5. Principles

PRINCIPLE 1: Define your appetite for risk, and make it real

A fundamental principle of Agile delivery is the focus on meeting customer needs and a fundamental principle of risk management is providing assurance that an organisation understands and mitigates the threats to delivery. In order to allow an organisation to understand the needs of its customers and also provide assurance when needed to manage risk, the definition and agreement to use risk appetite levels is essential.

Traditional approaches to the definition of risk appetite focus on simple descriptions of appetite across different business dimensions, or even for the organisation as a whole. For example an organisation may state it is ‘averse’ to risk around information security, or ‘cautious’ around financial risk. These simple statements of appetite may give a broad indication but are open to interpretation (one person’s ‘cautious’ is another person’s ‘actively seeking’) and can remain static over a period of time.

An alternative approach and one that is more suited to risk management in an Agile environment is to define risk appetite in a way that drives correct and consistent behaviours within the organisation in line with expectations of its senior stakeholders. In order to achieve this, the organisation needs to agree to the behaviours expected at different levels of risk appetite and articulate these specifically as a framework for decision making.

The main benefit of this approach is that it sets clear behaviours that are expected at different levels of risk appetite, rather than a series of bland statements open to interpretation. The articulation of behaviours in this way will give clarity to the organisation of the expectations and allow for the risk appetite to cascade and align through the organisation. Risk management in an Agile environment, where risk is focussed on decision making is a key enabler to success.

Figure 6 shows an example of a risk appetite statement for a particular type of risk, in this case ‘Data Security’, and how the expected behaviours can be articulated to ensure consistency in decision making.

PRINCIPLE 2: Identify threats and opportunities

Risk management in an Agile environment remains important to identify both threats and opportunities. However, the approach to this identification should be clearly linked to the organisation’s objectives, the decisions it needs to take, and its defined risk appetite. Risk identification can follow these steps for individuals within the organisation:

- The business plan or project plan articulates the deliverable
- Decisions need to be made to ensure successful delivery (to get from A to B as effectively as possible)
- Align the decision you make to the risk appetite which relates to the activity
- Decisions which create threats or opportunities outside appetite require someone to take responsibility, to document on the corporate risk system, and to manage
- If you make a decision to achieve delivery which creates a threat above or beyond the risk appetite, you must then choose to either treat the risk, or tolerate it
• If you choose to treat a threat or opportunity, you must provide evidence of what you are doing to decrease the threat to within the appetite level.
• If you choose to tolerate (accept) the threat, you must document the threat on the risk register.

These steps should help to ensure that risk management is integrated into delivery and is not a separate process from the day to day operations of the organisation. They are also useful in ensuring the ‘right’ (true and honest) threats or opportunities are identified, so effort can be focused on the true threats to delivery rather than documenting generic ‘non’ threats to provide false assurance. The diagram at figure 1 illustrates when and how threats/opportunities can be recorded or escalated (also related to Principle 3).

It should be recognised that this principle can be followed whether an organisation is operating with an Agile approach or not. However, it is the understanding of risks as opportunities as well as threats which demonstrates a more mature approach to risk management and this is particularly relevant in an Agile environment. Agile is focused on delivery and therefore exploiting opportunity risk to allow for quick delivery, to deliver incremental improvements and to meet customer needs is important. A shift of focus from mitigating threats (stopping bad things from happening) to exploiting opportunities (making good things happen) is fundamental to risk management in an Agile environment.

**PRINCIPLE 3: Deal with threats and exploit opportunities at the most appropriate level but document and escalate if necessary**

In order to support an Agile environment it is important for risk management to create an environment where decisions are taken at the right level, where staff are empowered and able to address threats and opportunities quickly and without having to follow an overly prescriptive process.

Figure 6 shows a ‘Pyramid of Uncertainty’ demonstrating the level of oversight for each level of risk. The pyramid shows that a large number of daily decisions will be risk-based, they should not all be logged on a corporate system or wrapped up in layers of governance. Risk management in an Agile environment is where decisions should be taken quickly in line with risk appetite and only formally recorded when wider action needs to be taken to mitigate the risk or exploit the opportunity.

Figure 6: The Pyramid of Uncertainty

However, in order to provide assurance around the management of risk an organisation should still evidence those decisions being made which create threats or opportunities above or below the risk appetite level.

As demonstrated in Figure 6, there will be a large number of decisions taken on a daily basis within any organisation, these will in themselves be mitigating risks and exploiting opportunities.

