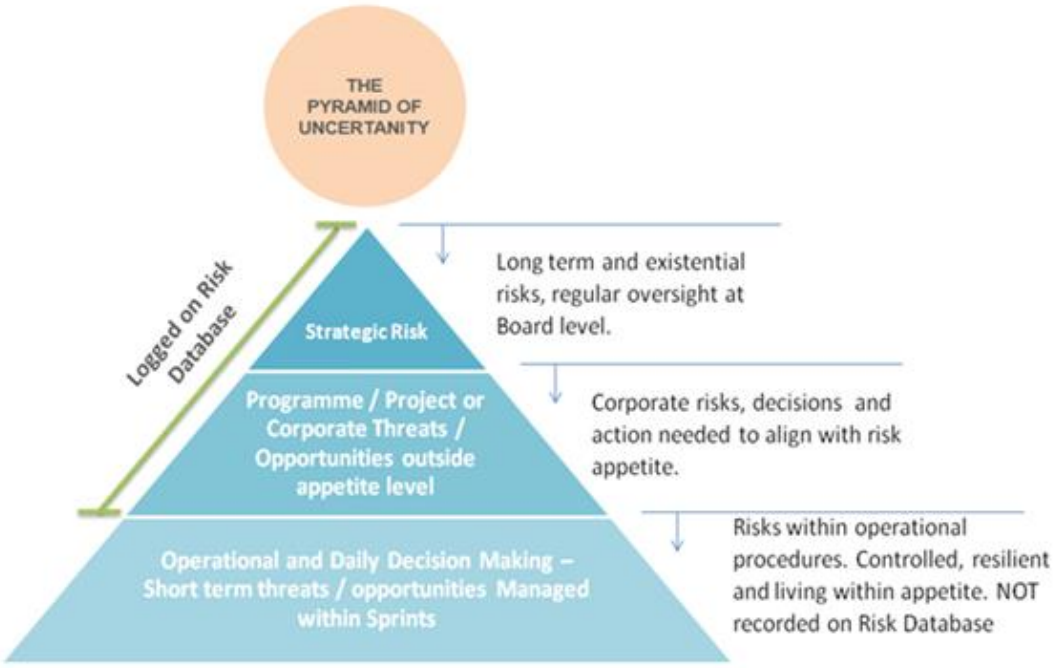
ПРИНЦИП 3: Управляй угрозами используй возможности на самом подходящем уровне, но обосновывай и переходи на следующий уровень в случае необходимости

Для поддержания гибкой среды, важно, чтобы управление рисками создавало среду, в которой решения принимаются на правильном уровне, где персонал наделен полномочиями и способен быстро и своевременно устранять угрозы и использовать

возможности, и при этом, имея право не следовать чрезмерно предписывающему процессу.

На рисунке 6 показана «Пирамида неопределенности», демонстрирующая степень надзора за каждым уровнем риска. Пирамида показывает, что большое количество ежедневных решений будет основано на рисках, они не должны регистрироваться в корпоративной системе или внедрены в уровни управления. Управление рисками в гибкой среде - это быстрое принятие в соответствии с готовностью к риску, которое должно формально регистрироваться только тогда, когда необходимо предпринять дополнительные действия для смягчения риска или использования возможности.

Диаграмма 6: Пирамида неопределённости



Однако, чтобы обеспечить уверенность в управлении рисками, организация должна по-прежнему доказывать эти решения, которые создают угрозы или возможности выше или ниже уровня готовности к риску.

Как показано на диаграмме 6, в любой организации будет приниматься большое количество решений, каждое из которых само по себе будет смягчать риски и использовать возможности.

Важно, чтобы эти решения принимались как можно ближе к месту воздействия, как по времени, так и по месту в организации. В гибкой среде исполнения, они будут идентифицированы и рассмотрены в скоростном процессе. Поэтому управление рисками в гибкой среде должно быть сосредоточено на регистрации угроз или возможностей как официальных корпоративных рисков только, если:

- Можно обосновать разумное смягчение с целью попытки управления угрозой / возможностью, и
- Угроза / возможность - это уже не чья-то работа, или установленный процесс для управления угрозой / возможностью, и

Угроза или возможность за пределами готовности организации к риск

Диаграмма 7: Модель зрелости гибкого управления риском

Темы	Уровень зрелости №1	Уровень зрелости	Уровень зрелости №3	Уровень зрелости №4	Уровень зрелости №5

		№2			
Зрелость готовности к риску	Обычное заявление о готовности	Заявление о готовности на разных уровнях деятельности и организации	Заявления о готовности подкрепляются более подробными планами относительно того, как организация должна вести себя, чтобы соответствовать готовности	Готовность, является частью ежедневного и стратегического процесса принятия решений. Допустимости готовности объективно оспариваются на уровне совета директоров, используя в качестве параметров, существующие модели поведения	Принятие соответствующего решения,приемлемое для целостного процесса принятия решений. Общесистемная интуитивная способность при оценке решений связанных с риском, вытекающая из готовности к риску,для определения стратегии
Зрелость культуры риска **Зрелость культур**	Сотрудникам руководящего звена и лидерам известно, что необходимо управлять рисками и действовать, но не могут понять почему и как, при существовании информационных материалов об управлении риска, рядовые сотрудники не вчитываются и не разбираются в них.	Риски часто не соответствуют целям бизнес-сферы или директората. Есть знания о необходимости управления рисками, но концепция до конца не постигнута. Есть понимание теории и процессов, лежащих в основе формального управления рисками. Но управление риском вопринимается как упражнение , которое нужно выполнить, чтобы поставить галочку, а не	Сотрудники, руководители и лидеры знают, как идентифицировать, анализировать, оценивать, и сообщать о рисках в последовательноми структурированном виде в соответствии с руководящими принципами. Присутствует самостоятельное участие в действиях связанных с риском. Руководство на всех уровнях организации чётко понимает как следует управлять риском и соответственно действуют. Руководство на всех уровнях информирован	К дополнению к 3-му уровню, здесь сотрудники могут: эффективно управлять этими рисками, самостоятельно или совместно с партнерами, и также уверенно настаивать на своей точке зрения в работе с партнерами. Обеспечить эффективную работу департамента отчитывающегося перед общественностью о значительных рисках, возникающих в их районе Формально проанализировать эффективность всех аспектов своей деятельности по управлению	К дополнению к 4-му уровню, здесь сотрудники могут : Создавать долгие и крепкие патртнёрские союзы , рабочие режимы и отношения Использовать управление рисками для выявления возможностей, а также и угроз. Руководство высшего звена активно участвует в расширении своих горизонтов относительно управления рисками, участвуя во внешних мероприятиях. Есть ключевые сотрудники,у которые, возможно, обладают либо

ы риска		как инструмент для реального улучшения бизнеса. Понимание организационной деятельности на сегодняшний день, в том числе, высшего руководства, стратегические риски и наличие заявления политики управления рисками, структуры/ руководства и учебных программ по управлению рисками. Они понимают, к кому обратиться для дальнейшей поддержки. Ключевые фигуры заинтересованы и ищут тренинги по теме. Понимание основных рисков для организации и сферы их воздействия. Понимание формальных процедур, которые необходимо выполнять. Но пока всёже их все не выполняют (за	о о работе, которую они контролируют, и обладает навыками интерпретации и оспаривания того, что они видят, чтобы выявить риск. Ключевые сотрудники осознают необходимость управления рисками совместно с партнерами и обладают навыками и знаниями, необходимыми для управления этими рисками. Все владельцы информационных активов прошли базовую подготовку и поняли: Риски выявлены и зафиксированы, но едва ли предпринимаются действия для эффективного смягчения угроз или использования возможностей.	рисками. Топ менеджеры активно участвуют в расширении своих горизонтов относительно управления риска, путем участия во внутренних мероприятиях и обучении. Организация все чаще рассматривается в качестве лучшего примера в правительстве. Все обладатели и менеджеры информационных активов знают о важности эффективного управления информационными активами и ценят их преимущества .И, если они принимают решение, тесно связанное с риском ,оно должно соответствовать готовности организации к риску. Угрозы / возможности за пределами готовности регистрируются и принимаются или допускаются.	профессиональной квалификацией в области управления рисками, или у которых есть опыт проактивного подхода в этой области, с готовностью к постоянному обучению. Этих людей слушают. Высокопоставленных лиц, например генеральных директоров можно заметить выступающих на семинарах по управлению рисками. Пропагандисты управления рисками или руководители обладают навыками преподавания и обучения других сотрудников. Организация признана Центром передового опыта и знаний в правительстве и во всем мире. Сотрудники всех уровней осведомлены о важности эффективного управления информационными активами и ценят его преимущества

		неимением наывоков или обязательства) Недостаточная грамотность в сфере управления рисками Официально, риски не выявляются и не фиксируются в журналах.			
Зрелость гибкого (Agile) исполнения	Планы определяются наперёд . Выполнение осуществляется нечастыми «скачками».	Группы по исполнению проводят общие встречи на тему гибкого исполнения (ежедневные быстрые встречи, спринты, планирование в краткие сроки и т.д.), здесь занимаются рисками низкого уровня. Но всё это по-прежнему довольно поверхностно - на данном уровне планы общего / высокого уровня по-прежнему в значительной степени фиксируются, а исполняются все еще нечасто. Таким образом, низкая степень	Частота исполнения намного выше, и постепенно увеличивается значимость. Группы по исполнению признают так называемые фильтры рисков / проблем / вопросов /неопределенностей , которые влияют на планы более высокого уровня.	Организация должна постепенно увеличивать значимость исполнения. Исполнение «скачками» дело прошлого. Для изменения планов регулярно используются обратная связь пользователей, клиентов и рынка.	Управление неопределенностью заложено во все планы и процессы исполнения; команды (и организация) постоянно проверяют предположения и гипотезы; непрерывно отчитываются о значимости и обратная связь в результате исполнения влияет на последующие процессы исполнения .

		использования гибкой методологии еще не повлияла на более высокие уровни			
Зрелость ресурсов управления рисками и гибких ресурсов	У организации нет команды по управлению рисками или экспертов гибкой методологии и	Есть специальные команды по управлению рисками экспертов гибкой методологии и	Регулярное сотрудничество команды по управлению рисками и команды экспертов гибкой методологиии	Объединенная сеть квалифицированных, обученных и опытных представителей обеих команд: управления рисками и гибкой методологиии	Эксперты обеих команд-управления рисками и гибкой методологиии формально являются частью всей структуры правления

6. Заключение

5. Принципы | РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов

Этот пункт и работа Целевой группы, которая поддерживала его разработку, выявили ряд общих проблем в НСО относительно применения управления рисками и преимуществ работы в гибкой среде исполнения.

Очевидно, что управление рисками является эволюционным процессом, и разные организации находятся на разных уровнях зрелости. Для тех организаций, которые внедрили подход к управлению рисками в соответствии с лучшей международной практикой, принципы в этой статье могут быть использованы для ускорения с этих оснований и повышения зрелости до уровня высокоэффективной организации.

В диаграмме 7 представлена модель зрелости, что демонстрирует поведение, которое может квалифицировать организацию для достижения разных уровней зрелости в отношении различных измерений. К ним относятся: «Готовность к риску», «Культура риска», «Гибкое исполнение» и «Риск и гибкий ресурс»). Эта модель была разработана целевой группой, чтобы помочь организациям понять путь и положительные шаги на каждом этапе.

Мы продемонстрировали согласованность между управлением рисками и гибкой методологией, с целью заверения того, что управление рисками в корне основано на эффективном принятии решений, чтобы воспользоваться гибким исполнением, как процессом, который по своей сути снижает риск и использует гибкие методы для лучшего управления рисками.

В быстро меняющемся мире и в условиях множества новых угроз и возможностей НСО могут использовать эти принципы для обеспечения их постоянного успеха.

Работа целевой группы ЕЭК ООН по управлению рисками в контексте гибкого развития выявила многие аналогичные проблемы, с которыми сталкиваются НСО со всего

мирового сообщества. С революцией данных это сообщество организаций сталкивается с беспрецедентными изменениями и возможностями.

Чтобы продолжать помогать друг другу в этой сложной среде, члены целевой группы согласились продолжать совместную работу. В этой работе основное внимание будет уделено практическому применению, в дальнейшем рассмотрению тематических исследований и модели зрелости и оказанию помощи друг другу в реализации принципов, изложенных в настоящем документе.

В случае утверждения содержания настоящего документа целевая группа вновь соберётся в новом году для дальнейшего развития этой работы. Также предлагается провести последующий практикум для более широкого сообщества с целью рассмотрения как результатов этой целевой группы, так и других приоритетных областей, включая разработку регистра рисков самого высокого уровня, которые являются общими для НСО учётом возможности коллективного управления для взаимной выгоды.

Выражение признательности

РАЗДЕЛ 3: Укрепление существующего управления рисками в национальных статистических организациях посредством использования гибких принципов	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	Annex - Focus on risk management practices	

Выражение признательности

Рабочая команда

Выражение признательности	НСО и статистические организации	

Проект данного руководства было составлено в Комиссии по модернизации организационной структуры и оценки (MCOFE) под руководством Джеки Майда, Директора отделения проектирования систем в Статистике Канады, во взаимодействии со Стивеном Вейлом, Старшим статистиком из ЕЭК ООН, а также при поддержке Татьяны Коломиец, Помощника по вопросам статистики в ЕЭК ООН.

Руководство было составлено Рабочей группой, координируемой национальным институтом статистики (Истат) в сотрудничестве с Римским университетом «Тор Вергата», и состоящей из следующих членов (в алфавитном порядке):

1. ИСТАТ: Фабрицио Ротунди (Координатор), Марко Тоцци и Анжела Леонетти, Главное управление – Управление рисками; Элеонора Паолоцци и Элеонора Роччи, Управление по человеческим ресурсам – Персонал, Филомена Грассиа, Управление по обслуживанию гражданских служащих (DCPS) – Международные дела;

2. Римский университет «Тор Вергата»: Профессор Алессандро Хинна (Координатор), Доктор философии Федерико Кесчел и Доктор Данила Скарозза.

Paragraph n. 10 has been provided by the *UNECE's Task Team on Risk Management in the Context of Agile Development:* Ben Whitestone and Rich Williams, ONS UK (Co-Chairs), Michael Quinlan, CSO Ireland, Michael Goit and Sarah MacKinnon, Statistics Canada, Phillip Wise, Carrollyn Wall and Patrick West, ABS, Fabrizio Rotundi and Marco Tozzi, Istat, Alessandro Hinna and Federico Ceschel, University of Rome, Armando Zuñiga, INEGI Mexico, Anna Borowska and Agnieszka Komar-Morawska, CSO of Poland, Olja Music, Statistical Office of the Republic of Serbia, Alexander Sindram, Statistics Netherlands, Alessandra Politi, Eurostat, Steven Vale and Tetyana Kolomiyets, UNECE.

The ISTAT's Case study in the Annex (ph. 10) has been described by Cecilia Colasanti, ISTAT.

НСО и статистические организации

Рабочая команда	Выражение признательности	

The three surveys on risk management have involved more than 60 among national and international statistical organizations.

Here follow all the participant countries:

1st survey on risk management (April – May 2015)

Albania, Andorra, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Monaco, Mongolia, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Tajikistan, The former Yugoslav Republic of Macedonia, Turkey, Turkmenistan, Ukraine, United Kingdom, United States, Uzbekistan.

2nd survey - In-depth survey on risk management practices (September 2015)

Australia, Croatia, Austria, Ireland, Canada, The Netherlands, Lithuania, Sweden, Mexico, South Africa, New Zealand, United Kingdom, Romania, Italy

3rd survey – "What was most Successful, What was most difficult, What not to do when implementing risk management in NSOs' experiences" (July – September 2016)

Australia, Austria, Belgium, Canada, Croatia, Estonia, Eurostat, Finland, Iceland, Ireland, Italy, Lithuania Malta, Mexico, The Netherlands, New Zealand, Norway, Poland, Republic of Armenia, Romania, Slovakia, Slovenia, South Africa, Sweden, The Netherlands, United Kingdom, USA.

After the workshop on risk management practices in statistical organizations held in Geneva on 25-26 April 2016, the NSOs involved in reviewing the guidelines have sent observations and suggestions which have significantly contributed to draw up this final document.

Annex - Focus on risk management practices

Выражение признательности	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	List of reviews	

Introduction

This Annex has to be considered an integral part of the guidelines for developing risk management practices coming from the survey analysis. Its goal is, on the one hand, to highlight the amount of information obtained, on the other hand, to show a more practical approach to the different domains of risk management.

Like the first, "theoretical" part, the Annex consists of two sections, risk framework and risk process; the paragraph arrangement also mirrors the guidelines in order to help the two parts in referring to each other.

Within both sections two categories of examples are shown:

1. Focus points on risk management core topics, in order to share practices, coming from the NSOs, able to substantiate "theoretical" information;

2. Case-studies, shortly reporting some NSOs' significant experiences on particular features of the risk management systems in order to, on the one hand, share the know-how gained from implementing risk management within the different organizational contexts, on the other hand, highlight any elements in common among the different experiences.

Section 1. Risk framework

Annex - Focus on risk management practices	Section 2. Risk management process

Paragraph 1.2: Establishment risk policy.

Corporate risks are linked to the strategic objectives. In order to face each risk, a response strategy, organized in planning and actions, is developed. The example of Canada reflects the top-down approach to risk management, starting from the risk identification phase (please see the theoretical part of the guidelines for further information).

Focus on - Building-up a risk policy and a corporate risk profile in Statistics Canada
At Statistics Canada, Integrated Risk Management (IRM) is an ongoing and dynamic activity that supports corporate decision-making, and is a central theme of the annual integrated strategic planning process. An integral part of Statistics Canada's risk management model is the corporate risk profile, a high-level summary of the most critical risks being managed by Statistics Canada. The development corporate risk profile was a comprehensive process that included a review of risk information from several sources and reflected recommendations from the Management Accountability Framework Round IX, as well as feedback from managers. The process also included an improved risk questionnaire, revised guidelines, and clearer definitions of risk sources. A communication strategy was developed and implemented involving information sessions, a documentation package and reinforcement of the importance of IRM in

the Agency. The information sessions also served to remind managers of their roles and responsibilities in the IRM process and to address any questions and concerns they had.

All program area risk registers were reviewed and approved by the respective Field Planning Board to ensure that the risks were equally understood, explicitly identified in the long-term planning process and took into consideration interdependencies between projects. After having identified the key risks, the managers were also required to assess likelihood of occurrence and potential impact. The information collected from risk registers provided the Agency with a hierarchical risk assessment.

To ensure that the revised corporate risk profile reflected the major risks currently facing Statistics Canada, a number of significant documents were also reviewed (risk registers, program performance reports, project executive dashboards, program quality reviews, internal audit reports, the Report on Plans and Priorities, the Departmental Investment Plan, the Departmental Security Plan, and the Business Continuity Plan). This approach also responded to the advice received from the Departmental Audit Committee (DAC), the Administrative Practices Committee (APC) and the Corporate Planning Committee of Policy Committee.

The draft corporate risk profile was developed following this advice and included the six key risks and the corresponding mitigation strategies, the risk's link to the Program Alignment Architecture and its link to organizational priorities (see example below).

Risk	**Risk Response Strategy**	**Link to Program Alignment Architecture**
Increased difficulties in reaching respondents	Mitigation strategies identified in the Agency's corporate risk profile for 2012/2013 to 2013/2014 comprise closely monitoring response rates and assessing potential biases in survey results; continuing the research and development of the dwelling-based household survey frame as an alternative to existing frames respondents; engaging respondents through various mechanisms (Statistics Canada, Government of Canada and other departments' websites as well as social media) to ensure high response rates; reviewing the possible use of administrative data sources, keeping in mind privacy concerns as these sources are used further; continuing to innovate to meet respondents' needs, which includes greater use of multi-mode data-collection options, such as e-questionnaires and mobile devices; continuing to investigate the possibility of conducting interviews by cellphone; undertaking additional studies; and incorporating lessons learned.	• Socio-economic Statistics • Labor, Education, Income and Tourism Statistics • Health and Justice Statistics • Demographic, Aboriginal and other Social Statistics • Analysis of Socio-economic Statistics • Censuses • Census of Population • Census of Agriculture • Professional and Statistical Services • Cost-recovered Services related to Socio-economic

Source: ***Corporate risk profile methodology and outcome*****. Statistics Canada: http://www.statcan.gc.ca/**

Once the 2012-13 and 2013-14 corporate risks were validated, functional leads and management committees were assigned to review existing and potentially new mitigating strategies and prepare action plans and timelines. The APC then reviewed and approved the full corporate risk profile, before it was presented to the DAC. After receiving final approval by the Corporate Planning Committee, the corporate risk profile was posted on Statistics Canada's Internal Communications Network.

The following list identifies and describes the Agency's (SC) three top corporate risks:

Increased difficulties in reaching respondents: An ongoing challenge to the quality of social statistics is the growing difficulty with collecting information from respondents. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

Reputational risk related to respondent information: Any releases of confidential information, or real or perceived breaches of Statistics Canada's informatics infrastructure and related business processes, pose the risk of damaging reputation, credibility, image and public trust. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

Common tools and government wide priorities: At present, the Agency is not using any of the software tools that have been prescribed for corporate systems (i.e., the back-office systems that support human resource and financial administration and records management). The Agency's existing systems are efficient by any standard and, in the short term, re-assigning staff from core activities to implement new systems would pose a risk to providing the statistical program. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

Focus on: A behavioral approach to risk appetite

The practice described below concerns a behavioral approach to the definition of risk appetite in order to align the Institute's risk policy with the staff's risk approach.

CASE STUDY

UK, Office for National Statistics (ONS)

Risk appetite is defined as the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time. The Office for National Statistics has had in place an overall 'risk appetite statement' for some time. However in order to truly embed risk management in decision making, deliver the organization's strategy and respond appropriately to the pressures of an increasingly changing world, ONS decided to not only review its risk appetite but to use appetite as a catalyst for transforming its behaviors.

ONS recognized that, whilst a definition of risk appetite was essential to allow consistent and appropriate decision making, a single statement of risk appetite could be bland and open to interpretation. On a scale from 'averse' to 'actively seeking' risk, a single organization position seemed to end up at the mid-point as it would take account of areas at either end of the spectrum. Also, a statement along the lines of 'we are averse to risk in x area' is open to interpretation. What does this mean? How should staff act? What are the expectations of the organization's leaders?

To address these questions ONS ran an approach to redefine risk appetite and to ensure the strategic alignment of risk based decision making, to bring risk appetite to life, and to drive cultural change. The overall approach involved setting a level of risk appetite for each of the organization's highest level 'strategic risks', which themselves were aligned to the strategic aims within the organization's strategy. A fundamental part of the approach, however, was defining the expected and specific behaviors aligned to the level of appetite, therefore developing a clear framework for decision making.

The approach taken by the ONS risk management team was simple, it involved 1) inviting the Executive and Non-Executive Directors of the organization to individually assess risk appetite across risk types (on a matrix, see overleaf), 2) to challenge and explore their views through a series of one-to-one meetings, and 3) to discuss a consolidated view at Board level and to agree the levels of risk appetite with articulated behaviors.

The ONS experience has proven the benefits of this process. Thinking through specifically what risk appetite means for culture/behaviors has been of great benefit, by way of illustration:

- Under a 'Cautious' appetite for ‘statistical quality’ risks a potential behavior may be "Formal outputs must be of high quality to maintain reputation and confidence, but development and timeliness needs to be challenged in order to improve quality. Timeliness is recognized as an element of quality therefore we aim for timely statistics whenever possible."
- Under an 'Actively Seeking' appetite for ‘innovation’ a potential behavior may be "We recognize the risk of irrelevance without innovation and are relentlessly curious, investing considerable time in new approaches and being prepared to try new things even if many of them do not result in a viable product."

In order to ensure the success of this exercise in ONS there was a parallel approach with managers from across the organization. The idea of this was to gain buy-in to the approach and to highlight any potential disconnect between the view of the senior leadership team and that of the wider organization – therefore highlighting areas where the agreed appetite would be difficult to implement.

Following approval by the organization’s Board the risk management team subsequently took the newly approved risk appetite statements and cascaded the new expectations throughout the business via seminars, risk training courses and the organization’s intranet. The risk appetite matrix is also used to regularly challenge decision making and articulate Board expectations.

Redefining the ONS risk appetite through this approach has brought color to what can be a transactional and subjective process. As well as encouraging a more uniform approach to risk taking within the organization, it supports the development of an organizational culture which is strategically aligned.

	Averse	Minimal	Cautious	Open	Actively Seeking
Risk Approach Definition	Avoidance of risk and uncertainty is a key organizational objective	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have potential for limited reward	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward and value for money	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)
Risk Type 1			• Behaviors if we were to take less risk • ...	• Agreed risk appetite and expected behaviors • ...	• Behaviors if we were to take more risk • ...
Risk Type 2			• Behaviors if we were to take less risk • ...	• Agreed risk appetite and expected behaviors • ...	• Behaviors if we were to take more risk • ...
Risk Type 3				• Behaviors if we were to take less risk • ...	• Agreed risk appetite and expected behaviors • ...
Risk Type 4	• Behaviors if we were to take less risk • ...	• Agreed risk appetite and expected behaviors • ...	• Behaviors if we were to take more risk • ...		

Paragraph 1.3: Adopting an integrated risk approach connected to statistical quality management.

Risk management must be integrated with: statistical quality management, strategic and operational planning cycle and performance assessment. Both examples proposed below have been selected because of their innovative approach to the themes of risk and quality management.

Focus on: Integration risk and quality management

Australian Bureau of Statistics (ABS)
Statistical collections are often exposed to the risk that one or more of the components of the process fail to meet the quality standard expected, such that the quality or the integrity of the statistical outputs are affected. This kind of risk is the "statistical risk".

Statistical risk arises for various reasons, some of which may include inadequate inputs, processes not being well defined, changes to existing processes, or human error.

Errors in statistical outputs can be minimized by committing to quality management strategies, such as risk management. Risk management is concerned with identifying potential risks, analyzing their consequences, and devising and implementing responses, ensuring that corporate and business objectives are achieved while upholding quality.

ABS has endeavored to instigate better quality management practices through the development and use of the risk mitigation strategy known as quality gates.

The six components of a quality gate are:

1. Placement,

2. Quality Measures,

3. Roles,

4. Tolerance,

5. Actions,

6. Evaluation.

1. **PLACEMENT.** "Placement" is the first component of the quality gate. It refers to the placement of quality gates throughout a statistical process (also known as a business process cycle, or statistical process cycle). Placement of a quality gate is determined by the level of risk associated with given points in the production process. Specifically, the placement of a quality gate should occur where a risk assessment of the process reveals that there is a need for a quality gate due to the impact on the process and statistical outputs that would occur if the risk was realized.

The ABS uses the Generic Statistical Business Process Model (GSBPM) as a guide to map the activities of statistical processes against. This is done to ensure all aspects of the statistical process are included for monitoring purposes.

By identifying the key activities associated with each step of the statistical process, an assessment of whether there are any risks in those steps can be made up front. This assists with determining where best to place quality gates. Some common risky areas in a process include:

• Hand-over or integration of data between multiple areas;

• Data transformation;

• Changes to processes, methods and systems.

The ABS has an overarching risk management framework, based on the International Risk Management Standard ISO 31000:2009, which details the ABS approach to risk management. The ABS has adapted this risk management framework to suit the business needs of the organization.

If a statistical risk assessment reveals that the risk rating is extreme or high it is recommended that a quality gate be utilized to mitigate the statistical risk.

For medium risk ratings it may be useful to utilize additional quality measures in existing quality gates that assist in monitoring the aspects which will highlight if the process isn't working correctly.

Routine procedures are generally sufficient for the monitoring of low risk ratings.

2. **QUALITY MEASURES.** Quality measures are a set of indicators that provide information about potential problems at a given point in the process. When determining what quality measures should be included in a specific quality gate it is important to consider the risks and what information would be required in order to make an assessment about fitness for purpose at that point in time.

3. **ROLES.** This component involves assigning tasks to various people or areas involved in the operation of a quality gate. Roles identifies areas or people who are directly connected to the quality gate and its operation, along with people or areas who are affected by issues with the process.

4. **TOLERANCE.** Tolerance refers to an acceptable level of quality. The acceptable level could be qualitative (e.g. Yes/No) or quantitative (e.g. 97%). Tolerance levels or thresholds are generally set by expectations of what should be observed at that point in the process for a given quality measure.

5. **ACTIONS.** Actions are predetermined responses to various outcomes for a quality gate. They provide a definition of what will be done if threshold or tolerance levels are met or not met with regards to each quality measure.

6. **EVALUATION.** As with any process that is undertaken an evaluation or review should occur to examine where improvements can be made for future use. At the end of each statistical process cycle is it recommended that the quality gates should be evaluated to determine what worked well, what didn't and where improvements can be made.

The Netherlands, Central Bureau of statistics (CBS)

Object Oriented Quality and Risk Management (OQRM) model (Nederpelt, 2012) is a quality framework developed in the field of official statistics in order to improve compliance with the European Code of Practice and deal with quality standards of statistical output.

One of the goals of OQRM was making CBS being able to decide on focus areas (60). For each of them, eleven steps can be made, including risk analysis and determining the right measures or actions to put the focus areas under control.

These measures, proposed by the managers, are integrated in the regular planning and control cycle of CBS:

1. Actions on corporate level: a set of high level objectives is identified on strategic, finance, operational and compliance level. Actions are identified to meet the objectives and assigned to the heads of divisions. Progresses of these actions are regularly monitored.

2. Action on process level: The audit framework is based on the quality guidelines for statistical processes. In these guidelines, international frameworks (CoP/QAF), national frameworks, (SN-law, privacy law, security regulations, archiving) and board decisions are integrated. Audits are also risk oriented.

The risk level is used to prioritize the recommendations in the audit report and these recommendations are converted into an action plan by the process owner.

Section 2. Risk management process

/*<![CDATA[*/ table.ScrollbarTable {border: none;padding: 3px;width: 100%;padding: 3px;margin: 0px;background-color: #f0f0f0} table.ScrollbarTable td.ScrollbarPrevIcon {text-align: center;width: 16px;border: none;} table.ScrollbarTable td.ScrollbarPrevName {text-align: left;border: none;} table.ScrollbarTable td.ScrollbarParent {text-align: center;border: none;} table.ScrollbarTable td.ScrollbarNextName {text-align: right;border: none;} table.ScrollbarTable td.ScrollbarNextIcon {text-align: center;width: 16px;border: none;} /*]]>*/

⇦	Section 1. Risk framework	Annex - Focus on risk management practices	

Paragraph 2.1: Context analysis.

Risk philosophy, risk appetite e risk strategy should be always kept aligned, as one reflects the other. To this purpose it's necessary to "measure" risk perception by the management staff – as some managers may be prepared to take more risk while others are more conservative – as well as the risk maturity of organizational context, since this latter could be more or less resilient in facing risk.

Focus on: Measuring risk perception.

The following example has been selected because of the experimental and iterative approach; the risk perception is strictly connected with the subjectivity of the human element and with the peculiarities of the organizational context whose impact on the risk management effectiveness is often underrated.

CASE STUDY

Italian National Institute of Statistics (ISTAT)

At Istat (Italian National Institute of Statistics), in order to measure risk perception, a questionnaire was submitted to the Top-Management in 2011. The survey was carried out through a web application to about 30 Top Managers and it regarded their perception of the dynamics and severity of risk factors that could affect the activities of single offices or of the entire Institute. Among the possible methodological options evaluated for the topographic analysis of risk perception in ISTAT, the selected questionnaire is based on an international standard (ISO 31000:2009, AS / NZS 4360:1999, A & O) and modeled according to the definitions of an EU framework (PD ISO / IEC Guide 73:2002 and standards FERMA - Federation of European Risk Management Associations).

The Survey is made up of more than 60 questions and focuses on:

1. the level of attention given to risk management when programming and monitoring the main activities of the Directorates and the Institute;

2. the alignment of the current tools used for programming and control with the risk management system;

3. finding, although in simplified form, the factors that may cause injury, distinguishing among internal risks, external risks and cross sectional risks.

The questionnaire uses heterogeneous expressions and different types of responses, in order to keep constant the level of attention of the respondent; and it sometimes uses subjective terms, such as "substantially", "normally", "total", etc. as the survey is used to detect perception.

The survey on risk perception explored the most representative dimensions of managers' organizational behavior when the critical events occur. The information obtained was processed to highlight the incidence of risk factors on planning and organizing the activities of each single structure and of the Institute's goals. For this purpose, ISTAT selected four dimensions, which are most representative of the attitude of managers with respect to critical events. They describe:

1. the perception of risk compared to the activities of the manager: measured by the content of those responses that determine "whether" and "how much" the risk affects the planning and management of the manager's activities within the structure of belonging;

2. the perception of risk compared to the Institute: related to the connection between the existence of risk and the achievement of the strategic objectives of the Institute;

3. the maturity of the control environment headed by the respondent: depending on the individual property to apply the risk management system adopted by the Institute;

4. the maturity of the control environment of the Institute: its value derives from answers to questions that investigate the ability of the Institute to implement and support a system of risk assessment.

Each of these dimensions corresponds to a set of answers, not necessarily placed in sequence, that highlight the character and the criteria used by the Manager when converting the perception of risk into organizational behavior.

Given the variability and subjectivity of risk perception, the results of the analysis of the responses showed a trend in behavior and do not establish a psychological profile or aptitude of the manager.

To facilitate understanding and interpretation of data, the four behavioral dimensions have been represented using a radar chart, in which the value placed on each vertex is the average of the values declared by the manager in the set of questions that express the meaning of the relative dimension. Depending on the risk profile to be analyzed, the results of the survey can be differently interpreted.

Specifically were examined 3 situations:

- The risk perception by management, (highlighting the outliers);

- The risk perception by management, by level of responsibility;

- The risk perception by management, by area of activity (technical and administrative).

Example: The risk perception by management

Figure 1 compares the average rating given by all the executives involved in the survey (brown line) with the profile of the Top management (dashed blue line), including General Director and Chief of Departments, who, in the current theoretical framework, is the level of acceptance of risk consistent with corporate strategies (risk appetite). It also shows outliers, i.e. the maximum values (green bubbles) and minimum values (red bubbles), recorded for each dimension.

Figure 1 – Representation of the average of management profile

The graph shows that the risk is considered an important component in planning activities (Size A), for all groups of respondents considered, even though there is a more favorable approach by apical managers (value of 4 to a maximum of 5) compared to all respondents (value of approximately 3.5).

On the other hand, both groups show a moderate mistrust in considering the risks an essential planning element to achieve the strategic objectives of the Institute (Size B). Again, however, it should be noted an attitude more inclined to consider the risk as an important factor for the Institute's activities, by the Top management, although the gap between the two values is not so large as in the case of A. In addition, for this dimension, even the maximum value recorded (bubble green equal to 3.8 points) is by far divergent from the average. It is worth noting, however, a positive general judgment about the maturity level of the control environment, both the single structure of belonging and for the Institute (Dimensions C and D: values slightly higher 3 out of a possible 5), such that it is allowed a positive development of the risk management system, based on the current organizational configuration. Even for these two dimensions, the orientation of the apical Leadership is demonstrated more favorable than that of all the respondents, although the gap between the two values is more pronounced about the overall vision of the Institute (Size D).

Paragraph 2.2: Process mapping

Focus on: Process mapping methods

CASE STUDIES

The mapping process is a crucial element of the document management system.

To exemplify the process mapping, the methodology applied by the Mexican Institute of Statistics (INEGI) and by the Institute of Statistics of Lithuania are described below.

- INEGI applies the IDEF standard; its characteristic is being modular, analytical and suitable for mapping processes involving a large number of people.
- Statistics Lithuania has focused on the interaction among production and organizational processes and on their impact on the statistical quality in terms of performance analysis; by doing so, this NSO considered the process mapping as the basis for quality management according to the standard ISO:9001**.**

Mexico, The National Institute of Statistics and Geography (INEGI)

The National Institute of Statistics and Geography (INEGI) has been using the Standard 'Integration Definition for Function Modeling' (IDEF) to map processes since 2011. IDEF0 is an engineering technique for performing and managing functional analysis, systems design, needs analysis, and baselines for continuous improvement. The Standard has been issued by the National Institute of Standards and Technology after approval by the United States Department of Commerce.

IDEF0 is used to produce a "function model": a structured representation of the functions, activities or processes within the modeled system or subject area. The IDEF0 methodology includes procedures for developing and critiquing models by a large group of people, as well as integrating support subsystems into an IDEF0 Architecture. The result of applying IDEF0 to a system is a model that consists of a hierarchical series of diagrams, text, and glossary cross-referenced to each other. The two primary modeling components are functions (represented on a diagram by boxes) and the data and objects that inter-relate those functions (represented by arrows). An IDEF0 model is composed of a hierarchical series of diagrams that gradually display increasing levels of detail describing functions and their interfaces within the context of a system. There are three types of diagrams: graphic, text, and glossary. The graphic diagrams define functions and functional relationships via box and arrow syntax and semantics. The text and glossary diagrams provide additional information in support of graphic diagrams.

The graphic diagram is the major component of an IDEF0 model, containing boxes, arrows, box/arrow interconnections and associated relationships. Boxes represent each major function of a subject. These functions are broken down or decomposed into more detailed diagrams, until the subject is described at a level necessary to support the goals of a particular project. The top-level diagram in the model provides the most general or abstract description of the subject represented by the model. This diagram is followed by a series of child diagrams providing more detail about the subject.

Statistics Lithuania (SL)

Process mapping in Statistics Lithuania (SL) has involved core processes, cross-cutting processes, operational activities in detail. As for the methodology followed in process mapping, ISO 9001 standard was used as a basis. Afterwards detailed analysis of performance was made, activities, their sequence and interactions were identified. In fact, ISO-certified Quality management system is based on process mapping.

Moreover, among the main elements of quality management system conforming to ISO there are: definition of the processes, identification of their interactions and sequences; documentation of quality management system: process map, quality policy and quality tasks, quality manual. Quality management system is based on process management, which in turn is based on a detailed process map to which documented rules and guidelines on the various processes are linked. Management rules, structures, processes, activities, responsibilities, sequences and links, and associated documentation, are clearly defined and documented. The process map is a strong tool for standardization and the improvement of quality, and is also used as the backbone of the documentation system.

Processes of Statistics Lithuania: General Scheme

Paragraph 3.2: Risk assessment

Focus on: Risk assessment methodology

The C & Risk Self-Assessment method involves:

• valuators are the same staff that have identified the risks;

• all assessment criteria must be the same by number and type.

In addition, the scale used for the evaluation of the likelihood and impact can be of 3, 5 or 6 levels. The higher the rating scale, the greater the distribution of the occurrences.

It is recommended to evaluate multiple types of impact, both qualitative (reputational) and quantitative (financial, operational). Each rating level must be described as objectively as possible to facilitate the task of the evaluators.

Statistics Austria
Risk indexes

Category	Range	Level
From very unlikely to impossible	0-10%	1
Unlikely or rare	10-20%	2
Possible	20-40%	3
Likely	40-60%	4
Very likely	60-80%	5
From pretty sure to sure	80-100%	6

Category	Impact (Loss)		Level
	Qualitative Interpretation	in Euro	
Very small to immaterial	Just or no substantial negative consequence on the project objectives, easily remedied	until 5.000	1

Small	Little negative impact on the project objectives	> 5.000 until 20.000	2
Remarkable/ tangible	Significantly adverse effect on the project objectives, remediable with additional expenses	> 20.000 until 100.000	3
Very remarkable/ tangible	Significant adverse impact on the project objectives, remediable with great additional expenses	> 100.000 until 200.000	4
Critical	Possible failure of the whole project or one of its fundamental part, remediable with great additional expenses	> 200.000 until 400.000	5
Extremely critical to catastrophic	Fearsome failure of the entire project, remediable with difficulty. Likely reputational damage and legal consequences	> 400.000	6

Italian National Institute of Statistics (ISTAT)

Risk indexes

Illustrative impact scale		
Rating	**Descriptor**	**Definition**
5	Very high	1) Extra expenses or Financial Loss ≥ € 150.000 2) Additional human resources ≥ 30 days FTE. 3) Increasing workload ≥ 50%
4	High	1) Extra expenses or Financial Loss ≥ 100.000 and < 150.000 € 2) Additional human resources ≥ 20 and < 30 days FTE 3) Increasing workload ≥ 30% and < 50%
3	Medium	1) Extra expenses or Financial Loss ≥ 50.000 and < 100.000 € 2) Additional human resources ≥ 10 and < 20 days FTE 3) Increasing workload ≥ 20% and < 30%
2	Low	1) Extra expenses or Financial Loss ≥ 10.000 and < 50.000 €

		2) Additional human resources ≥ 5 and < 10 days FTE 3) Increasing workload ≥ 10% and < 20%
1	Very low	1) Extra expenses or Financial Loss ≥ 5.000 and <10.000 € 2) Additional human resources ≥ 1 and < 5 days FTE 3) Increasing workload ≥ 5% and < 10%

Illustrative likelihood scale		
Rating	**Descriptor**	**Definition**
5	Almost Certain	90% or greater chance of occurrence over life of asset or project
4	Frequent	a) 75% up to 90% chance of occurrence b) Once in one year
3	Likely	a) 50% up to 75% chance of occurrence b) Once in 2 years
2	Possible	a) 25% up 75% chance of occurence b) Once in 3 years
1	Rare	a) 10% up to 25% chance of occurence b) Once in 5 years

Chapter 4: Risk treatment

Section 2. Risk management process | Chapter 7: Risk management information system

Decisions regarding the risks to be treated and the treatment / mitigation methods follow prioritization by top management. The response strategy to risks must include the improvement of statistical quality among the main objectives. To this end, the effectiveness of the implemented actions must be periodically assessed, also in terms of cost / benefit analysis. The treatment responsibilities are assigned and formalized at operational level.