It is important that these decisions are taken as close as possible to where the impact will be, both in time and location within the organisation. In an Agile delivery environment these will be identified and addressed through the sprint process. Therefore, risk management in an Agile environment should focus on only logging threats or opportunities as formal corporate ‘risks’ if:

• Reasonable mitigation to try to manage the threat/opportunity can be evidenced, and
• The threat/opportunity isn’t already someone’s job, or an established process is in place to manage the threat/opportunity, and
• The threat or opportunity is outside the organisation’s risk appetite

Figure 7: Agile Risk Management Maturity Model
## Risk Appetite Maturity

<table>
<thead>
<tr>
<th>Issues</th>
<th>Maturity Level 1</th>
<th>Maturity Level 2</th>
<th>Maturity Level 3</th>
<th>Maturity Level 4</th>
<th>Maturity Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Simple statement of appetite</td>
<td>Statement of appetite across different business dimensions</td>
<td>Appetite statements underpinned by more detailed expectations for how the organisation should behave in order to live up to appetite</td>
<td>Appetite used as part of daily and strategic decision making. Appetite tolerances are challenged objectively at board level using existing behaviours as metrics</td>
<td>Appropriate decision making inherent within all decision making. Organisational and unconscious competency at evaluating risk decisions based on appetite to achieve strategy</td>
</tr>
</tbody>
</table>

## Risk Culture Maturity

<table>
<thead>
<tr>
<th>Issues</th>
<th>Maturity Level 1</th>
<th>Maturity Level 2</th>
<th>Maturity Level 3</th>
<th>Maturity Level 4</th>
<th>Maturity Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Employees, managers and leaders are aware that risk management is something that should be done, but do not understand why or how. Communications material on risk exists, but is not fully read and understood by all employees.</td>
<td>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 into the concept. Understand the theory and processes behind formal risk management, but may think of risk as a compliance tool/tick box exercise, not as a tool for real business improvement.</td>
<td>Employees, managers and leaders know how to identify, assess, address, monitor and report risk in a consistent, structured manner, in line with guidance. Real ownership for risk and actions exists. Management at all levels in the organisation 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.</td>
<td>In addition to level 3, employees: 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.</td>
<td>In addition to level 4, employees: Embedded and long-term partnership working regimes and relationships evidenced. 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.</td>
</tr>
</tbody>
</table>

## Risk Culture Maturity

<table>
<thead>
<tr>
<th>Issues</th>
<th>Maturity Level 1</th>
<th>Maturity Level 2</th>
<th>Maturity Level 3</th>
<th>Maturity Level 4</th>
<th>Maturity Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understand organisational activity to date, including senior management, Strategic Risks and existence of risk policy statement, Risk Framework/guidance and training programmes They understand who to contact for further support. Training is sought by, and for, key people. Understand, some of the key risks to the organisation and to their area. Understand there are formal procedures that need to be implemented, but not yet implemented them all (lack of skills or commitment). Low understanding or risk literacy. Risks are not formally identified or recorded.</td>
<td>Key employees 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: Risks identified and recorded but little action taken to truly mitigate threats or exploit opportunities.</td>
<td>Senior management are actively engaged in broadening their horizons on risk through participation in internal events and training. The organisation 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 Decision making closely aligned to organisational appetites Threats / opportunities outside appetite recorded and accepted or tolerated</td>
<td>Have key employees who probably, either have professional qualifications in risk management or who have track record for a proactive approach in this area, with an appetite for ongoing learning. These people are listened to. High profile individuals, such as Director Generals, noted for speaking at seminars on risk. Key risk champions or managers have skills to lecture and train other employees. The organisation is recognised as a centre of excellence and expertise across government and globally. All employees at all levels are aware of the importance of managing information assets effectively and appreciate the benefits of doing so</td>
<td></td>
</tr>
<tr>
<td>Issues</td>
<td>Maturity Level 1</td>
<td>Maturity Level 2</td>
<td>Maturity Level 3</td>
<td>Maturity Level 4</td>
<td>Maturity Level 5</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agile Delivery Maturity</td>
<td>Plans fixed up-front. Delivery is made with infrequent “big bang” launches.</td>
<td>Delivery teams holding the common Agile meetings (daily stand-ups, sprints and sprint planning, etc.), and low-level risks are dealt with here. But it’s still fairly superficial - at this level the overall/high level plans are still largely fixed, and launches are still infrequent. So the low level use of Agile hasn’t impacted the higher levels yet.</td>
<td>Launches/deliveries are much more frequent and value builds incrementally. It is accepted some risks/issues/concerns/uncertainties filter up from the delivery teams and do influence the higher level plans.</td>
<td>Organisation to be delivering value incrementally. Big bang launches are largely a thing of the past. Feedback from users, customers and the market is regularly used to reshape plans.</td>
<td>Management of uncertainty is built into all delivery plans and processes; teams (and the organisation) continually tests assumptions and hypotheses; value is delivered continuously and reaction to what’s delivered is fed back into the delivery process.</td>
</tr>
<tr>
<td>Risk and Agile Resource Maturity</td>
<td>No risk management team or Agile expertise employed by organisation</td>
<td>Specific risk management team in place, as well as Agile experienced teams in place</td>
<td>Risk management team and Agile teams collaborate regularly</td>
<td>Combined qualified, trained and experienced Agile and risk management network</td>
<td>Risk and Agile expertise formally part of all board decision making structure</td>
</tr>
</tbody>
</table>