Case Studies

Australian Bureau of Statistics (ABS)

In ABS (Australian Bureau of Statistics), accountability for risk treatment is determined by the risk owner and is often shared across a range of areas that are best placed to implement controls that can reduce the risk which may sit outside the risk owner's immediate span of control. The ABS bases the approach to risk management on the AS/NZS ISO 31000 standard. The ABS's risk appetite only tolerates high or extreme risks when treatment measures are unable to reduce the level of inherent risk to an acceptable level (i.e. Low or Moderate). Any

extreme risk, such as a risk which would seriously threaten the credibility/reputation of the ABS and/or with the potential to result in a parliamentary enquiry, must be brought to the immediate attention of the Executive Leadership Group (ELG). The Senior Management Group (SMG) must be informed of any high risk, including those that may impact/tarnish the reputation of the ABS and/or achievement of program objectives e.g. through sustained media coverage. Treatment measures are essential for high and extreme risks. If strategies to mitigate the risk take time, they must be added as standing Agenda Items to ELG meetings (extreme risks) or SMG meetings (high risks) until the risk is reduced. All low or moderate risks will be managed within the specific area and/or routine procedures. All treatment measures are selected by considering the cost of implementing versus the benefits. In some cases, low and moderate risks might be accepted if the cost of treating the risk outweighs the benefit. Acceptable risks do not require treatment. Unacceptable risks will need to be treated. The Australian Bureau of Statistics (ABS) leads Australia's national statistical service, running hundreds of surveys and publishing thousands of pages of output every year. As with any large and complex organization, problems with processes do arise and the ABS has suffered errors in their data in the past with varying degrees of impact on the public domain. Most errors are detected in-house before publication, however this has at times resulted in intense last-minute work to correct the problems leading to delays in the release of data. Other errors have only been discovered after release, resulting in re-issue of statistical output. As a result of these errors the ABS has endeavored to instigate better Quality management practices through the development and use of the risk mitigation strategy known as ‘Quality gates’. Quality gates are designed to improve the early detection of errors or flaws in production processes.

Statistics Lithuania (SL)

In Statistics Lithuania (SL), according to approved descriptions of procedures, if any risky activity is identified, management is informed and improvement actions are defined and performed by responsible staff. On the base of the situation, improvement actions are implemented as soon as possible or deployed into the improvement action plan.

Process managers, appointed by the order of Director General of Statistics Lithuania, analyze identified risks, determine their causes and possible ways of their elimination, appoint staff responsible for improvements and monitor the effectiveness of improvement actions implemented. The priorities for risk treatment are set by Top management, according to the risk measurement results. The priority is given to the activities, which are the most risky for the process and process results. Usually, process managers are responsible for the risk treatment, if the risk was identified in their process. They analyze the problems, determine their causes and possible ways of their elimination, appoint staff responsible for improvements and monitor the effectiveness of improvement actions implemented.

Especially with reference to the preparation proposals for treatment, in concrete statistical areas cross-institutional commissions and working groups (e. g. group of experts in national accounts) established on the initiative of SL, play important role.

Statistics Sweden

In Statistics Sweden, risk treatment is documented in connection to the risk, specifying the treatment itself and the person responsible for carrying out the action (always a manager at department or unit level, in exceptions it can be the Director general). It also has to have a starting and finishing point. If treatment is more or less constant over time the end date is set to last of December and the action is carried over to the next year as are risks that have not been eliminated. Risks and treatments are included in the regular follow up of operations after each 4 month period with focus on effectiveness and deviations from plan. All risks that are critical require treatment unless they are impossible to prevent and/or too costly to mitigate. High value risks shall, as a rule, result in activities to mitigate the risk, either prevent it from happening or reduce the consequences. Under corporate risks are included the risks managed by the security organization. These risks have treatments that are different in characteristics and more of permanent solutions like insurance policies, contingency plans, fixed installations, firewalls and so on. Also some compliance risks are included here. They are documented in a separate module of the system since they have other needs for follow up purposes than operational risks.

All critical risks are to have treatment though and many of the medium and low risks also have treatments.

On corporate level treatments are in general delegated to the director of one or more departments and added to their risk lists. The director's comment on deviations and effectiveness and the comments are compiled by the risk manager who may suggest changes in risk values based on this. The updated risk report for the agency is presented to the DG, the deputy DG, the Director of the Director General's Office, the head of internal audit and the Head of Security by the risk manager and after discussions any adjustments are made. Once a year, after the second four month period follow up, the risk report is signed by the DG and a preliminary risk list for the coming year is set up based on the preliminary operational plan for the next year (operational risks at agency level). At the same time the risk list for corporate risks (the internal control plan) is signed by the DG.

The directors of each department are responsible for all risks within their department but can delegate carrying out treatment to unit managers. The units' risks shall be listed at department level though, since the central follow up only covers the department level and all operational risk are to be put forward to the Director general and be more easily analyzed by the risk manager. This means that the units' risk lists are generated from the departments' risk lists and they cannot add risks themselves at unit level according to the routine currently used.

Chapter 7: Risk management information system

Chapter 4: Risk treatment	Section 2. Risk management process	Chapter 8: Risk management maturity model	

Focus on: The risk management information system

Efficient IT tool is crucial for an effective risk management. The information system must be modulated and integrated with the quality management and performance management system.

CASE STUDIES:

Statistics Austria

In Statistics Austria a specific software tool for RM and the Internal Control System (named OBSERVAR) is in place. In Statistics Austria the OBSERVAR system provides:

- modular architecture (risk management dealing with corporation-wide risks (strategic level), Internal Control System dealing with risk in operational processes, Compliance Management System dealing with compliance risks;

- the whole RM process covered;

- specialized, user-friendly and scalable software product covering over 25 modules for EGRC (Enterprise Governance, Risk and Compliance) and MIS (Management Information System) solutions;

- web-based, integration of RM, ICS and CMS;

- individually customizable system;

- prioritization approach, focus on the real important issues;

- using the tool including tailor-made risk catalogues and questionnaire forms.

Risk treatment actions are monitored by using OBSERVAR. Staff members who are responsible for risk treatment actions have to report periodically (e.g. monthly, quarterly, yearly) on the implementation/execution of actions, adherence to guidelines respectively, within OBSERVAR. The Internal Audit also uses OBSERVAR for internal audits. Risk catalogue steps (within

OBSERVAR) are as follows: 1. Qualitative assessment (risk identification and risk analysis), 2. Prioritization, 3. Quantitative assessment (risk measurement). In the OBSERVAR catalogue risks are subdivided into 1. Leading Processes, 2. Core Processes, 3. Supporting Processes, 4. External Influences and Stakeholders. Statistical as well as organizational risks are included in Statistics Austria risk catalogue: both categories are integrated within the RM software tool.

Statistics Lithuania (SL)

The monitoring and control mechanism is performed via electronic document management system named SODAS and later the implementation of the actions is reported to the senior management. When risky activity is identified, the situation's causes are identified and analyzed via interviewing related staff, examination data from various systems (e.g. electronic document management systems SODAS, non-conformities and IT incidents registration system, time use recording system, providing detailed information on time used for different processes, and a specific system for recording quality characteristics of statistical surveys), performing causal-effect analysis or detailed statistical analysis. The monitoring and control mechanism is performed via electronic document management system SODAS.

The main features of the system are: effective and systematic documents management; fast and time cost saving sharing of documents; assurance of authenticity and reliability of stored documents; expeditious allocation of tasks and assignments, adequate monitoring of their implementation at all levels. The drawbacks and risky activities are registered online in special non-conformities recording system, which not only allows recording drawbacks and risky activities in a user friendly way, but also warns other staff members against possible threats.

Every staff member can inform process managers about the drawbacks and risks identified in their process via this system. It automatically informs Methodology and Quality Division, responsible for the management of the system, about new record. The system is also used for the documentation of the recorded risk analysis results and progress made in implementation of risk treatment actions.

From *Statistics Lithuania Annual Report 2010*: "As regards the realization of the vision of a paperless office, an electronic document management system Sodas was implemented at Statistics Lithuania at the end of 2009 and put into operation in 2010. The system – that has replaced the previously used system KONTORA – enables an efficient, automated and standardized management of institution's documents, control over tasks and assignments".

Statistics Sweden

All operational planning on agency/department/unit level, along with operational risks, are documented in a tool named Stratsys that is an operational support software used in the various phases of the strategic planning, implementation, analysis, operational planning, reporting. All managers also report within the system. The internal control plan and the reports from internal quality audits are documented in the system too (certified according to ISO 20 252). It may include more things in the future. All employees have viewing rights to the agency's operational plan and to their own department's action plan and all its units' action plans. All managers have viewing access to everything, except quality audit reports concerning other units/departments than their own, and writing/creating permissions on everything on their unit/department level. Quality audits can be accessed by the auditors and the specific unit and department managers concerned. There are 3 business controllers at the Director General's Office who have admin permissions.

Most of the set up in the system is made in house by the administrator, but a contract for consultant aid from the provider is available if needed. All data is saved in a database on servers managed by the provider or its sub-contractors. The information stored is not considered to be sensitive and according to the contract the servers are guaranteed to be located within Sweden. When the contract is terminated the database shall be returned to Statistics Sweden.

Especially risks, but also plans concerning core activities are carried over between years. For the risks, values and comments for previous periods and years can be seen in the screen. Reports can easily be downloaded in different formats.

Chapter 8: Risk management maturity model

Chapter 7: Risk management information system	Section 2. Risk management process	Chapter 9: Lessons learned

Focus on: Risk management maturity model

In order to pursue the continuous improvement of the risk management system, the most advanced statistical organizations, have introduced methods to analyze the maturity of their risk management models, defining assessment grids, composed of variables representing the main components of the system itself.

CASE STUDIES:

UK, Office for National Statistics (ONS)

ONS has developed a model to analyze and measure the level of its maturity risk management system significantly advanced.

It consists of 5 levels of maturity, each of them is described by the following variables:

1. Knowledge & Skills;

2. Behaviors;

3. Metrics.

Level	Knowledge and Skills	Behaviors may include…	Metrics – for measuring progress
LEVEL 1 Awareness	Staff, managers and leaders are aware that risk management is something that should be done, but do not understand why or how. Have received but not fully read and understood communications material on risk.	Staff, managers and leaders are not yet taking action to identify and control risk across the organization or in high risk areas. Training gaps are known and being addressed. Staff has to decide for themselves what level of risk taking is acceptable.	1. No risk champions or other indicators of a risk management culture. May have heard of the concept, or be able to identify with it, probably in the context of project management. Risk registers may have been produced, but will have been done for them, by 'experts' or as a one-off. 2. It may have a coordinator who is a 'voice in the wilderness'. 3. Risk appetite not defined - excessive risk aversion in some places and excessive risk taking in other places. 4. Risks not shared with Director unless there is a crisis.
LEVEL 2 - Basic Understanding	Risks often not aligned to the objectives of the business area or Directorate. Awareness of the need for good risk management – but may not have fully bought in to the concept. Understanding the theory and processes behind formal risk management, but it may think of risk as a compliance tool, not as a tool for real business improvement. Understanding activity to date, including senior management, strategic risks and existence of risk policy statement, risk framework/guidance and training programmes Understanding who to contact for further support. Training is sought by, and for, key people. Understanding some of the key risks to the Organization and to their area. Understanding there are formal procedures that need to be implemented, but not yet implemented them all	Possible attendance at introductory risk training courses and key staff will probably have read ONS risk policy statement or practical guidance. If applied, risk management has been a time-consuming, mechanistic process. Often involves a junior team member creating a risk on the risk database, which is collecting dust and rarely updated. Risks often materialize which should have been foreseen and recorded on the risk register. Staff has participated in collating or drafting reports (e.g. Strategic Risks). Senior management arenot yet persuaded of the benefits, or rarely lead by example. Staff very unwilling to bring forward and expose problems and vulnerabilities unless instructed to. Perceived culture of 'shooting the messenger'. Risk mitigation sometimes hampered by a lack of clarity in the articulation of individual risks. Blame culture apparent, with people too scared to say 'no'. Staff has to decide for themselves what level of risk taking is acceptable leading to excessive risk aversion in some places and excessive risk taking in other places.	1. Normally have risks recorded at divisional and probably at directorate levels, plus at least 50% of directorates have them. 2. Risk registers will typically be mechanistic and compliance-focused documents, which are updated on request of overseers (e.g. the center). 3. Risk not normally a standing item at management, project, programmes or divisional board meetings. 4. Organizations will have a nominated risk champion. Organizations will have risk coordinator, who is departmental 'expert'. 5. Some staff have been on Risk management training. Corporate center normally called on to support management, units, projects, programmes or departmental boards within the directorate. 6. No evidence of a systematic approach to escalating risks from team/divisional levels. Risks escalated from the team/divisional levels on an exceptional basis for example, as the result of a crisis or externally generated event such as media interest. 7. Strategic and Directorate risks have either not reduced in severity over the last two quarters or reductions in severity cannot be traced to the actions taken by the risk owner / business. 8. Risks in the database are not clearly articulated in all cases and / or risk owners have not been allocated. 9. Mitigating Action and Contingency plans do not exist where they are needed. 10. Risk appetite not defined.

Level	Knowledge and Skills	Behaviors may include…	Metrics – for measuring progress
LEVEL 3 Application	Staff, managers and leaders know how to identify, assess, address, monitor and report risk in a consistent, structured manner, in line with Organizational guidance. Real ownership for risk and actions exists. Management at all levels in the organization have a clear understanding of how risk should be managed and they act in accordance with this. Management at all levels have visibility of the work they oversee, and have the skills to interpret and challenge what they see in order to expose risk. Key staff are aware of the need to manage risks with partners and have the skills and knowledge needed to manage these risks. All information asset owners have received basic training and understand: • The nature, value and benefits of the information assets they own; • the principles of risk management; and • the risks inherent in the data and systems they own. Information Asset Owners know who their risk coordinators are, and vice versa, and the IAOs know how to escalate IA risks within their business areas.	Risk workshops have been held to kick start the process. Staff are implementing basic risk management processes. Staff are using basic risk information to inform decision-making, e.g. information asset owners will typically ask why information is being requested and query which elements of the data they hold needs to be passed on. Information that is passed on will be done as safely as possible. Losses will be reduced, but not eradicated. SCS, G6 and G7 act as role models and lead on risk management. Heads of Directorate/Unit/Branch/ project/programme regularly ask: • Have you been to see for yourself how this risk is managed? • Has the risk severity changed in the last week? • What level of severity are you seeking to manage this risk down to? • What has been done about this risk in the last week? • Have you discussed this risk with your Director? • Managers: • Send a message to staff that they can be confident escalated risks will be acted upon. • Ensure risks are updated regularly, including information asset risks they are responsible for. • Identify and manage risks that cut across delivery silos. • Discuss risk each week with their staff and up the line, monitor actions weekly and check they are sufficient. • Communicate downwards what the top risks are. o Escalate risks from Divisional level • Link risk to discussions on finance – and stop/sequence projects to reduce risk as well as to cope with budget. • Demonstrate we really have an appetite for setting priorities – and stopping / slowing down the non priority areas. • Learn about good risk management from other organizations. • Send out a message that we are still ambitious but need to reduce our risk exposure. • Ensure we do not blame people for escalating risk. • Check regularly that processes are well controlled. Proactive "can do" attitude to problem solving. Leaders, managers and staff learning the lessons from past mistakes.	**We know what our top risks are, especially those affecting public protection and those escalated from the front line:** 1. Risk exist on the database at divisional, directorate and 95% of teams have recorded risks on the database. All divisions with responsibility for Agencies either have identified and recorded risks which take account of their risks shared with these bodies. This will include information asset risk registers. Risks clearly articulated in all cases 2. Risk registers, including information asset risks, are regularly updated and used at management meetings throughout the organization. 3. A process is universally and visibly in operation for escalating risks from the team level – through divisions, public bodies, suppliers, contractors, partners, projects and programmes, to directorate level and strategic level. Such risks can be tracked through the risk database. 4. Risks to data/reputation are foreseen, included on the risk database, and the extent of the risk is clearly articulated. The business is alert to risks, including those in low priority areas, e.g. such as small information systems. **Good risk behaviors – as well as good process:** 5. Risk is a standing item at management meetings throughout the organization. Managers regularly discuss risk with their staff – what the key risks are, what has changed since last week or month, how mitigating actions are being progressed. 6. Leaders and managers are visible, approachable and actively encourage staff to escalate risk. No one is blamed for escalating a risk and good risk management is recognized positively in Performance Agreement assessments. But staff are held to account for failing to escalate a risk or to take mitigating actions. 7. There is a risk champion and they support staff, actively promote good risk management behaviors and compliance with corporate standards throughout the business. 8. Key staff (project managers, SROs, business and strategic support staff) have been trained in Risk management to the appropriate level and can explain the benefits to other staff, which they do on a regular basis. Likewise, Information Asset Owners have all been trained in Risk management and can identify and escalate risks to their assets where necessary. **Planning for risks over the long term as well as the short term:** 9. All black and red risks have contingency plans, where appropriate. 10. Senior Board has been alerted to the risks including those identified on risk registers. Risks are discussed regularly (weekly) with Directors and are identified in submissions. 11. The business has defined its risk appetite, including those relating to information asset risks, and plans are in place to achieve this. 12. Risks that are three to five years away are identified and mitigating actions or contingency plans are in place. **Managing process, and information asset, risks as well as project risks and risks:** 13. Risks on the database identify process risks, especially (but not only) where: • the process is poorly defined or compliance is infrequently checked; • gaps exist between adjoining processes; • Data gets lost in the system; • the ownership of a process is not clear or is in dispute; • the process has been improved, but a legacy of old cases remains; • there is a backlog of casework; and • there are interactions between processes that are owned by different people. 14. **Information asset owners are aware of the criticality of their information assets and the attendant legal requirements and are beginning to follow the published governance processes and guidance. Business areas can show the following:** • all new IS are subject to accreditation, as a matter of course; • where appropriate, Privacy Impact Assessments are used and effective contract mechanisms are used to apply IA through life, and information risks have been identified for all accredited in-service Information Systems.)

Level	Knowledge and Skills	Behaviors may include…	Metrics – for measuring progress
LEVEL 4 Embedding	In addition to the above, staff: Effectively manage those risks owned by or shared with partners, and can confidently press this point with partners. Ensure the Department communicates effectively on significant risks to the public which arise in their area. Formally review the effectiveness of all aspects of their Risk management activity. Senior management, including the Board, are actively engaged in broadening their horizons on risk through participation in internal events and training. The Organization is increasingly seen as an example of best practice across government. All information asset owners and managers are aware of the importance of managing information assets effectively and appreciate the benefits of doing so and the risks if they get it wrong.	Open communication internally on risk. Assessments of the effectiveness of risk management being undertaken. Longer term risks are integrated into the strategy and business planning functions. Business planners are beginning to think about whether enough resource has been allocated to the potential risks that may materialize during the planning cycle and allot money accordingly. Our people and workstreams are increasingly 'plugged in' to our partners. Share risk information with delivery and other business partners. Where risks are owned by others we are ready to challenge if appropriate and if we perceive there are weaknesses in their risk management. Risk workshops shared with partners. We are beginning to become more comfortable sharing risks with partners, when in the past we wouldn't. Discussions about risk are becoming increasingly more mature and widespread (and this is evidenced in minutes and notes). These discussions underpin the escalation process and form part of both the informal and formal escalation process. Executive Boards can be seen to be giving direction in the oversight and management of risk. An understanding of upside risk is beginning to be shown. Staff becoming noticeably more aware of the importance of management information and how to exploit it.	As LEVEL 3 above, but risk is becoming mainstreamed and less noticeable as a separate activity – can show evidence of this across all the business – quality of risk dialogue critical. Key elements from level 3 that are strengthened here are: • discussing, handling and escalation (metric 3 below; strengthening metric 2, 3 and 5 above); • strategic risks (metric4 below, strengthening metric 12 above); and • Process risk management (metric 6 below, strengthening metric 13 above). We know what our top risks are 1. We also share or discuss our critical risks amongst ourselves (cross-cutting risks) and in our key partnerships (OGDs; 3rd party contractors and suppliers), where appropriate, and we can evidence this. [In practice, this means business areas can evidence that in their top processes, (where shared, see metric 6 below); their top programmes and projects (as agreed between us and the business areas) and any other significant initiative or operational undertakings (not covered above, but agreed), assurance can be given that the top risks are discussed or shared as appropriate, supported by mapped and repeatable processes.] Good risk behaviors – as well as good process: 2. Risk management has been evaluated and judged to be effective and this can be shown through assurance and governance reporting. [In practice, this means that business can show through own governance mechanisms and/or external assurances. 3. Continuing embedment of the risk escalation process. [In practice this means that all the parts of the organization can show that there is a robust network and hierarchy for escalating risk with the 'dialogue' up and down the line as the linchpin of this framework i.e. discussions on risk take place, as regularly as the need dictates, throughout most of the organization. Escalated and de-escalated risks will be found at all levels. There is no one single model that is right, though evidence will be there through analysis/use of management info. An effective system will typically have evidence of risk discussions in the minutes and be backed up by audit returns showing the movements of risk through a business areas hierarchy.] Planning for risks over the long term as well as the short term: 4. Evidence of risk being taken account of in the business planning and resource allocation/budget setting process throughout the planning period. [Assessed as part of the business planning cycle, each business area can point to clear evidence that resources have been allocated to significant risks i.e. Risk management activity can be taken account of in the business and financial priorities for that coming year.] 5. Business Continuity Planning is in place, as required, so that: • All units, directorates and groups – where appropriate - have workable, up to date and tested BC plans in place; and • The Divisional BC Plan is on track against the prescribed timetable towards BS 25999. (This sub-metric not for individual business areas to report on, but measured centrally). Managing process, and information asset, risks as well as project risks and risks to organizational Units: 6. Where not assessed at Metric 1 above, process risks have been identified and mitigating actions are in place. [In practice this means that business areas will be expected to outline their key business processes and the attendant risks – PDU will assess if all significant threats have been identified and if they have, whether they are being adequately mitigated.] 7. All information systems that are critical to the business have been identified and subjected to Accreditation and the organization has effective information risk management processes in place to manage the residual risks* and the related, systemic IA risks. * NB In this instance, this has been taken to mean the residual risks identified by the Accreditation process. (Level 3 HMG IA Model) 8. Health and Safety improvements are on track against the Health and Safety improvement programme. (This metric for individual business areas to be marked on, but via the HO Health and Safety Sub-Committee, not via risk coordinators). 9. Compliance with information security management systems requirements - BS 27001 (Not formal accreditation).

Level	Knowledge and Skills	Behaviors may include…	Metrics - for measuring progress
LEVEL 5 Excellence	In addition to the above, staff: Embedded and long-term partnership working regimes and relationships in evidence. Use risk management to spot opportunities as well as threats. Senior management are actively engaged in broadening their horizons on risk through participation in external events. Have key staff who probably, either have professional qualifications in risk management or who have track record for proactivity in this area and an appetite for ongoing learning. These people are listened to. High profile individuals, such as DGs, noted for speaking at seminars on risk. Key risk coordinators or managers have skills to lecture and train other staff. The Organization is recognized as a centre of excellence and expertise across government. All staff at all levels is aware of the importance of managing information assets effectively and appreciates the benefits of doing so and the risks if they get it wrong.	Innovative and creative application of risk theory to everyday operations. Appreciate aspects of risk management that are not related to their day-to-day activities. Open communication internally on risk with little evidence of blame culture from raising risk issues. Regular 'stock takes' as to the effectiveness of their own risk management. Clearly recognize personal incentives for managing risk better. "It's my job to expose the errors". Staff at all levels act as a role model. Longer term risks are integrated into the strategy and business planning functions including policy making. Effective and regular public communications on potential threats. Excellent relationships with the most significant/strategic partners and stakeholders. Identification and prioritization of upside risk to actively pursue opportunities. Personal performance objectives include targets for risk management; performance appraisal and promotions include aspects related to risk management. Calculated risk taking the norm. Everyone is responsible for their own actions and their accountabilities are clearly understood. Can be used to 'showcase' risk as role models. Recognized by other organizations as leaders in risk management. Lecture and train other staff. Staff attitudes and behaviours towards assuring information are aligned to the needs of the business. Information is both 'exploited' and safeguarded, in equal measure, at all levels of the business.	*As LEVEL 4 above, but risk is mainstreamed and less noticeable as a separate activity – can show evidence of this across all the business –can point to evidence that they are 'not often 'surprised' as an organization and when this does occur, the threats are normally external in origin.:* **We know what our top risks are, especially those affecting public protection and those escalated from the front line:** 1. Ministers actively engaged in the process of risk identification and setting the organization's Risk appetite. 2. The Organization responds quickly and effectively to unanticipated risks. 3. For all key information systems, the residual risks that are to be tolerated are quantified and the Board is aware of the level of residual information asset risk being carried. **(Level 4 HMG IA Model)** **Good risk behaviours – as well as good process:** 4. Stories of good risk management are in common currency. 5. Sustained monthly discussions on risk are long time established and routine throughout the organization. 6. Staff at all levels act as good role models with evidence of staff whom have identified risks being rewarded/recognized positively. **Planning for risks over the long term as well as the short term:** 7. Evidence of identified strategic risks being taken account of in, and giving direction to, the business planning and policy making mechanisms. 8. Risk exposure is in line with the leadership's appetite. **Managing process, and information asset, risks as well as programme/project risks and risks:** 9. Process risks have been identified and mitigating actions are in place. 10. For all IS, the residual risks that are to be tolerated are quantified and The Board is aware of the total level of information risk and systemic IA risk the organization is carrying. **(Level 5 HMG IA Model)**

Italian National Institute of Statistics (ISTAT)

ISTAT has developed a model that considers all components of the framework and risk management process described in the guidelines; each component is articulated on 4 levels that represent the specific maturity level, based on the statements deriving from the analysis of the practices collected through the surveys and from the comparison among the most relevant international risk management standards.

Some descriptors have been made up for the purpose of illustrating in greater detail the different topics connected to the core areas. These allow the items to be allocated among four maturity levels characterized by reference to attributes / performance indicators, consisting of potential / typical features.

The grid highlights, for each descriptor reflecting the extent to which each risk management competency or capability is defined and controlled, three elements or Reading-keys used both in the survey design and in the processing phase:

1. *Risk rationalities (processes)* that corresponds to the organizations' efforts to translate uncertainty into manageable and communicable conceptualization of risks, and the definitions of activities and tasks to deal with them.
2. *Uncertainty experts (roles)* that refers to the actors - their experience, background and interactions -, organizational units or structures to which the organization assigns the responsibility for risk management.
3. *Technologies (support)* that denotes the complex sets of practices, procedures and tools enacted to accomplish the management and control of risks.

Coherently with this framework, core areas / items are graded using a four-point scale, designed taking into account that each maturity level is a defined position in an achievement hierarchy establishing the attainment of certain risk management capabilities.

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	MULTIDIMENSIONAL ANALYSIS AND READING GRID: RM MATURITY			
			STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Risk Framework	*Attitude towards uncertainties (Risk Philosophy)*	No proactive though: the organisation is reacting to situations and risk issues after they occur and it is not able to distinguish between positive and negative risk	Risk is considered a static phenomenon instead of a dynamic one. Risk approch mainly focuses on past events	Opportunistic approach: a common and consistent definition of risk exists and is applied throghout the organisation, but risk approch mainly focuses on avoiding unexpected large loss events	Open and proactive approach to risk that considers both threat and opportunity. Risk based approach to achieve goals is used at all levels
		Mandate	The board does not feel the need for managing risk	Following an external demand (legislative or regulatory, government pressure, stakeholders' influence)	By an administrative or political board	Both by a strong administrative and political board
		Risk strategy and policy	The need for a risk strategy and related management policy has not been identified and accepted	A corporate risk strategy and policy has been drawn up and formally documented. It is interpreted as compliance. The need for formalizing risk tolerance and appetite is not understood	A corporate risk strategy and policy is organisation-wide documented, communicated and followed. Levels of acceptable risks are established for key and relevant areas	A risk policy states in a quantitative and multi-disciplinary way the level of risk acceptable to all organisational departments and units
		Approach to RM	No RM approach to dealing with uncertainties	Project-approach mainly based on previous organizational practices, methods, knowledge and routines	International standards and models	Customized / ad hoc model
		Management leadership and committment	Management is not committed to establishing risk management and has not assumed a leadership role in implementing it	Some risk management initiatives are supported by top management on ad hoc basis across the organisation	Senior managers take the lead to ensure that approaches for addressing risks are being developed and implemented in all key and relevant areas	The leadership for risk management is embedded at all levels of the organization. RM is a formal and regular senior management activity. Senior management also oversees all the risk management framework and is visible involved in risk management practices and initiatives
	Environmental analysis	*Internal and external context analysis*	A detection of internal (governance, organizational structure; policies, objectives, strategies; resources and knowledge; etc.) and the external RM context (regulatory / financial, technological, economic / competitive environment; key drivers and trends having impact on the organization's objectives; etc.) has been neither carried out nor planned	An internal and external context analysis has been planned or kicked-off in a fragmented / experimental or unstructured way by a core group of managers	A consultative team approach has been implemented to define the internal and external context, primary for the purpose of ensuring risks in key and relevant areas are identified effectively	The organization uses state-of-the-art methodologies for environmental scanning and accurately and periodically updates and documents the internal and external context for ensuring different views are appropriately considered in evaluating risks, for appropriate change management during risk treatment, to review policy to reflect changes in the internal and external environment

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Environmental analysis	*Process Mapping*	An analysis concerning the organizational processes has been neither carried out nor planned	Some stand-alone processes have been identified at macro-level: their frame or boundaries (start / inputs and end / outputs) have been determined	A process analysis increasingly involves all key activities and relevant areas, while distinguishing among core and cross-cutting, down to operational activities in detail	All processes are broken down, analyzed and represented (while identifying objectives, inputs, information flows, roles and accountabilities, sequences and links among them / key cross-organizational dependencies and significant control nodes, outputs), combining different methods (e.g. Cause & Effect Diagram, Brainstorming, Job Shadowing , ICOR, Process Flowcharting, etc.)
		Staff risk perception evaluation	Never evaluated	A pilot evaluation is carried out with reference to a core group of people conscious of the need to manage risks and also having basic skills and knowledge	Evaluation is carried out regularly with reference to resources working in all key and relevant areas where risk management is being developed and implemented	Evaluation is carried out by expert people, regularly, at all staff levels and through advanced mixed-method approaches (e.g. questionnaires, focus groups, one-to-one focused interviews, etc.)
	Risk assessment	*Risk Identification*	No attempt is made to identify risks or to develop mitigation or contingency plans	People with appropriate knowledge have involved in identifying possible risks. Some stand-alone risk processes have been identified by central office or senior management only (Top-Down approach). The organization initiates attempts to identify and document risks and sometimes begin structuring mitigation activities	The executive and board consider risks elating to the achievement of key organisational goals and objectives. The organisation has applied a set of risk identification tools and techniques, usually of a qualitative nature. Information has been gathered from different sources to identify risks that result in key and relevant areas and events are associated with their process source	Risks are identified throughout the organization at any level and in consultation with external stakeholders (Bottom-up / Mixed approach). The organisation assesses the effectiveness of the risk identification process, identifies the drivers for identified risks and applies a set of advanced quantitative and qualitative methods. Research is performed to understand common NSO-specific risks. Risk identification is extended to all partners
		Risk Analysis & Measurement	Risk registers may have been produced by "experts" or as a one-off	Risk registers will tipically be mechanistic and compliance-focussed documents, which are up-dated on request of overseers	Risk Assessment is granular. Risk registers provide key-inputs for sharing and discuss top-risks and cross-cutting risks.	Escalated and de-esclated risks will be found at all levels. For all key information systems, the residual risks that are tolerated are quantified and the Board is aware of the level of residual information asset being carried
		Risk Treatment	Mitigation Actions and Contingency plans do not exist where they are needed	Mitigation Actions/Contingency plans exist only for some risks	Risk Treatment measures are periodically monitored and corrective plans exist for significant risks	Each business area can point to clear evidence that resources have been allocated to significant risks. All units, directorate and groups have workable, up to date and tested business continuity plans.
	Controls	*Risk Based Control & Audit*	There are no criteria in place to evaluate wheter risk management practices are efficient and effective	Controls are usde on ad hoc basis to respond to new risks and a changing environment	Ongoing oversight and monitoring of the risk function occurs on a regular bais to identify opportunities for improvement in the framework and processes of the entity. Regular reviews of compliance with the risk framework are undertaken by internal audit	Review and monitoring plans are indipendently monitored to determine progress and outcomes. Processes are assessed on a regular basis by an independent party

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Risk dissemination policy	*Outcomes and deliverables*	No evidence of improved outcomes	There is limited evidence that risk management is being effective in at least most relevant areas	There is evidence that risk management is supporting delivery of key outcomes in all relevant and key areas	There is clear evidence of very significantly improved delivery of all outcomes and showing positive and sustained improvement: RM arrangements clearly acting as a driver for change and linked to plans and planning cycles
		Impact on work and personnel	No impact on work and staff	Low impact on top / senior management culture with reference to awareness of priorities and attention to results	Middle and Low Management approach through which strategic goals are pursued is being changed. Human resources management policies related to key and relevant areas have improved	Full understanding of performance impacting factors within the organisation. Communication processes inside the organisation have significantly improved
		Benefits on the organization as a whole	No impact on the organisation	Some improvement of effectiveness related to some stand-alone processes	Key activities and quality of services in all relevant areas have improved and duplication in both activities and services have been removed	All ineffective / duplicated services and activities have been removed. All project and activity effectiveness and quality has improved.Strong sense of teamwork exists across the organization
	RM system integration	*Linkage to corporate and operational planning*	Programs operate independently and have no common framework, causing overlapping activities and inconsistencies	Risk Management is not linked with the strategic/operational planning process	Risk management is done as part of strategic/operational planning at the functional level, but non on a consistent basis throughout the organization	Risk Management is an integral part of strategic and business planning, at corporate and operational level. Risks are identified in the strategic and operational plans and mitigation plans are developed. Strategic and operational risks are aligned
	RM system integration	*Use of RM information in decision making*	Risk management information is not used in the decision making process	Risk management information is used in a fragmented and not regularly way or to fulfil a legal obligation with reference to specific processes	Information derived from the risk management process is used to assess the level of strategic goal attainment by business units, managers and employees dealing with all and relevant areas	Risk management information is used in a structured and regularly way to review corporate strategic priorities, decide on allocation of financial, HR and tangible assets, to concentrate relevant stakeholders' and employees' attention on particular key messages giving rise to change in their behaviors
		Integration with quality framework	No connection	Programs for compliance, quality management, process improvement and RM still operate independently and have no common framework, causing overlapping activities and inconsistencies	The functions are alligned but not completely integrated	The functions are completely integrated
		Connection with performance assessment system	No connection: performance in managing risks is not a factor considered in organisation / individual assessment system	Performance in managing risks is a residual factor considered in rewards and sanctions system with reference to a core group of people. Consistent organisational tracking of the performance is missing	Risk management is an objective in all senior management's performance agreements and in middle management's performance agreement in charge of key and relevant activities: roles in relation to risk are articulated in in the individual DPAs (Development and Performance Agreements). Sanctions are in place for knowingly ignoring risks	The personal performance review include assessment of risk management skills for all staff. Recognition and reward systems encourage employees to manage risks and take advantage of opportunities. Connection with both organization and individual performance assessment system is in place

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Monitoring & Review	*RM system Monitoring & Review*	A risk management system is not in place	Periodic review to ensure that risk management system is effective and continue to support organizational performance is not envisaged. Marginal and/or pilot RM implementation project monitoring activities may be carried out in a fragmented and unstructured way	A framework to measure progress in implementing risk management is in place (progress against and deviation from the RM policy and plan; review to ensure that policy and plan are still appropriate; RM process review), but performance indicators are not well refined and/or information collected to measure achieved is not available on a trend basis	A periodical and structured RM system review is carried out. The RM framework and processes are aligned to the objectives/priorities of the organisation, changes to the context are promptly addressed, resources are adequate and people have enough RM skills. Performance indicators and benchmars to measure outcomes are updated on an ongoing basis, measured regularly and results are tracked over time
UNCERTAINTY EXPERTS: PEOPLE, ROLES, STRUCTURES AND INTERACTIONS	Organizational chart	*RM function in the organization*	The board does not feel the need to manage risk and the related function is not included in the organisation chart	Top management / senior managers take the lead to ensure that a not-formalised core group of people have the basic knowledge to manage risk. An experimental / pilot function is being introduced	RM function is formalised within the organisation and a specific RM unit may be envisaged in the organisation chart	An independent operational risk management function exists. Staff responsible for implementing the entity's risk management framework are dedicated resources to the risk management function, with a well developed understanding of the entity and its operations
	Culture	*RM internal culture*	The focus is primarily on responding to crises and is reactive rather than proactive. Prevails a culture resistant to change witjh emphasis on protecting physical and financial assets	People tend to be risk adverse: a caution approach is taken to risk management overall (risk avoidance)	RM is done proactively and a culture of control is being disseminated	Individual and organisational expectations for RM are synchronised. The focus is on opportunities, not just risk avoidance. The organisation fosters a culture of continuous learning and participation and people are encourage to be innovative. Staff is highly committed to the success of the organisation
		Linkage to ethics and value	No ethics policy or guidelines in place. No clear statements of shared values or principles or attention to legal issues	Organisation may have an ethics statement but philosophy reflects legal and political considerations (compliance approach) and any written policies are applied inconsistently	Ethics and values principles/guidelines and legal/political considerations are understood by staff and risk management approach is aligned with them	Ethics and values are consistently reflected in RM organisation practices and actions. Regular surveys on this topic consider risk. An organisational climate of nmutual trust exists at all levels
	Stakeholders	*Internal stakeholders involvement in RM process*	No formal communication have been channels have been set up to report on risk issues.	Risk management information is shared within organisational units. Managers tend to work independently with some interaction	Risk management information is shared across organizational units and employess are encoruaged to discuss best practices and lessons learned within the organization	Best practices are shared between organizational units in a structure manner. A wide range of mediums are used to involvr all employess in managing risk
		External stakeholders involvement	Stakeholders have been identified, but there is no formal communication or understanding of theri information needs or risk tolerances	Ad hoc ommunication with stakeholders occurs and there is some understanding of theri information needs and risk tolerance	A process framework have been implemented to regularly communicate with stakeholders . Information is shared openly with stakeholders on a fully transaprent basis	The organization regularly report its strategic objectives, risks, tactics for managing risks and its performance on managing risks. Feedback from stakeholders is obtained and incorporated in the risk planning cycle.

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
UNCERTAINTY EXPERTS: PEOPLE, ROLES, STRUCTURES AND INTERACTIONS	**Roles & accountabilities in managing risks**	*Roles and responsibilities of senior management*	Corporate culture has no risk management accountability with process owners not defined	Specialists are responsible for managing risks and taking action in their area. Senior managers identify and respond to risks on an ad hoc basis	A formal process is in place whereby senior management assume responsibility for the overview risk management practices. Risks are identified by senior management on a collective basis, and plans of action developed	Risk management responsibilities are formally stated in accountability agreements and/or governance documents and are communicated, applied and monitored at all levels of organizations
		Staff accountability	Staff culture has no risk management accountability	Staff culture has little risk management accountability with process owners not well defined or communicated	Authorities, roles, responsibilities are identified: risk ownnership is clearly defined and well communicated to all staff	The management of risk is everyone's responsibility
	Human Resources	*Human resource adequacy*	No resources are envisaged to implement a RM system	Human resources made available to manage risk are very limited and shared with other pilot programmes (not suitable or not yet evaluated)	Specific resources to support the implementation of the organisation's risk framework are envisaged but not yet adequate	The allocation of suitable human resources for managing risk is sistematically considered in the organisation's operating budget and staffing plan
		Specialist support	Specialists are not available	A core group of people understand risk concepts and principles and have skills to carry out basic, qualitative risk analysis on behalf of top management	Specialists are used on ad hoc basis to support management in key and relevant areas. They are known throughout the organisation, are seen as a key anabler in initiating change and are often called to provide services and advice with respect to specific risk management issues. Managers are aware of how best to use them	An integrated and multidisciplinary centre of excellence exists for risk management. There is a cross-fertilisation between specialists and all staff. Specialists have a broad understanding of strategic, operational and functional risk issues and are recognized externally.
	Relationship	*Internal Communication strategy*	No internal communication flows about risk	Communication issues are not considered strategic to fully inform RM policy and programme implementation	Internal communication and RM process are closely linked. RM plans/policy papers, methodological documents and information resulted from the RM system are disseminated. Clear communication protocols are in place aimed at ensuring there is a common understanding of the respective responsibilities	Open, transparent, inclusive and two-way communication to risks, uncertainty and opportunities exists. A reliable communication strategy about risk issues are in place. Interfaces are periodically reviewed. Unsolicited views are encouraged, acknowledged and appreciated
TECHNOLOGIES: SUPPORT	**RM Information system**	*ICT tools*	No RM information system has been envisaged	A specific pilot RM information system is being implemented as a part of other information systems	A generic software may be used to support management in tracking key and relevant process areas	Each stage of the risk management process is tracked in a Web based tool thoroughly integrated with other corporate information systems
		Document management	Record management supporting activities and decisions is focused on physical and financial assets. The organisation does not document information about risk	A document management system, mainly focused on past events, may be envisaged: 1. to comply with legal, regulatory and governance requirements; 2. to record information with reference to some stand-alone processes identified and related mitigation actions	Organization identify resources in terms of document systems to support management in recording key and relevant process areas	Information about risks are recorded in a consistent and secure way, establishing the policies and procedures needed to access, use and transfer information, as part of a structured Information Management Plan. Each stage of the risk management process is recorded appropriately

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
TECHNOLOGIES: SUPPORT	**Techniques**	*Risk Identification*	The effects of risky events might be identified but not associated with their process sources	Unstructured or informal qualitative methods since the know-how required could not be available from the staff (e.g. historical data review, semi-structured interview, prompt / check list)	Structured qualitative methods (e.g. brainstorming, Delphi method, scenario analysis, etc.) are used to determine what needs deeper quantitative methods	Multidisciplinary approach: structured qualitative and quantitative/statistical (e.g. Monte-Carlo analysis, Bayesian analysis, etc.) methods, tools and models since risks may cover a wide range of causes and consequences
		Risk Measurement	Managers tend to use their own individual approach, based on personal experience	Techniques have limited focus in specialized areas (financial risk; IT project management)	A wide range of qualitative and quantitavive tools is used for risk measurement. Knowledge transfers occurs between risk specialists and managers to balance benefits and limitations of available tools and models	Risk management tools are integrated with departmental management tools and techniques. Tools and models are assessed on a periodic basis and updated based on most recent technology
	Reporting system	*Internal Executive & Operative reporting*	Information about risk is not reported and used as a basis for decision making	Internal reporting, mainly focused on past events, may be envisaged: 1. to comply with legal, regulatory and governance requirements; 2. to disclose information with reference to some stand-alone processes identified and related mitigation actions identified but often not executed	The organization establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail	Comprehensive and periodic internal reporting on both significant risks and risk management performance and process is provided regularly, at both executive (board of directors) and operative level (management). It contributes to strategic oversight, decision-making and improved operational decisions. Reliability and detail of risk information has significantly increased
	Reporting system	*External reporting*	There might be some ad hoc reports are provided on specific external request (e.g. public bodies, users of statistical information through citizens' associations, media) about the effects of risky or disruptive events after they have occurred	External reporting, mainly focused on past events, may be envisaged to disclose RM information with top management / senior managers with reference to some stand-alone processes identified and related mitigation actions identified but often not executed	Organization assures external stakeholders that key risks related to relevant areas are well-managed through reports including the actions taken and why they are appropriate	There is alignment of externally and internally reported information. Both real-time and periodic risk reporting are provided to external stakeholders about the risks the organization is facing and the plans to capitalize on emerging opportunities. Periodically a review of the effectiveness of the RM system is also reported
	Training system	*RM Training and people's competence*	RM training program and activities are not evisaged. No understanding of risk principles or language. No information exists on RM competency requirements. RM is not perceived to be a formal competency	A pilot training programme on RM concepts and principle has been implemented and a core group of managers have skills to manage risk. Risk knowledge competencies have been identified	A specific training program for management is provided and personnel running RM matters in all key and relevant areas is equipped with necessary skills, guidance and learning tools. Most people have relevant skills & knowledge to manage risks effectively. Risk skills gap is being addressed	All staff at any level receives regular and appropriate guidance and training to rapidly address risks, on typical risks that the organisation faces in relation to their role/job, on the action to take in managing these risks. New staff receives early RM training. Skills transfer take place. RM competencies and training are an integral component of individual learning plans

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
TECHNOLOGIES: SUPPORT	Communication system	*RM internal communication instruments and tools*	No specific internal means for communicating about risk are envisaged	Some internal tools to share knowledge among a core group of people about risk have been implemented (e.g. Knowledge sharing systems such as wiki platforms, sharepoint sites)	An Internal Communication plan and a team responsible for communicating about organization's policy and ownership have been defined. Meetings with all the organizational divisions involved are organized. Other tools to share RM information are face-to-face discussion, field debriefing sessions	Adequate and efficient communication plan and tools to share RM knowledge, information and practices with all internal stakeholders and to promote co-operation and dialogue are in place (e.g. regular internal meetings, workshops and seminars, web info sessions, Intranet site regularly updated about RM issues, RM newsletter, etc.)
		RM external communication instruments and tools	No specific external means for communicating about risk are envisaged	Some external tools to share knowledge among a core group of selected stakeholders about risk may be used	Specific external tools to communicate with stakeholders about how the organisation is dealing with key risk related to relevant areas are envisaged (e.g. meetings, web info sessions, other according to selected target-audience)	Adequate plan and tools to communicate with all external stakeholders and to promote co-operation and dialogue are in place (e.g. annual meetings, annual report, workshops and seminars, Internet site regularly updated about RM issues, RM newsletter, etc.)
	Financial Resources	*Financial resources adequacy*	No resources are envisaged to implement a RM system	Finanical resources made available to manage risk are very limited and shared with other pilot programmes	A specific RM budget is provided but not yet adequate. It includes primary financial resources such as the allocation of staff to support the implementation of the organisation's risk framework and a budget to treat specific risks related to key and relevant areas	The allocation of suitable resources for managing risk is sistematically considered in the organisation's operating budget: senior executive management discusses target maturity levels for each critical component of RM and a decision is made about the necessary investments. This includes the costing of opportunities for improved processes or additional programmes and resources to implement, monitor and review the framework

Chapter 9: Lessons learned

Chapter 8: Risk management maturity model | Section 2. Risk management process | Chapter 10: Enhancing Existing Risk Management in National Statistical Institutes by Using Agile Principles

Focus on: Lessons learned from the NSOs experiences in implementing Risk management

The following summary table shows more details about the answers to each of the survey items, which have been then grouped together in the following 5 affinity clusters to facilitate analysis:

- Cluster 1 - MANDATE & RISK POLICY. Items: Mandate and commitment to manage risks; Defining a risk policy
- Cluster 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP. Items: risk management Procedure; Setting up of a risk management Unit/Office
- Cluster 3 - RISK MANAGEMENT PROCESS. Items: Risk Identification phase; Risk assessment phase; Risk treatment phase
- Cluster 4 - RISK MANAGEMENT INTEGRATION. Items: Risk management Integration with other Organizational Functions; Risk management Integration with Quality Management; Risk management Integration with Internal Control/Internal Audit;
- Cluster 5 - RISK MANAGEMENT: SUPPORTING SERVICES. Items: Training; ICT System Supporting the RM process; Communication & Consultation.

For each ITEM the following features are higlighted:

- "WHAT WAS MOST SUCCESSFUL": Which have been the best effects on the organization coming from introducing risk management;
- "WHAT WAS MOST DIFFICULT": Which have been the main stumbling blocks in developing risk management;
- "WHAT NOT TO DO": According to the experience gained by NSOs participating in the Survey, which errors are best not to be repeated in implementing risk management.

CLUSTER 1- MANDATE & RISK POLICY					
Item	**Plus & Minus**	***Risk management Area***	***Organizational process management Area***	***Internal Audit/Control Area***	***Statistical Production process management Area***
Mandate and commitment to manage risks	Successful	a) Senior Management/Top Management Commitment b) Embedding systematic risk management into business processes c) Management engagement in risk plan at strategic, portfolio and operational level	a) Senior Management/Top Management Commitment b) Definition or risk appetite at board level and particularly the articulation of behaviors expected c) Defining the scope and boundaries of risk management	a) Senior Management/Top Management Commitment	a) Senior Management/Top Management Commitment b) Integrate risk management to planning, operations and decision making processes
	Difficult	a) Getting risk made part of Senior management objectives b) Communicating clearly scope and objectives c) The process of making the staff aware of the analysis of risk in an objective manner to counter the sense of confidence that generates the knowledge and experience of work they have done for a long time, so staff commonly considered that all tasks were under control and nothing unfortunate can happen	a) Maintaining the focus of Senior Management on risk management expectations	a) Promoting the implementation of a risk management system without a regulatory framework to support audit observations and recommendations	a) Balancing additional work load with effectiveness of risk management activities, consistently with risk appetite b) Design an integrated approach an oversight of risk management to limit additional burden on program managers c) Setting a mandate that envisages the total elimination of risk, with a limited budget
	Not to do	a) Imposing risk management without sharing expected benefits with staff b) Do not set a mandate of the RM Committee without proper resources to support it		a) Do not start the implementation of a risk management system without a regulatory framework that clearly establish responsibilities of the participants b) Do not limit RM responsibilities to a single office or individual	a) Not to consider non statistical risks (organizational risks) b) Ad hoc monitoring of risks response and tailored approaches for each divisions/programs c) Not consulting broadly with relevant stakeholders' expectations in the risk management plan development process

CLUSTER 1- MANDATE & RISK POLICY		
Item	**Plus & Minus**	**Risk management Area**
Mandate and commitment to manage risks	Successful	a) Risk policy and framework have been endorsed by senior executives, as well as across the whole organization b) The Policy includes risk management goals, context and purpose, a risk appetite statement and articulates accountabilities and responsibilities for risk management, providing instructions for staff on how to carry out risk assessments c) It's accessible to all staff and it is formally approved by the Board d) Standardizing RM process at all levels of the organization e) Establishing RM Committee, responsible for oversighting the implementation of RM system f) Clear definition of role and accountabilities
	Difficult	a) Changing the behaviors across the organization when our risk appetites were reviewed b) A low appetite for risk, while necessary to protect the integrity of estimates, can stifle innovation. c) Clear definition of risk appetite and risk tolerance
	Not to do	a) Not adapting risk policy to the official statistics business environment b) Start the implementation of risk management without having a proper regulatory framework and without a solid strategy according to the institution's priorities. c) Do not set a procedure that can be perceived as a supplementary administrative burden that demotivates management and staff

CLUSTER 2- RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk management Procedure	Successful	a) Consolidation of risks, with high level risks and detailed underpinning (treatment) actions b) Including risk into organizational planning c) Traceability of the process (stages, deliverables, documents) d) One central and integrated IT system for risk management (RM), Internal Control System and Compliance Management System covering all phases of the processes e) Monitoring that risk management procedure is flexible at all levels f) Having a senior executive staff member allocated to each strategic risk ensures accountability for the management of each area of strategic risk	a) Active involvement of risk owners in the RM process b) Cooperation of the RM unit with other relevant units (QM, IA, Controlling) c) Defining clear accountabilities d) Process Mapping help highlight key areas of focus for quality gates and where the program is most exposed to risk, aligning risk management plans to key issues and priorities	a) Risk management procedures integration with the existing quality management system b) Quality Indicators should be useful to inform the risk management process. c) Understanding and communicating risk appetite; d) Agreeing on appropriate escalation process (including roles and accountabilities) e) Ensuring that the data is used only for statistical purposes, minimizing the risk of data disclosure f) Linking of risks vertically to Strategic Risks and aligning expected behaviors through risk appetite. Also horizontal linking of risks to identify dependencies within the portfolio and wider Organization. g) Risks are managed within Total Quality Management framework
	Difficult	a) Adequacy of the risk escalation in the RM process b) Motivation of staff due to lack of financial and human resources, as the process is resource-intensive c) Achieving balance between being overly prescriptive and mantaining sufficient flexibility for people to adopt and adapt to the circumstances	a) Defining when and how to reconcile senior management and program management views (i.e. integrating top-down and bottom up approach) b) Communicating to the organization that any change could be a source of a statistical impact and therefore require effective risk management	a) Defining, developing, producing and monitoring/analyzing the appropriate quality indicators for all statistical programs to inform the risk management process b) Changing attitudes from one of expecting risk management to be a compliance issue to one where all management levels are engaged and the documents are seen as central tools in the production process, which need to be regularly revisited and refreshed c) Engaging with stakeholders to provide input into final risk management plans d) Definition of duties and responsibilities for risk treatment in cases where the risk is related to more than one process or the whole organization

CLUSTER 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk management Procedure	Not to do	a) Develop a procedure without consulting customers across the organization about how it can benefit them b) Completing stand-alone templates not linked to other documents c) Not integrating central system and tool d) Not relying on point in time assessments, such as once a year.	a) Not becoming overly focused on risk management documents/artefacts and losing sight of the importance of embedding the risk management approach into the work program	a) Not to distinguish between the risk management procedures and performance management b) Not have risk and quality management integrated with the financial planning process. c) Begin implementing a new process without a clear delivery timetable (the dates, areas involved and required deliverables changed several times during implementation of new risk management process) d) Have multiple areas assigned to provide similar support for the same risk/quality management plan development process without publicizing clear roles and responsibilities at the outset.

CLUSTER 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP		
Item	**Plus & Minus**	***Risk management Area***
Setting up of a Risk management Unit/Office	Successful	a) Formal integration of the risk management in each department in the organizational chart b) The RM team operates as a centralized function area responsible for overseeing the implementation of the risk management framework in the ABS, and coordinating strategic risk management at the organizational level The team offers support and advice on risk management rather than undertaking risk management activitiesc) Establishing a risk management committee who coordinates the RM team d) RM unit reporting directly to the DG Finance and DG Statistics
	Difficult	a) Ensuring adequate independence between Internal audit and risk management functions b) Managing a large risk management work program, with a small RM Team in which expertise is concentrated in a few key staff members c) Overseeing cross-agency risks with a devolved risk management approach
	Not to do	a) Making the risk team invisible: it needs to be prominently placed and given sufficient senior support to prevent the team being viewed as a corporate burden, instead, a corporate enabler to delivery b) Underestimate funding and resources required to effectively operate the risk management office c) Not creating too many RM bodies d) Focusing more on operational risks rather than strategic ones

CLUSTER 3 - RISK MANAGEMENT PROCESS				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk Identification phase	Successful	a) Focus on the real important issues through yearly workshops b) Implementation of an ad hoc reporting for risks system within the RM information tool c) Ensuring risks align with other corporate strategies d) Using simple "if" … "then" … statements, and considering factors external to the organization e) Flexibility of the identification model to guarantee more points of view f) Workshop approach to identification	a) Clear guidance to apply the methodology b) Aligning risk management cycle to field planning cycle c) Use a framework that considered regular cyclical risks and long term program transformation risks as separate but related groups d) Framing quality risks in an holistic manner to ensure the risks best reflected the totality of key stakeholder expectations around quality	a) Involvement of quality management into risk management workshops to identify key risks b) The results of SWOT analysis (performed to detect context of institution) are used as one of the sources for risk identification, getting Top Management involved in identification c) Performing regular quality review of statistical surveys d) Staff motivation and appropriately collaboration to identify risks and describe them in terms of statistical quality objective
	Difficult	a) Identify the interdependencies between the risks b) To imagine risky situations that have never materialized c) Ensuring everyone has the same understanding of terminology d) Determining risk owners when risks occur in different areas of activities e) Grouping risks into small enough groups f) Choosing the appropriate risk identification methodology	a) Common understanding of risks b) Establishing relation/link between strategic and operational risks	a) Identifying emerging risks or planning for unanticipated risks
	Not to do	a) Identifying too many risks and risks which aren't risks. b) To consider the process is safe and not susceptible to risks. c) Have too many strategic risks; d)Identify risks that can't realistically be treated and managed (i.e. risks that are beyond the control of the organization)	a) Use non-knowledgeable/amateur resources to train and support program managers b) Focus only on one dimension of risk (for example, cyclical risk) or on only a narrow view of quality	a) Don't see risks only as threaths but also as opportunities b) Not having a clear risk identification process and stick to it for a few years. c) Brainstorm risk identification without necessary stakeholders in the discussion

CLUSTER 3 – RISK MANAGEMENT PROCESS				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk Assessment phase	Successful	a) Prioritization at the Senior Management Board b) Qualitative assessment and prioritization of risks with support of IT tool c) Using a relatively simple risk assessment matrix d) Regular reviews of risks to prevent escalation e) Performing (for risk owners) training to support risk management process as well as a definition of risk identification and risk assessment criteria	a) Clear guidance to apply the methodology b) Having a small team made up staff from different work areas within the branch worked best for assessing the risk c) Evaluating and assessing selected risks by the especially created group consisting of the top management of the office and representatives of different departments within the office d) Sharing the results of risks management process with key stakeholders	a) While assessing the risk it is useful to evaluate its impact not only on the image of the institution, on the achievement of strategic objectives, etc., but also on the each group of interested parties (e.g., users, staff, data providers, etc.). Such assessment highly facilitates subsequent assessment of the effectiveness of the risk treatment actions.
	Difficult	a) Quantitative assessment of risks b) Encouraging staff to consider risks in areas outside their technical proficiency c) Getting personnel involved d) Risks prioritization	a) Keeping the risks current b) Measuring risk based on residual exposure c) Measuring the appropriate impact level of risk on the corporation vs division	
	Not to do	a) Over quantify, a lot of risk management is subjective and qualitative, this needs to be recognized b) Not to consider new emergent risks c) Not define risk evaluation criteria d) Not to discuss with regard to a common understanding of risks, as well as the probability of occurrence and impact of risks e) Overestimating risks f) Not relying on point in time assessments, such as once a year g) Under or over reporting in order to hide or artificially highlight risk	a) Do not rely on a single stakeholder to assess risks on behalf of the program or keep assessment limited within the one work area b) Using complex tool and irrelevant examples c) Not applying a standard approach to risk assessment	a) Push for only compliance (i.e. review frequency) and also focus on just high scoring risk.

CLUSTER 3 - RISK MANAGEMENT PROCESS 2/2				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk treatment phase	Difficult	a) Assigning resourcing for treatment plans that have cross-agency effects to ensure an integrated whole of organizational response is achieved b) Cost-benefit analysis	a) Cost benefit analysis b) Transferring risks appropriately following staff changes c) Finding time to incorporate risk treatments with business as usual priorities d) Exploring and adopting of a combination of response options	a) Aligning expected behaviors to appetite statements b) Definition of duties and responsibilities for risk treatment in cases where the risk is related to more than one process or the whole organization c) Tendency to address a small risk on a large/important survey rather than a larger risk that may affect several smaller programs d) Agreeing on controls and accountabilities for risks outside direct line management e) Having a global view of risks to quality, (i.e. across a set of programs, rather than a local view). f) Describing complex treatments for risk (e.g. controls that affected multiple risks or required coordination across multiple operational areas); g) Getting the right input from stakeholders to shape controls.
	Not to do	a) Don't keep track of progress of the implementation of treatment plans b) Not clearly identifying responsibility for treatment and timeframe of individual risk treatments c) Not monitoring of risks treatment	a) Not consider the systematical documentation of risks in case they occur b) Not reporting on progress of implementation	a) Not providing cost-benefit analysis b) Not defining appropriate deadlines for risk treatment c) Not ignoring the quality management staff when planning risk treatment

CLUSTER 4 - RISK MANAGEMENT INTEGRATION		
Item	**Plus & Minus**	***Risk management Area***
Risk management Integration with other Organizational Functions	Successful	a) Risk management integration with the internal audit function b) Different Areas of risks integrated within the organization: Strategic risk, Transformation risk, Statistical risk and Project risk c) Integration with other corporate functions such as planning, business continuity, and work health and safety d) Focus on statistical production and formal integration in all operational organizational functions e) Risk owners' responsibilities for specific risk areas
	Difficult	a) Making reporting at corporate level is difficult, when using separate management systems across different areas of organization b) To integrate RM with strategic planning, project management and quality management
	Not to do	a) Do not create an idealistic RM system that does not consider the actual organizational structure, functions, processes and capabilities

CLUSTER 4 - RISK MANAGEMENT INTEGRATION (1/2)		
Item	**Plus & Minus**	***Statistical Quality analysis Area***
Risk management Integration with Quality Management	Successful	a) Taking the recommendations made by the Quality Management team and storing them on the risk database, to focus audits b) Good collaboration in error treatment management c) Risk management integration with the existing quality management system based on the ISO 9001:2015 standard as this standard promotes the risk-based thinking through the whole organization d) Articulation of risk appetite for different statistical products e) Identification of weaknesses of statistical surveys by quality experts during quality reviews means discovery of potential risks that could occur in statistical processes and elaborating preventive program of improvements f) Quality review by outside organizations g) Risks are managed within Total Quality Management (Framework) h) Commitment at all management level to quality risks management

CLUSTER 4 - RISK MANAGEMENT INTEGRATION (2/2)		
Item	**Plus & Minus**	***Statistical Quality analysis Area***
Risk management Integration with Quality Management	Difficult	a) Getting the output managers to understand the value in recording and documenting the recommendations on the risk database b) Embedding process of surveillance of quality guidelines into risk management (or internal control system) c) Assuring production areas that development of the quality gates component of the quality system would not be onerous and would add value to their existing quality processes
	Not to do	a) Trying to monitor quality guidelines on a basis which is too granular b) Not implementing the risk management system, as well as no to try to integrate it with the quality management system without clear vision how to do it, without sound understanding and the knowledge of requirements defined for the both systems, related standards and their application and without designated coordinator with clear responsibilities for the procedure. c) Do not limit risk management and quality responsibilities to a single office or individual

CLUSTER 4- RISK MANAGEMENT INTEGRATION		
Item	**Plus & Minus**	***Internal Audit/Control Area***
Risk management Integration with Internal Control/IA	Successful	a) Close cooperation and coordination of Risk Management Unit and Internal Audit Unit b) Clear roles, responsibilities and accountabilities of risk management and internal audit outlining them in a framework c) Clear delimitation between the auditing and risk management functions outlined in a framework d) Use a risk based approach in determining priorities of treatment, according to audit recommendations: formal consultation of the RM by the Internal Audit during the audit planning process; Risk treatment monitoring outcomes are reviewed by Internal Auditing e) Using a risk base approach in determining priorities in recommendation in case of audits f) More awareness for staff around their responsibilities, accountabilities and how internal audits and internal controls work in the organization
	Difficult	a) Definition of risk areas for selected (planned) audit engagements b) Cooperation between IA and departmental structures, without a formal RM unit c) Fitting Expectations from management that Internal Audit would provide "assurance" on risks
	Not to do	a) Not to rely periodically on risk assessments

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
Training	Successful	a) Including information on risk management as a part of the initial HR training programme b) Establishing a competency model c) Annual training is mandatory, ongoing reminders are provided when appropriate. d) Approved funding for dedicated resources to support RM activities e) E-learning modules on risk management targeted on specific recipients f) The presence of a widespread culture of risk management as part of the work inherent in statistical production
	Difficult	a) Matching training to specific audiences needs b) Remain current and fit for purpose c) Ensuring that there is sufficient promotion of education materials for staff, including about training modules, and monitoring that staff undertake the training
	Not to do	a) Focusing training only on the transmission of knowledge about risk b) Not relying on one-time training

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
ICT System Supporting the RM process	Successful	a) ERM software covers all steps taken in connection with risk management, internal control system and compliance management (risk identification, risk assessment, risk mitigation, monitoring, audits, reporting). All information entered is unchangeably stored and recoverable for audit procedures ERM software integrates the criteria of relevant standards and frameworks (ISO 31000 ERM, COSO II ERM & Internal Control, ISO 19600) b) Mandatory IT security training for new employees before they are granted access to IT resources c) Plans to leverage existing tools, templates and project risk management web tool d) Awareness of importance of supporting tool/application in risk management process e) Using a simple tool that does not require complex computer knowledge to be used and operates as an application in Microsoft Excel, covering all the phases of the risk management process
	Difficult	a) Managing cross-agency risks and reporting at the whole of organization level without an ERM software b) Intuitive software layout c) Lack of a specialized software integrated with planning, internal control system, quality management system, compliance management
	Not to do	a) Not relying on tools as a replacement to processes

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
Communication & Consultation	Successful	a) Implementation of regular risk management workshops for top and middle management employees b) Leveraging Field Portfolio Managers to disseminate information and coordinate input from fields c) Risks discussions integrated with performance d) The risk management Framework Communicated and dissemination to staff and to external stakeholders through different channels (e-learning, seminars, internal communication channels, forum, workshops) and at different levels (strategic, operational) through the support of Quality Assurance Section e) Consultation with staff to support the implementation of the risk management framework through the Risk Team at strategic and project level (fraud risk, transformation risks, project risks, statistical risks), the Quality Assurance Section at the operational/program level (statistical risks), Internal auditors and external consultants to assist in conducting a series of risk workshops
	Difficult	a) Managing burden associated with additional monitoring and reporting requirements b) Engagement of staff to active participation during the implementation phase
	Not to do	a) Establish a limit to the participation of staff

Chapter 10: Enhancing Existing Risk Management in National Statistical Institutes by Using Agile Principles

Chapter 9: Lessons learned | Section 2. Risk management process

CASE STUDIES:

Ireland, Central Statistics Office (CSO)

CSO's Household Survey Development Project (HSDP)

The purpose of the HSDP is to create a new household survey environment to meet additional national and international needs for a wider range of social statistics. The key aim of this modernisation programme of related projects is to develop an efficient integrated system for household surveys across multiple collection modes thus enabling the CSO to deliver on the expanding requirements for social statistics in a cost effective and timely manner.

For example one of the sub-projects in this overall programme of projects is the Computer Assisted Telephone Interviewing (CATI) project which involves the outsourcing of interviewing for waves 2-5 of the QNHS (Labour Force survey) to an external call centre.

The HSDP has and remains a very significant modernization programme for CSO, spanning several years in terms of delivery and involving significant numbers of staff and management from both the IT side and business side of the Office.

Agile project management has been employed extensively during the HSDP to maximize delivery of desired outcomes. For example daily Agile scrums and regular Agile sprints maximize achievement of deliverables. Agile management has ensured that active and dynamic management of project risks happens and so risks that have potential to impact development progress are dealt with as they arise.

Agile practices ensure project teams are suitably empowered to drive deliverables but this is matched with regular assurance processes to most senior managers to ensure overall desired corporate direction is achieved.

Agile management practices have and are significantly enhancing the risk management on our HSDP.

UK, Office for National Statistics (ONS)

RRM's Scheduling and Workflow Mechanism.

The Response and Respondent Management system (RRM) was looking to integrate a scheduling and workflow mechanism that would be strategic to the entire office.

There was a threat to delivery of RRM, as this was needed for a forthcoming survey, but early indication was that the work was potentially too much for the time available (or else workarounds would be costly).

An Agile approach meant that its implementation had been put off, as the team always prioritized value, and this was never the most valuable thing at earlier stages. Then there was a significant strategic shift - RRM stopped being the long term strategic solution for that component of the system, and it was given a limited lifespan.

Although this was disappointing to the team, it meant the scheduling and workflow mechanism no longer needed to be strategic - they could implement something quickly and easily that just did the job. Being strict about prioritizing by value (an important agile concept) postponed the decision and sure enough the landscape changed in the time of the postponement so that when the decision had to be made it became much more achievable.

Italian National Institute of Statistics (ISTAT)

Territorial Bases System

Purpose of the project

The purpose of the TBS was to create a new system to update via web the territorial basis by municipalities. The key aim of this project was to develop an efficient system, with a limited number of accesses (more or less 8500 municipalities), to update the territorial basis for Census. The whole system, reachable through authentication, is divided in two separated areas, Front Office accessed by municipalities and Back Office, accessed by Istat Personnel.

After a short description, on the home page there is a login/password box. After authentication, for security reasons, the Responsible of Municipality of territorial bases had to fill in a form with his data to associate a Municipality to a physical person.

The main implemented features for the Front End are:

1. A download section with one or more PDF file with the territory map, an application to modify these files, an Access MDB with 2-3 tables;
2. An upload section where to put the modified files;
3. A documental area that contains the software manuals and user guides, legal documents, and a movie with the operating instructions;
4. An area with history files related to the territorial basis of the last Census (2001).

Software application and documental area are common. Other materials are specific for each Municipality.

The Back Office area contains a monitoring system to trace all operations referred to each Municipality.

Relationship between Istat's Census Department and ICT Department

The project owner was the Istat's Census Department which played the client role. The ICT Department supplied this service and the project manager belonged to ICT Department.

Main critical issues of the project

This project presented some critical point, summarized in: limited time to deliver, no margin for error, due to the compliance with current regulation for Census and the involvement of 8.500 municipalities.

Advantages to use agile approach

To mitigate risk of failure, Agile project management has been employed extensively during this project to maximize delivery of desired outcomes. Not only weekly meetings were held to verify together, client and supplier, each system release, but also the project manager obtained a resource (programmer) from Census Department, for 5 weeks, to work in his team. In this way, the customer had his own/assigned person to monitor the progress of the project and to actively contribute at the job development. The supplier engaged the client to share the responsibility of each deliverable. As consequence, the strong collaboration between Departments made impressive the speed and the quality of releases.

Comparing agile and traditional methods of project management, there is no doubt that Agile enables collaboration among structures. Moreover, traditional PM doesn't take in account that often customers change requirements during the project. In fact, during the deployment phase, the client really understands the potential of the system and asked for new features. As well known, change requests are often very expensive. Agile method mitigates this risk.

For Istat, this is a good example of successful project, carried on through an Agile approach.

List of reviews

⇦	Annex - Focus on risk management practices	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	References	⇨

First Draft (April 2016) – Risk management guidelines presented during the "Workshop on risk management practices in Statistical Organizations", held in Geneva on 25-26 April 2016.

Second Draft (July 2016) – Review of risk management guidelines after the "Workshop on risk management practices in Statistical Organizations", according to the observations and suggestions received by the NSOs participating in the Survey.

- The following paragraphs/chapters have been revised: Foreword: “what risk is and why risk management is relevant” statements added (page 9-11);

- Risk Nomenclature and definitions: meaning of risk Plan clarified (page 17);

- Risk appetite: risk Appetite and risk Profile issues implemented (page 18-20).

- Risk management commitment: paragraph revised as required (page 20);

- Risk management approach: example of “mixed approach” clarified (Fig. 2, page 23);

- Internal control according to a risk-based approach: relationships between internal controls and risks clarified (page 24-26);

- Integration with GAMSO: proposal to align GAMSO and risk management process added referring to the integration between risk and quality management (page 27);

- Roles and Responsibilities: responsibility of he “governing board” clarified (page 31);

- Monitoring and Review of the Framework: the importance of periodically reviewing the risk management maturity level underlined (page 34);

- Review Audit Report: the importance of the audit report in aligning risks with internal controls underlined (page 37);

- Communicating risks: the importance of documenting risk communication in the risk management /Internal communication Plan underlined (page 42-44);

- Establishing the context: the importance of risk maturity assessment in order to successful implementing a risk management policy underlined (page 46-47);

- Risk treatment: the differences between mitigation actions and contingency actions clarified (page 61);

- References: the standard ISO 27000 “*Information technology - Security techniques Information security management systems – Requirements”* quoted in “References”

The following paragraphs/chapters have been included/added:

- Risk management approaches: paragraph on risk management approaches (top-down, bottom-up) implemented (page 21-22);.

- paragraph on risk identification modified (page 50);

- Risk management Maturity Model paragraph added (page 76);

- Risk Appetite: UK case study added (page 9-11, Annex);

- Risk Maturity Model: UK Case study added (page 29-34, Annex);

- Risk Maturity Model combining both international standards and analysis of surveys on risk management practices results added (page 35-42, Annex)

Third Draft (October 2016) – Risk management guidelines integrated with the analysis of results from the III Survey "What was most successful, What was most Difficult, What not to do when implementing risk management in NSOs' experiences" (July – September 2016).

The following chapters have been included/added:

a) Lessons Learned (page 85): new chapter on analysis of 3rd survey on risk management practices results.

b) Summary table of 3rd survey on risk management practices results: (page 36-48 Annex).

References

List of reviews	РУКОВОДСТВО «ПРАКТИКА УПРАВЛЕНИЯ РИСКАМИ В СТАТИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ»	Глоссарий

Research INVESTIGATION / AD HOC ANALYSIS

UNECE (The United Nations Economic Commission for Europe)

High-Level Group for the Modernisation of Official Statistics

Modernisation Committee on Organizational Framework and Evaluation

- *Survey on Risk Management Practice*, April, 2015
- *In-Depth Survey on Risk Management*, September, 2015

Short summary

In 2015 two surveys have been carried out by the Italian Institute of Statistics in cooperation with University of Rome Tor Vergata and UNECE, in order to analyze to what extent Risk management systems are adopted among NSOs members of UNECE as well as among countries and international organizations not belonging to UNECE but yet participating in Commission's activities. The surveys were aimed at building criteria through which the practices could be identified and classified. Due to the complexity of the matter as well as in order to get more solid achievements, a multi-method model was chosen in order to use heterogeneous yet complementary approaches for analysis. According to the explorative approach, both qualitative and quantitative-descriptive tools were used: a mixed model allows to include context factors that enable a deeper understanding of phenomena, also taking into account the strategic components of the practices observed. The first Survey was submitted in May 2015 to 60 countries and 4 organizations; the response rate was around 57%. Among all respondents, thirteen countries were selected for an In-depth analysis of the Risk management most interesting practices from a NSO point of view. The selected countries were invited to answer to a second questionnaire during September 2015.

To validate as well as underpin the Guidelines, a closing survey has been designed to get a full picture of the implementation routes for Risk management systems among statistical organizations.

This Survey has been made up of six different questionnaires addressed to as many organizational areas (*Risk management; Statistical quality analysis; Statistical production process management; Organizational process management; Internal control and/or internal auditing; Services supporting statistical production*). The sample selected has consisted of organizations presenting different levels of *Risk maturity*; therefore, the approach has been comprehensive enough to catch the diverse perspectives and so to help bring out elements that are as much as possible representative of the different contexts analysed. A dedicated Survey section made up of no more than 6 (six) questions has been provided for each target-audience area.

The third Survey was submitted in July 2016 to 26 NSOs and 1 statistical organization; the average of the responses rate of the all sections was around 53%.

1. UNECE – MCOFE Survey on Risk Management Practice, April, 2015

Respondent countries / organizations: Australia, Austria, Canada, Croatia, Eurostat, Ireland, Italy, Lithuania, Poland, Norway, México, Romania, The Netherlands, Belgium, Estonia, Cyprus, Finland, Germany, Hungary, Iceland, Israel, Japan, New Zealand, Republic of Armenia, Republic of Macedonia, Republic of Moldova, Russia, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Turkey, United Kingdom.

2. In-Depth Survey on Risk Management, September, 2015

Respondent countries: Australia, Austria, Canada, Croatia, Ireland, Lithuania, México, Romania, The Netherlands, Sweden.

3. Final Survey on Risk Management, July, 2016

Respondent countries: Armenia, Australia, Austria, Canada, Estonia, Finland, Lithuania, Malta, Mexico, Norway, Poland, Republic of Armenia, Romania, Slovenia, The Netherlands, United Kingdom, USA, Croatia.

Complementary documentation provided by the respondent countries throughout the research was carried out by:

(*In most cases, the following documents are intended for the internal use of recipients only and may not be distributed or reproduced for external distribution)

Statistik Austria:

- *Risikobewertung – Risikokatalog (Observar, angepasst). 2015*
- *Data Collection for Social Statistics Project - Erhebungsinfrastruktur (EIS) Neu (Survey infrastructure). New Risk Management. 2015*
- *Risikomanagement-Katalog. Assessment von Chancen und Risiken. 2013*
- *Summary Event Catalogue, 2009.*

Australian Bureau of Statistics (ABS), Australia:

- *Risk Management Framework. Part A - The Risk Policy.* 2015
- *Risk Management Framework. Part B- The Risk Guidelines.* 2015
- *Corporate Plan 2015-2019.* 2015
- *Quality Management of Statistical Processes Using Quality Gates.* 2010
- *ABS Internal Control Framework.*
- *Accountable Authority Instructions. 01-01 Managing Risk and Internal Accountability.*

Statistics Canada:

- Corporate Risk Profile methodology and outcome (http://www.statcan.gc.ca/)
- Corporate Risk Profile 2012-2104. 2012

Statistics Lithuania:

- Extraction from SL risk register

Instituto Nacional de Estadística, Geografía e Informática (INEGI), México:

- *Matriz de Administración de Riesgos.* 2015
- *Selected items of Risk Matrix for the 2015 Intercensal Survey.* 2015
- *Manual de integración y funcionamiento del comité de auditoría y riesgos del instituto nacional de estadística y geografía. 2014*
- *Metodología para la Administración de Riesgos en el INEGI. 2014*
- *Acuerdo de la junta de gobierno del instituto nacional de estadística y geografía, por el que se establecen las normas de control interno para el instituto nacional de estadística y geografía. 2014*
- *Draft Federal Information Processing Standards Publication 183. Standard for Integration Definition for Function Modeling (IDEF0). 1993*

Institutul National De Statistica, Romania:

- *Ordin nr 1038-2011 - procedura sistem management riscuri.* 2011

National / International Standards, Models and Guidelines

ANAO (The Australian National Audit Office)

Reference published Guide:

- *Public Sector Audit Committees. 2.1 Risk Management.* August, 2011
- Highlights

The Guide updates and replaces the Australian National Audit Office's (ANAO) 2005 *Public Sector Audit Committees Better Practice Guide*. While many of the principles and practices remain the same, this Guide incorporates a number of enhancements. These include a discussion on: a committee's responsibilities in relation to Risk management and other portfolio entities; the benefits of periodically engaging with the entity Chief Executive/Board, including in relation to the committee's responsibilities for reviewing high risk programs and projects. This Guide is intended to complement the Fraud Control Guidelines, and to augment the key fraud control strategies referred to in the Guidelines. While this document is an important tool for senior management and those who have direct responsibilities for fraud control, elements of this Guide will be useful to a wider audience, including employees, contractors and service providers. The aim of the Guide is to provide guidance on the operation of the Audit Committees of public sector entities operating under both the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997*. As with all of the ANAO's Better Practice Guides, each entity is encouraged to use it to identify, and apply, better practice principles and practices that are tailored to its particular circumstances. The Guide discusses a range of functions and responsibilities, grouped under nine broad areas, that are appropriate for an Audit Committee.

Available:

www.anao.gov.au/html/Files/BPG%20HTML/BPG_PublicSectorAuditCommittees/2_1.html

AS/NZS (Joint Australian New Zealand International Standard). Joint Technical Committee OB-007, Risk Management

Reference published Guide:

- *AS/NZS ISO 31000:2009. Risk Management – Principles and guidelines*. November, 2009

Highlights

The Standard is a joint Australia/New Zealand adoption of ISO 31000:2009, and supersedes AS/NZS 4360:2004. It was approved on behalf the Council of Standards Australia on 6 November 2009 and on behalf of the Council of Standards New Zealand on 16 October 2009. Its predecessor, AS/NZS 4360 *Risk management*, was first published in 1995. After AS/NZS 4360 was last revised in 2004, the joint Australia/New Zealand committee OB-007 decided that rather than undertake a similar revision in 2009, it would have promoted the development of an international standard on risk management, which could then be adopted locally. The standard provides organizations with guiding principles, a generic framework, and a process for managing risk. New to this edition is the inclusion of 11 risk management principles an organization should comply with, and a management framework for the effective implementation and integration of these principles into an organization's management system. Emphasis is given to considering risk in terms of the effect of uncertainty on objectives, rather than the risk incident. This edition also includes an informative annex that sets out the attributes of enhanced risk management for those organizations that have already been working on managing their risks and may wish to strive for a higher level of achievement.

Available:

https://shop.standards.govt.nz/catalog/31000%3A2009%28AS%7CNZS+ISO%29/view

Basel Committee - Risk Management Sub-group

Reference published guidance:

- *Framework for Internal Control Systems.* September, 1998

Highlights

The Basel Committee on Banking Supervision, which includes supervisory authorities from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States, introduced the *Framework for Internal Control Systems* in 1998. The Basel Committee distributed this Guidance to supervisory authorities worldwide in the belief that the principles presented will provide a useful framework for the effective supervision of internal control systems. More generally, the Committee wished to emphasize that sound internal controls are essential. The five elements of internal control are: management oversight and control culture, risk recognition and assessment, control activities and segregation of duties, information and communication, and monitoring activities and correcting deficiencies. The effective functioning of these five elements is key to an organization achieving its performance, information, and compliance objectives. The guidance does not focus on specific areas or activities within a banking organization. The exact application depends on the nature, complexity and risks of the organization's activities. While closely linked to the specific sector, the principles of this guidance can be taught and effectively applied throughout different areas.

Available:

www.bis.org/publ/bcbs40.htm

CIMA (The Chartered Institute of Management Accountants)

Reference published Guide:

- *Introduction to managing risk.* Topic Gateway series no. 28. February, 2008

Highlights

The Chartered Institute of Management Accountants is the world's largest and leading professional body of management accountants. It has more than 229,000 members and students in 176 countries. It has strong relationships with employers and sponsor leading research. The Chartered Institute of Management Accountants supports its members and students with its Technical Information Service (TIS) for their work and needs. Topic Gateways are intended as a refresher or introduction to topics of interest to CIMA members. They include a basic definition, a brief overview and a fuller explanation of practical application. Finally they signpost some further resources for detailed understanding and research. The Guide was prepared by Technical Information Service.

Available:

www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf

CNRMA

Reference published Guidance:

- *OPNAVINST 3500.39 (series), Operational Risk Management (ORM)*. July, 2010

Highlights

ORM is the guiding Navy instruction for implementing the Operational Risk Management program. CNRMA manages and oversees shore installation management support and execution within the Mid-Atlantic region. The naval vision is to develop an environment in which

every individual (officer, enlisted and civilian) is trained and motivated to personally manage risk in everything they do on and off duty, both in peacetime and during conflict, thus enabling successful completion of all operations or activities with the minimum amount of risk. Commands have a number of responsibilities relative to ORM, including designating

the Executive Officer as the ORM Program Manager to oversee command ORM training and implementation and ensuring that at a minimum one officer and one senior enlisted are qualified as ORM instructors. While closely linked to this specific sector, the principles of this guidance can be taught and effectively applied throughout different areas: many ORM techniques can be incorporated into operational planning and decision making processes related to various sector of activity.

Available:

www.public.navy.mil/airfor/nalo/Documents/SAFETY/OPNAVINST%203500.39C%20OPERATIONAL%20RISK%20MANEGEMENT.pdf

COSO (The Committee of Sponsoring Organizations of the Treadway Commission)

Reference published Guidance:

- *Enterprise Risk Management (ERM) – Integrated Framework.* September, 2004

Reference published papers:

- *Risk Assessment in Practice*. October, 2012
- *Developing Key Risk Indicators to Strengthen Enterprise Risk Management.* December, 2010.
- *Strengthening Enterprise Risk Management for Strategic Advantage*. 2009

Highlights

COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. The members of COSO are: the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, the Institute of Management Accountants and The Institute of Internal Auditors. ERM is a widely used framework in the United States and around the world. Over two decades ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued “Internal Control – Integrated Framework” to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule and regulation and used by thousands of enterprises and organizations to better control their activities in moving toward achievement of their established objectives. In 2001, COSO initiated a project, and engaged *PricewaterhouseCoopers*, to develop a framework that would be readily usable by managements to evaluate and improve their organizations’ enterprise risk management. COSO engaged PricewaterhouseCoopers after concluding there was a need for a broadly recognized enterprise risk management framework. *PricewaterhouseCoopers* was assisted by an advisory council composed of representatives from the five COSO organizations. Because of the importance of the project, the Framework was exposed for public comment before final publication. COSO recognized that while many organizations may be engaged in some aspects of enterprise risk management, there has been no common base of knowledge and principles to enable boards and senior management to evaluate an organization’s approach to risk management and assist them in building effective programs to identify, measure, prioritize and respond to risks. “ERM – Integrated Framework” expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management for all organizations, regardless of size. The framework defines essential enterprise risk management components, discusses key principles and concepts, suggests a common language, and provides clear direction and guidance for enterprise risk management.

Available:

www.coso.org/ERM-IntegratedFramework.htm

www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf

www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf

www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf

A (Chartered Professional Accountants of Canada)

Reference published Guide:*Guidance on Control. CoCo (Criteria of Control) Framework.* 1995

- Highlights

Chartered Professional Accountants of Canada (CPA Canada) is the national organization established to support a unified Canadian accounting profession. As one of the world's largest national accounting bodies, with more than 200,000 members across the country and around the world, CPA Canada carries a strong influential voice: it plays an important role in influencing international accounting, audit and assurance standards. CoCo was introduced in 1992 with the objective of improving organizational performance and decision-making with better controls, risk management, and corporate governance. In 1995, *Guidance on Control* was produced and described the CoCo framework and defining controls. The framework includes 20 criteria for effective control in four areas of an organization: purpose (direction), commitment (identity and values), capability (competence), monitoring and learning (evolution). This model describes internal control as actions that foster the best result for an organization. These actions, which contribute to the achievement of the organization's objectives, focus on: effectiveness and efficiency of operations; reliability of internal and external reporting; compliance with applicable laws and regulations and internal policies. CoCo indicates that control comprises: "Those elements of an organization (including its resources, systems, processes, culture, structure, and tasks) that, taken together, support people in the achievement of the organization's objectives."

Available: https://www.cpacanada.ca/

FRC (The Financial Reporting Council)

Reference published Guidance:

- *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting (The Turnbull Guidance).* September, 2014

Highlights

The Financial Reporting Council is the UK's independent regulator responsible for promoting high quality corporate governance and reporting to foster investment. It promotes high standards of corporate governance through the UK Corporate Governance Code. It sets standards for corporate reporting, audit and actuarial practice and monitor and enforce accounting and auditing standards. The FRC issues guidance and other publications to assist boards and board committees in considering how to apply the UK Corporate Governance Code to their particular circumstances. These publications cover, among others: "Risk management, Internal Control and Related Financial and Business Reporting". This guidance revises, integrates and replaces the previous editions of the FRC's *Internal Control: Guidance to Directors* (formerly known as the *Turnbull Guidance*) and the *Going Concern and Liquidity Risk: Guidance for Directors of UK Companies* and reflects changes made to the UK Corporate Governance Code. It links the traditional *Turnbull* guidance on internal control with emerging good practice for risk management reflected in the conclusions of both the FRC's *Boards and Risk* report and the final recommendations of the *Sharman Panel of Inquiry into Going Concern*

and Liquidity Risk. *Internal Control: Guidance for Directors on the Combined Code* (The *Turnbull guidance*) was first issued in 1999. In 2004, the Financial Reporting Council established the Turnbull Review Group to consider the impact of the guidance and the related disclosures and to determine whether the guidance needed to be updated. In reviewing the impact of the guidance, consultations revealed that it had very successfully gone a long way to meeting its original objectives. Boards and investors alike indicated that the guidance had contributed to a marked improvement in the overall standard of risk management and internal control since 1999. The second version was issued in 2005 (*Internal Control: Revised Guidance for Directors on the Combined Code*). Consistent with the amendments to any Principles in the 2014 edition of the Code and with the aim of aligning the terminology, a new version of the Guidance was issued in 2014.

Available:

https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance/UK-Corporate-Governance-Code/Guidance-for-boards-and-board-committees.aspx#biscuit3

GAO (U.S. Government Accountability Office)

Reference published Standard:

- *Standards for Internal Control in the Federal Government (The Green Book).* September, 2014

Highlights

The standards provide guidance on assessing risks and internal controls system for federal agencies in programmatic, financial, and compliance operations. On September 10, 2014 GAO issued its revision of *Standards for Internal Control in the Federal Government*. The 2014 revision will supersede GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government* (November 1999). Federal Managers' Financial Integrity Act (FMFIA) requires that federal agency executives periodically review and annually report on the agency's internal control systems. FMFIA requires the Comptroller General to prescribe internal controls standards. These internal control standards, first issued in 1983, present the internal control standards for federal agencies for both program and financial management. *The Green Book* may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system. *Green Book* revisions involved an extensive, deliberative process, including public comments and input from the Green Book Advisory Council. GAO considered all comments and input in finalizing revisions to the standards. The standards in *The Green Book* are organized by the five components of internal control. Each of the five components contains several principles. Principles are the requirements of each component. Contol environment (5 principles); Risk assessment (4 principles); Control activiteis (3 principles); Information and communication (3 principles); Monitoring (2 principles).

Available:

www.gao.gov/greenbook/overview

Institute of Risk Management (IRM); Association of Insurance and Risk Managers (AIRMIC); Alarm (The Public Risk Management Association)

Reference published Standard:

- *A Risk Management Standard.* 2002

- Highlights

The Risk Management Standard was originally published by the Institute of Risk Management (IRM), The Association of Insurance and Risk Manager (AIRMIC) and The Public Risk Management Association (Alarm) in 2002. It was subsequently adopted by the Federation of

European Risk Management Association (FERMA). The Standard is the result of work by a team drawn from the major risk management organizations in the UK. In addition, the team sought the views and opinions of a wide range of other professional bodies with interests in risk management, during an extensive period of consultation. Despite the publication of ISO 31000, the Global Risk Management Standard, IRM has decided to retain its support for the original risk management standard because it is a simple guide that outlines a practical and systematic approach to the management of risk for business managers (rather than just risk professionals).

Available:

www.theirm.org/knowledge-and-resources/risk-management-standards/irms-risk-management-standard/

ISO (International Organization for Standardization)

- *ISO/IEC 27001:2005. Information technology -- Security techniques -- Information security management systems -- Requirements*
- *ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements*

Available:

https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Technical Committee TC 262 - Risk management

Reference published Standards:

- *ISO Guide 73:2009. Risk management - Vocabulary*
- *ISO 31000:2009. Risk management - Principles and guidelines*
- *ISO/TR 31004:2013. Risk management - Guidance for the implementation of ISO 31000*
- *IEC 31010:2009. Risk management - Risk assessment techniques*

Available:

www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=629121

Technical Committee TC 176/SC 1 - Concepts and terminology

Reference published Standard:

- *ISO 9000:2000. Quality management systems - Fundamentals and vocabulary*

Technical Committee TC 176/SC 2 - Quality systems

Reference published Standard:

- *ISO 9004.4:1993. Quality management and quality system elements - Part 4: Guidelines for quality improvement*

Available:

www.iso.org/iso/catalogue_detail?csnumber=29280

www.iso.org/iso/catalogue_detail.htm?csnumber=16544

Joint Technical Committee ISO/IEC JTC 1/SC 7 Software and systems engineering

Technical Committee ISO/TC 159/SC 4 Ergonomics of human-system interaction

Reference published Standards:

- *ISO/IEC 9126-1. Software Engineering - Product quality - Part 1: Quality model*
- *ISO 20282-1:2006. Ease of operation of everyday products - Part 1: Design requirements for context of use and user characteristics*
- *ISO/IEC TR 9126-4:2004. Software Engineering - Product quality - Part 4: Quality in use metrics*
- *ISO 9241-11. Part 11: Guidance on Usability*
- *ISO/IEC TR 9126-2. Software Engineering - Product quality - Part 2 External metrics*
- *ISO/IEC TR 9126-3. Software Engineering - Product quality - Part 3 Internal metrics*
- *ISO/IEC 18019:2004. Guidelines for the design and preparation of user documentation for application software*
- *ISO/IEC 15910:1999. Software user documentation process*
- *ISO 13407:1999. Human-centered design processes for interactive systems*
- *ISO/IEC 14598-1:1999. Software product evaluation*
- *ISO/TR 16982:2002. Usability methods supporting human-cantered design*

Available:

www.iso.org/iso/catalogue_detail.htm?csnumber=22749

www.iso.org/iso/catalogue_detail.htm?csnumber=34122

www.iso.org/iso/catalogue_detail.htm?csnumber=39752

www.iso.org/iso/catalogue_detail.htm?csnumber=16883

www.iso.org/iso/catalogue_detail.htm?csnumber=22750

www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22891

www.iso.org/iso/catalogue_detail.htm?csnumber=30804

www.iso.org/iso/catalogue_detail.htm?csnumber=29509

www.iso.org/iso/catalogue_detail.htm?csnumber=21197

www.iso.org/iso/catalogue_detail.htm?csnumber=24902

www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31176

Highlights

ISO has developed more than 16,000 international standards for stakeholders such as industry and trade associations, science and academia, consumers and consumer associations, governments and regulators, and societal and other interest groups.

Specifically, as for the family of Standards developed and published under the direct responsibility of TC 262, the first editions of ISO 31000 and ISO Guide 73 were published in 2009. ISO 31000 has been adopted as a national standard by more than 50 national standards bodies covering over 70 % of the global population. It has also been adopted by a number of UN agencies and national governments as a basis for developing their own risk-related standards and policies. All the terms and definitions in ISO 31000 are contained in ISO Guide 73, so any changes to the terms and definitions in ISO 31000 must be identical in both documents. At this end, ISO 31000, and its accompanying Guide 73 on risk management terminology come up for revision every five years.

The family of Standards developed by TC 176 are particularly relevant to support organizations in the process mapping activity and has been used as a reference source for drawing up that section. Its scope is the standardization in the field of quality management (generic quality management systems and supporting technologies), as well as quality management

standardization in specific sectors. ISO/TC 176 is also entrusted with an advisory function to all ISO and IEC technical committees to ensure the integrity of the generic quality system standards and the effective implementation of the ISO/IEC sector policy on quality management systems deliverables.

The family of Standards published under the direct responsibility of JTC 1/SC 7 and TC 159/SC 4 are particularly useful to support organizations in the design and implementation of the RM Information systems. JTC 1/SC7 has the following mandate from ISO and IEC: standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems. As for the TC 159/SC 4, its scope is the standardization in the field of ergonomics, addressing human characteristics and performance.

OCEG

Reference published Standard:

- *The GRC Capability Model 3.0 (Red Book).* 2015

Highlights

OCEG is a global, nonprofit think tank and community. It informs, empowers, and helps advance more than 50,000 members on governance, risk management, and compliance (GRC). Its members include c-suite, executive, management, other professionals from small and midsize businesses, international corporations, nonprofits and government agencies. Founded in 2002, OCEG is headquartered in Scottsdale, AZ. The OCEG framework is centered on the GRC Capability Model (commonly known as the *Red Book*). It describes key elements of an effective GRC system that integrates the principle of “Good governance”, “Risk management”, “Compliance”. The first *Red Book* was released in 2004: after months of analysis, collaboration, and vetting, the first OCEG standard emerges. Originally called the OCEG Capability Model, the cover was a deep red. It quickly became known as the OCEG *Red Book*. This standard provided both high-level and detailed practices that helped organizations address compliance and ethics issues. The standard gained wide adoption with over 100,000 downloads in a single year. Version 2.0 was published in 2009; version 2.1 was issued in 2012. The *Red Book* version 3.0 reflects 10 years of use and consideration by OCEG's global membership, which is now approaching 50,000 individuals worldwide. The Red Book Steering Committee attended several drafting and review sessions and prepared comments on each draft of the Red Book documents throughout the development process.

Available:

www.oceg.org/resources/red-book-3/

The British Standards Institution (BSI)

Reference published Guidance:

- *BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000*. June, 2011

- Highlights

Formed in 1901, BSI was the world’s first National Standards Body. The BSI Kitemark was first registered by BSI on 12 June 1903. Originally known as the British Standard Mark, it has grown into one of Britain’s most important and most recognized consumer quality marks. Through more than a century of growth, BSI now delivers a comprehensive business services portfolio to clients, helping them raise their performance and enhance their competitiveness worldwide. Based on the consensus of the UK committee of risk management experts, BS 31100 provides practical and specific recommendations on how to implement the key principles of effective risk management as specified in ISO 31000. According to British Standards Institute (BSI), “BS 31100 will provide a basis for understanding, developing, implementing and maintaining risk management within any organization, in order to enhance an organization’s likelihood of successfully achieving its objectives”. This British Standard establishes the principles and

terminology for risk management, and gives recommendations for the model, framework, process and implementation of risk management. The recommendations of BS 31100 are generic and intended to be applicable and scalable to all organizations across the public and private sector, regardless of type, size and nature. How recommendations are implemented will depend on an organization's operating environment and complexity. BS 31100 is intended for use by anyone with responsibility for: ensuring that an organization manages to achieve its objectives; ensuring risks are managed in specific areas or activities; overseeing risk management in an organization; providing assurance on an organization's risk management". The first edition was issued in 2008: this version was replaced by the 2011 edition.

Available:

http://shop.bsigroup.com/ProductDetail/?pid=000000000030228064

The Institute of Directors in Southern Africa (IoDSA)

Reference published Models:

- *King Report on Corporate Governance (King III).* September, 2009
- *King Code of Governance Principles (King III).* September, 2009

Highlights

The Institute of Directors in Southern Africa (IoDSA) established in July 1993 the King Committee on Corporate Governance: it produced the first *King Report on Corporate Governance* which was published in 1994. The first *King Report* was recognized internationally, when published, as the most comprehensive publication on the subject embracing the inclusive approach to corporate governance. The *King Report on Corporate Governance for South Africa* – 2002 (*King II Report*) was launched at an Institute of Directors (IoDSA) Conference attended by 700 persons at the Sandton Convention Centre, 26 March 2002. The Institute of Directors in Southern Africa (IoDSA) formally introduced the *King Code of Governance Principles* and the *King Report on Governance (King III*) at the Sandton Convention Centre in Sandton, Johannesburg, in 2009. *King III* came into effect on 1 March 2010 – until then *King II* applied. The new *Code* and *Report* also falls in line with the Companies Act no 71 of 2008, which became effective on 1 May 2011. Like its 56 commonwealth peers, *King III* has been written in accordance to comply or explain principle based approach of governance, but specifically the apply or explain regime. This regime is currently unique in the Netherlands and now in South Africa. Whilst this approach remains a hotly debated issue globally, the *King III* Committee continues to believe it should be a non-legislative code on principles and practices.

Available:

https://iodsa.site-ym.com/store/ListProducts.aspx?catid=177819

https://jutalaw.co.za/uploads/King_III_Report/#p=1

UNECE High-Level Group for the Modernisation of Official Statistics (HLG-MOS)

Modernisation Committee on Standards

Reference released Models:

- *Generic Activity Model for Statistical Organizations (GAMSO), Version 1.0.* March, 2015
- *Generic Statistical Business Process Model (GSBPM), Version 5.0.* December, 2013

Highlights

The UNECE High-Level Group for the Modernisation of Official Statistics (HLG-MOS) was set up by the Bureau of the Conference of European Statisticians in 2010 to oversee and coordinate international work relating to statistical modernisation. It promotes standards-based modernisation of statistical production and services. It reports directly to the Conference of European Statisticians and received its mandate from this body. The mission of the HLG-MOS is to oversee development of frameworks, and sharing of information, tools and methods, which support the modernisation of statistical organizations. The aim is to improve the efficiency of the statistical production process, and the ability to produce outputs that better meet user needs.

The Joint UNECE / Eurostat / OECD Work Sessions on Statistical Metadata (METIS) have prepared a Common Metadata Framework (CMF). Part C of this framework is entitled "Metadata and the Statistical Cycle". This part refers to the phases of the statistical business process and provides generic terms to describe them. Since November 2013, this work has been taken over by the *Modernisation Committee on Standards*, under the HLG-MOS. During a workshop on the development of Part C of the CMF, held in Vienna in July 2007, the participants agreed that the business process model used by Statistics New Zealand would provide a good basis for developing a Generic Statistical Business Process Model. Following several drafts and public consultations, version 4.0 of the GSBPM was released in April 2009. It was subsequently widely adopted by the global official statistics community, and formed one of the cornerstones of the HLG vision and strategy for standards-based modernisation. In December 2012, a complementary model, the Generic Statistical Information Model (GSIM) was released. The work to develop and subsequently implement the GSIM resulted in the identification of several possible enhancements to the GSBPM. During 2013, the HLG launched a project on "Frameworks and Standards for Statistical Modernisation" which included a broader review of the GSBPM and the GSIM, to improve consistency between the documentation of the models, and to incorporate feedback based on practical implementations. The current version of the GSBPM (version 5.0) is the direct result of this work. Whilst it is considered final at the time of release, it

is also expected that future updates may be necessary in the coming years, either to reflect further experiences from implementing the model in practice, or due to the evolution of the nature of statistical production.

The *Generic Activity Model for Statistical Organizations* (GAMSO) Version 1.0 was endorsed for release by the HLG-MOS on 1 March 2015. Statistical organizations are invited to use GAMSO and provide feedback based on practical implementations on the GAMSO Review. GAMSO will be reviewed in 2016 taking into account this feedback. GAMSO describes and defines the activities that take place within a typical statistical organization. It extends and complements the GSBPM by adding additional activities needed to support statistical production. When the GSBPM was developed, such activities were referred to as over-arching processes, and were listed, but not elaborated in any great detail. Over the years there have been several calls to expand the GSBPM to better cover these activities. The GAMSO was therefore developed to meet these needs.

Available:

http://www1.unece.org/stat/platform/display/GAMSO/GAMSO+v1.0

http://www1.unece.org/stat/platform/display/metis/The+Generic+Statistical+Business+Process+Model

UK HM Treasury - Government Financial Management Directorate

Reference published Guidance:

- *The Orange Book Management of Risk - Principles and Concepts*. October, 2004

Highlights

In central government a number of reports, particularly the National Audit Office's 2000 report "Supporting innovation – managing risk in government departments" and the Strategy Unit 2002 report "Risk – improving government's capacity to handle risk and uncertainty", have driven forward the risk management agenda and the development of Statements on Internal Control. In 2001 Treasury produced "Management of Risk – A Strategic Overview" which rapidly became known as the *Orange Book*: it provided a basic introduction to the concepts of risk management that proved very popular as a resource for developing and implementing risk management processes in government organizations. This Guidance is the successor to the 2001 *Orange Book*. It continues to provide broad based general guidance on the principles of risk management, but has been enhanced to reflect the lessons learned about risk management through the experience. The most significant shift since the publication of the 2001 is that all government organizations had, in 2004, basic risk management processes in place. This means that the main risk management challenge did not lie in the initial identification and analysis of risk and the development of the risk management process, but rather in the ongoing review and improvement of risk management. It focuses on both internal processes for risk management and consideration of the organization's risk management in relation to the wider environment in which it functions.

Available:

https://www.gov.uk/government/publications/orange-book

Academic sources, institutional papers and professional handbooks:

Aabo, T., Fraser, J., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at hydro one. *Journal of Applied Corporate Finance*, 17(3), 62–75.

Alarm, The Public Risk Management Association – UK (2010). *The National performance Model for Risk Management in the Public Services.*

Ariff, M. S. M., Zakuan, N., Tajudin, M. N. M., & Ismail, K. (2015). A conceptual model of Risk Management Practices and organizational performance for Malaysia's Research Universities. *The Role of Service in the Tourism & Hospitality Industry*, 153.

Australian Government, (2013). *Comcover Risk management Maturity Model*

Bodein, S., Pugliese, A. & Walker, P. A road map to risk management. *Journal of Accountancy*, December 2001, Volume 192, Issue 6, pp 65-70.

Bruce, R. (2005). Swift message on risk management. *Accountancy* (April), 22.

Bruno-Britz, M. (2009). The age of ERM. *Bank Systems & Technology*, 1 (February), 20.

Burton, E. J. (2008). The audit committee: How should it handle ERM? *The Journal of Corporate Accounting & Finance*, 19(4), 3–5.

Chenhall, R. H., & Euske, K. J. (2007). The role of management control systems in planned organizational change: An analysis of two organizations. *Accounting, Organizations and Society*, 32, 601–637.

Chua, W. F. (2007). Accounting, measuring, reporting and strategizing – Re-using verbs: A review essay. *Accounting, Organizations and Society*, 32(4–5), 487–494.

CMMI Product Team (2002). *Capability Maturity Model Integration (CMMI)*, Software Engineering Institute (SEI).

Curtis, E., & Turley, S. (2007). The business risk audit – A longitudinal case study of an audit engagement. *Accounting, Organizations and Society*, 32, 439–461.

Drennan, L. T., McConnell, A., & Stark, A. (2014). *Risk and crisis management in the public sector*. Routledge.

Epstein, M.J., & Rejc, A. (2006). *The reporting of organisational risks for internal and external decision makers*, Management Accounting Guideline, Canada: The Society of Management Accountants of Canada (CMA-Canada)

European Statistical System Committee (ESSC) - Vision Implementation Group & Vision Implementation Network (2015). *Identification and Evaluation of Risks to ESS Vision 2020 Implementation*.

Fraser, I., & Henry, W. (2007). Embedding risk management: Structures and approaches. *Managerial Auditing Journal*, 22(4), 392–409.

Gates, S. (2006). Incorporating strategic risk into enterprise risk management: A survey of current corporate practice. *Journal of Applied Corporate Finance*, 18(4), 81–90.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies*, 30(02&03), 141–155.

Government Centre for information Systems (1993) *Introduction to the Management of Risk.* HMSO, Norwich.

Greenwood, R., & Hinings, C. R. (1993). Understanding strategic change: The contribution of archetypes. *The Academy of Management Journal*, 36(5), 1052–1081.

Griffioen, R., van Delden, A., & de Wolf, P.P. (2012). BLUE-Enterprise and Trade Statistics-SP1-Cooperation-Collaborative Project Small or medium-scale focused research project FP7-SSH-2009-A Grant Agreement Number 244767 SSH-CT-2010-244767. *Deliverable 7.3*.

Hillson, D. A. (1997) '*Towards a Risk Maturity Model*'. The International Journal of Project & Business Risk Management, Vol.1

Holton, G. A. (2003). *Value-at-risk: Theory and practice*. San Diego, CA: Academic Press.

Hopkin, P. (2014). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Hopkinson, M. (2000) *Risk Maturity Models in practice*. Risk Management Bulletin, 5.

Hutter, B. M., & Power, M. (2005). *Organizational encounters with risk*. Cambridge University.

IACCM – The International Association for Contract & Commercial Management (2002), *Business Risk Management Maturity Model (BRM),* Business Risk Management Working Group.

IIRM (Investors in Risk Management), (2015). *Risk Management Maturity Model (RMMM)*.

IMA – Institute of Management Accountants (2006). *Enterprise risk management: Frameworks, elements, and integration, statements on management accounting*.

Jaafari, A. (2001). Management of risks, uncertainties and opportunities on projects: Time for a fundamental shift. *International Journal of Project Management*, 19(2), 89–101.

Lam, J. (2003). *Enterprise risk management: From incentives to controls*, Hoboken. New Jersey: Wiley.

Lam, J. (2006). *Emerging best practices in developing key risk indicators and ERM reporting*. James Lam & Associates, Inc..

Lampel, J., Shamsie, J., & Shapira, Z. (2009). Rare events and organizational learning. *Organization Science*, 20(5), 835–845.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37–52.

Martin, D., & Power, M. (2007). *The end of enterprise risk management*. Aeibrookings Joint Center for Regulatory Studies, August.

MC Connell, P. (2012). *Operational Risk Management Maturity Model (ORMMM)*

Mikes, A. (2005). Enterprise risk management in action. *Centre for the analysis of risk and regulation (CARR) discussion paper report series no. 35*.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18–40.

Miller, K. D. (1998). Economic exposure and integrated risk management. *Strategic Management Journal*, 19(5), 497–514.

Miller, K. D. (2009). Organizational risk after modernism. *Organization Studies*, 30(2/3), 157–180.

Miller, P., Kurunmaki, L., & O'Leary, T. (2008). Accounting, hybrids and the management of risk. *Accounting, Organizations and Society*, 33(7–8), 942–967.

Orsini, B. (August 2002) *Mature Risk Management Diagnostic Tool,* The Internal Auditor.

Page, M., & Spira, L. F. (2004). *The turnbull report, internal control and risk management: The developing role of internal audit*. Institute of Chartered Accountants: Scotland.

PMI Risk Significant Interest Group (2002), *Risk Management Maturity Model (RMMM)*, RiskSIG.

Porter, M. E. (1990). The Competitive Advantage of Nations. *Harvard Business Review 68*, no. 2 (March–April 1990): 73–93.

Power, M. (2004). *The risk management of everything*. London: Demos.

Power, M. (2007). *Organized uncertainty designing a world of risk management*. Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6–7), 849–855.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organizing in late modernity. *Organization Studies*, 30(2–3), 301–324.

Price, T. (2008). Uncovering unknown risk. *Wall Street & Technology*, 1 (December), 36.

PricewaterhouseCoopers (2004). Managing risk: An assessment of CEO perspectives. New York: PwC.

Pritchard, C.L. et al. (2014). *Risk management: concepts and guidance*. CRC Press.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27(2/3), 183–213.

Rieger, L. (2005). Success factors for implementing enterprise risk management. *Bank Accounting and Finance*, 18(3), 21–26.

Risk and Insurance Management Society and LogicManager (2008). *Risk Maturity Model for Enterprise Risk Management* (RIMS).

Rittenberg, L., & Covaleski, M. A. (2001). Internalization versus externalization of the internal audit function: An examination of professional and organizational imperatives. *Accounting, Organizations & Society*, 26(7–8), 617–641.

Sarma, M., Thomas, S., & Shah, A. (2003). Selection of value-at-risk models. *Journal of Forecasting*, 22(4), 337–358.

Scapens, B., & Bromwich, M. (2009). Editorial: Risk management, corporate governance and management accounting. *Management Accounting Research*, 20(1), 1.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal*, 16(4), 640–661.

Statistics Netherlands. van Nederpelt, P.W.M. (2010). *A new model for quality management*. The Hague/Heerlen.

UK HM Treasury - Government Financial Management Directorate, (2009). *Risk Management assessment framework: a tool for departments*.

Taleb, N. N. (2007). The Black Swan: The impact of the highly improbable. Random House.

The Institute of Internal Audit, (2010). *Risk management Maturity Model*

Walker, P. L., Shenkir, W. G., & Barton, T. L. (2003). ERM in practice. *Internal Auditor*, 60(4), 51–55.

Walker, P., Shenkir, W., & Barton, T. (2002). *Enterprise risk management: Pulling it all together*. Altamonte Springs: Institute of Internal Auditors Research Foundation.

M Wheatley, (2007) *"Maturity Matters"*, PM Network.

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations, and Society*, 32(7–8), 757–788.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, 20(1), 69–81.

Zolkos, R. (2008). Financial crisis shows real need for ERM. *Business Insurance*, 6(October), 6.

Глоссарий

Приемлемый риск

часть выявленного риска, которая допустима после применения воздействия контроля. Риск может быть признан приемлемым, когда есть нехватка денег или когда дальнейшие усилия по его сокращению могут привести к ухудшению вероятности успеха операции или к пределу, за которым начинается уменьшение прибыли.

Связь и консультации

непрерывные и цикличные процессы, которые проводит организация для предоставления, обмена или получения информации и ведения диалога с заинтересованными сторонами и другими лицами в отношении управления рисками. Информация может относиться к существованию, характеру, форме, вероятности, серьезности, оценке, приемлемости, ведению или другим аспектам управления рисками. Консультация представляет собой двухсторонний процесс информированного общения между организацией и ее заинтересованными сторонами или другими лицами, по вопросу до принятия решения или определения направления по конкретному вопросу.

Консультация:

- процесс, который влияет на решение посредством влияния, а не власти; а также
- вклад в принятие решений, а не совместное принятие решений

Контроль

любые действия, предпринимаемые руководством, советом директоров и другими сторонами для управления рисками и повышением вероятности достижения поставленных целей и задач. Эти действия могут быть предприняты для управления либо воздействием, если риск происходит, либо частотой происхождения риска. Элементы управления включают любой план, процесс, политику, устройство, практику или другие действия, которые изменяют риск, а также организуют и направляют выполнение достаточных действий, чтобы обеспечить разумную уверенность в том, что цели будут достигнуты. Элементы управления могут не всегда оказывать предполагаемый или ожидаемый модифицирующий эффект. После того, как риски происходят, ведение риска переходит в контроль или изменение существующих средств контроля.

Управление рисками в масштабах всего предприятия

структурированный, последовательный и непрерывный процесс охватывающий всю организацию, для выявления, оценки, принятия решений и ответов на возможности и угрозы влияющие на достижение его целей.

Определение контекста

становление внешних и внутренних параметров, которые необходимо учитывать при управлении рисками, а также определение сферы действия и **критериев риска** для **политики управления** рисками.

Событие

возникновение или изменение определенного набора обстоятельств. Событие – это одно или несколькопроисшествий, которое может происходить нескольким причинам. Событие

может состоять из чего-то, чего не происходит. Событие иногда можно назвать «инцидентом» или «несчастным случаем».

Внешний контекст

- внешняя среда, в которой организация стремится достичь своих целей. Внешний контекст может включать:

  • культурную, социальную, политическую, правовую, нормативную, финансовую, технологическую, экономическую, природную я и конкурентная среду, будь то на международном, национальном, региональном или местном уровне;

  • ключевые факторы и тенденции, влияющие на цели организации; а также• отношения с внешними заинтересованными сторонами и их восприятие и ценности .

Выявленный риск

обнаруженный посредством аналитических методов риск. Время и затраты на усилия по анализу, качество программы управления рисками и состояние задействованной технологии влияют на количество выявленныхрисков

Неотъемлемый риск

риск для организации в отсутствие какого-либо управления действиями может повлиять на вероятность или влияние риска. Эти риски могут возникнуть в результате развития отрасли, стратегии и факторов окружающей среды.

Внутренний контекст

- внутренняя среда, в которой организация стремится достичь своих целей. Внутренний контекст может включать:
  - управление, организационную структуру, роли и подотчетность;
  - принципы, цели и стратегии, которые существуют для их достижения;
  - возможности, понятные с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);
  - восприятие и ценности заинтересованных лиц внутри организации;
  - информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);
  - отношения с заинтересованными лицами внутри организации и их восприятие и ценности;
  - культуру организации, целостность, этические ценности;
  - стандарты, руководящие принципы и модели, принятые организацией;
  - форму и объем договорных отношений.

Воздействие

представляет потенциальные влияние и последствия для организации и ее целей, связанные с конкретным событием. Событие может привести к ряду последствий. Последствие может быть определенным или неопределенным и может оказывать положительное или отрицательное воздействие на цели. События, которые оказывают положительноевоздействие, представляют собой возможности, а те события, которые

оказывают негативные последствия, представляют собой риски. Последствия могут быть выражены качественно или количественно. Организации часто характеризуют события, исходя из суровости, воздействий или сумм в денежном выражении. Первоначальные последствия могут усугубляться из-за косвенного воздействияs.

Уровень риска

величина **риска**, выраженная в условиях сочетания **последствий** и их **вероятности**.

Вероятность

вероятность того, что событие может произойти. Она может быть определен, измерена или выявлена объективно или субъективно, качественно или количественно, и её можно описать с использованием качественных терминов (таких как высокие, средние и низкие) или количественных показателей (таких как процент и частота).

Мониторинг

постоянная проверка, контроль, критическое наблюдение или определение статуса, с целью определения изменений в обязательном или планированном уровне производительности. Мониторинг может быть применен к **структуре управления рисками, процессу управления рисками, риску или контролю.**

Остаточный риск

часть общего **риска**, оставшегося после возле **воздействия на риск**. Остаточный риск включает **приемлемыйриск** и **неопознанный риск**. Руководство должно решить, находится ли этот остаточный риск в пределах готовности организации к риску. Остаточный риск также известен как «удержанный риск».

Риск

возможность возникновения события, которое повлияет на достижение целей. Эффект - отклонение от ожидаемого (положительного и / или отрицательного). Цели могут иметь различные аспекты (например, финансовые, медицинские и безопасные, а также экологические цели) и могут применяться на разных уровнях (например, стратегический, общесистемный, проект, продукт и процесс). Вся деятельность организации связана с риском. Организации управляют риском, идентифицируя его, анализируя его, а затем оценивая, должен ли риск быть изменен путем воздействия на него для соответствия с их критериями риска. Риск часто характеризуется со ссылкой на потенциальные события и воздействие или их комбинацию. Риск измеряется с точки зрения воздействия (включая изменения обстоятельств) и вероятности возникновения. Неопределенность - это состояние, даже частичное, недостатка информации, связанной с пониманием или знанием события, его последствий или вероятности.

Анализ риска

процесс постижения характера риска и определения уровня риска. Анализ рисков обеспечивает основу для оценки риска и принятия решений о воздействия на риск. Анализ рисков включает оценку риска.

Готовность к риску

количество и тип рисковдопустимых для организации в условиях достижения своей цели и предоставления выгодного предложения заинтересованным сторонам. Готовность к риску - это заявка более высокого уровня, где широко рассматриваются уровни рисков приемлемые для руководстваю Она отображает основные принципыуправления рисками предприятия и, в свою очередь, влияет на культуру и стиль работы предприятия. Многие субъекты определяют свою готовность к риску качественно, в то время как другие используют более количественный подход.

Оценка риска

общий процесс **идентификации рисков**, **анализ рисков**, **измерения риска** и **оценки риска**.

Отношение к риску

подход организации для оценки и в конечном итоге воздействия, удерживания, принятия или оухода от риска.

Предотвращение риска

Подход ухода от риска.

Критерии риска

Исходные требования, на основании которых оценивается значение риска. Критерии риска основаны на организационных целях и внешнем и внутреннем контексте. Критерии риска могут быть получены из стандартов, законов, принципов и других требований.

Подверженность риску

последствия, как сочетание воздействия и вероятности, которые организации могут испытать, если осуществится конкретный риск.

Выявление риска

процесс поиска, распознавания и характеристики рисков. Выявление риска включает в себя идентификацию источников риска, событий, их причин и их потенциальных последствий. Выявление риска может включать в себя исторические данные, теоретический анализ, информированные и экспертные заключения, а также потребности заинтересованных сторон.

Управление рисками

скоординированные действия по контролю и управлению организацией в отношении риска

Структура управления рисками

совокупность структур, методологии, процедур и определений, которые выбрала организация для разработки, внедрения, мониторинга, пересмотра и постоянного совершенствования управления рисками во всей организации. Основные положения включают политику, цели, мандат и обязательство по управлению рисками. Организационные механизмы включают планы, отношения, подотчетность, ресурсы, процессы и мероприятия. Рамки управления рисками включены в общую стратегическую и оперативную политику и практику организации.

План управления рисками

схема в рамках структуры управления рисками, определяющаю подход, компоненты и ресурсы управления для применения в управления рисками. Компоненты управления обычно включают процедуры, практику, распределение обязанностей,

последовательность и время действий. План управления рисками может быть применен к конкретному продукту, процессу и проекту, а также части или всей организации

Политика управления рисками

заявление об общих намерениях и направлении организации, связанной с управлением рисками.

Процесс управления рисками

систематическое применение политики, процедур и практики управления к информированию, консультированию, установлению контекста и определению, анализу, оценке, обработке, мониторингу и анализу рисков, с целью обеспечениядостаточной гарантии для достижении целей организации.

Карта рисков

графическое представление вероятности и влияния одного или нескольких рисков. Карты риска могут содержать количественные или качественные оценки вероятности и воздействия риска. Часто карты рисков называются «тепловыми картами», поскольку они представляют уровни риска по цвету, где красный цвет представляет собой высокий риск, желтый умеренный риск и зеленый низкий риск.

Зрелость рисков

измерение уровня развития практики управления рисками внутри организации на основании различных переменных и / или измерений, характеризующихся организационным поведением и показателями.

Оценка риска

присваивание значения каждому риску с использованием определенных критериев. Большинство организаций определяют шкалы для рейтинговых рисков с точки зрения воздействия, вероятности и других аспектов.

Ответственный за риск

подотчётные лица или организации наделённые полномочиями на управление рисками.

Профиль риска

описание любого набора рисков. Набор рисков может содержать риски относящиеся ко всей организации, части организации или,иначе как будет указано.

Регистр рисков / журнал рисков

основной документ, который регистрирует выявленные риски, их степень суровости и ответные действия, которые должны быть приняты.

Источник риска

компонент, который сам по себе или в совокупности обладает внутренним потенциалом для возникновения риска. Источник риска может быть материальным или нематериальным.

Стратегия риска

общий организационный подход к управлению рисками, определяемый субъектом, регулирующим управление рисками. Стратегия должна быть документирована и легко доступна на всех уровнях организации

Переносимость рисков

приемлемый уровень вариации относительно достижения конкретной цели. Этот вариант часто измеряется с использованием тех же единиц, что и связанная с ним цель. При установлении переносимости рисков руководство считает относительную важность связанной задачи и согласовывает переносимость риска с готовностью к риску. Таким образом, предприятие, работающее в узких рамках в отношении переносимости риска, допускает расширенные рамки по отношению к готовности к риску.

Обработка рисков

средства, с помощью которых организация выбирает управление отдельными рисками. Обработку риска также можно назвать реакцией на риск. В рамках управления рисками предприятия для каждого значимого риска предприятие рассматривает потенциальные ответные реакции из ряда категорий ответных реакций. Обработка риска может включать:

• **Предотвращение / Прекращение действия** - реагирование, в результате которого вы избегаете действий, которые вызывают риск. Некоторые примеры избежания - это выход из линейки продуктов, продажа подразделения или принятие решения о расширении.

• **Воздействие / Сокращение** - это реагирование, в результате которого принимаются меры для уменьшения вероятности и воздействия риска.

• **Передача / Обмен** - это реагирование, в результате которого снижается вероятность и влияние риска путем совместной деятельности или передачи части риска. Чрезвычайно распространенное реагирование- это страхование.

• **Толерантность / Принятие** - это реагирование, в результате которого,не предпринимаются никакие действия, чтобы повлиять на вероятность или эффект риска.

• Обработки рисков, которые касаются негативных последствий, иногда называются «смягчение рисков», «устранение рисков», «предотвращение рисков» и «снижение риска». Обработка рисков может создавать новые риски или изменять существующие риски.

Взвешивание рисков

процесс сравнения результатов анализа риска с критериями риска для определения приемлемого или допустимого риска и / или его величины. Это процесс определения приоритетов управления рисками путем сравнения уровня риска с предопределенными целевыми уровнями риска и порогами допустимого. Оценка риска помогает в принятии решения об обработке риска.

Обзор

действия проводимые для определения пригодности, адекватности и эффективности изучаемого предмета для достижения установленных целей. Обзор может применяться к рамкам управления рисками, к процессу управления рисками, к риску или контролю.

Заинтересованная сторона

лица или организации, которые могут повлиять, пострадать от решенияили деятельности, связанной с риском. Лицом, принимающим решения, может быть заинтересованная сторона.

Общий риск

сумма выявленного и неопознанного риска. В идеале выявленный риск будет включать большую долю этих двух.

Недопустимый риск

часть идентифицированного риска, которая не может быть допущена, и должна быть устранена или контролироваться.

Неопознанный риск

этот риск еще не определен. Некоторые риски невозможно выявить и оценить. Исследования Mishap могут выявить некоторые ранее неопознанные риски.