6. Risk based control and audit

The internal control framework, which includes the risk management framework and the internal audit framework, differentiates among three levels of control:

- Internal control (preventative or subsequent), deployed within the risk management framework, under the responsibility of management (risk owners), aiming to prevent or reduce the consequences related to risk occurrence;

- “Compliance” level, aiming to help and monitor an actual risk management implementation by risk-owners; such a level oversees risk assessment and control processes also ensuring their consistency with organizational goals (risk management unit);

- “Risk based audit”, ensuring an effective deployment of audit resources to assess management of those risks related to the actions of an organization, by examining and evaluating the adequacy of the risk management system and internal controls, processes and management. Therefore, internal audit monitors and shows the progress of implementation of audit recommendations and improvements in the audited area.

The Risk Based Audit (RBA) objectives are as follows:

Ø Assurance for the risk management strategy: to ascertain the extent to which all line managers review the risks/controls within the scope of their own responsibility; to evaluate the adequacy of risk management policy and strategy for achieving their objectives;

Ø Assurance for management of risks/controls: to encompass all the key risks as well as enough of the other risks to support confidence in the overall opinion reached; to evaluate the adequacy of the risk management processes designed to constrain residual risk to the risk appetite;

Ø Assurance for the adequacy of the review/assurance process: quality assured to engender confidence in the review process; to identify limitations in the evidence provided, or limitations to the depth/scope of the reviews undertaken; to identify gaps in control and/or over control, and provide opportunities for continuous improvement; to support preparation of internal audit summary report to the risk committee/chief statistician.

The RBA management cycle is carried out through the following six steps:

a) Object: procedures, processes and internal service charters, risks selected according to priorities but: risks within risk appetite, risks not requiring audit in the short term, risks otherwise audited, tolerable risks.

b) Audit Plan: internal audits to be carried out in the short term are managed according to an annual plan that is endorsed by the board, and shared with the organizational divisions involved. Such a plan shows, with reference to any action: i) the audit lifespan, ii) the team composition, iii) the accountabilities, iv) the audit tasks (according to procedures, contractual requirements, etc.), v) the documents required, vi) the lead times. The annual plan is prepared for a single year on the basis of the strategic plan, according to risk assessment. Therefore, audit planning takes into account the results of previous audit studies, as well as management assessment of current levels of risk related to specific organizational programs.

c) Audit run-up, consisting of some actions that are preliminary to actual audit, such as: a) formal assignment of duties; b) definition of the activity plan; c) identification of documents needed to define the audit range of reference and intervention; d) communication on audit start; e) kick-off meeting with the staff involved.

d) Audit implementation, actual audit, consisting of: i) operational meetings; ii) preliminary assessment of criticalities; iii) check of suitability and accordance with the risk management or quality system; iv) drawing up recommendations and possible mitigation actions. Audits can be used to assist risk managers in assessing the effectiveness of controls for each risk. An assessment could be made on whether the controls are adequate to reduce the level of risk (i.e., to reduce the risk from extreme/high to medium or low), or whether additional treatments/controls are required.

e) Reporting. Auditing ends with a meeting for sharing the main results obtained. An audit report is drafted that contains: i) its findings, ii) the actions performed, iii) the criticalities found, and suggestions proposed, iv) possible action plan, in cooperation with the unit/division involved. Following the assessment of the control effectiveness for each risk, proposals for additional treatment strategies to reduce the level of risk will emerge, and some of the treatment strategies proposed during this process will be suitable for inclusion in the internal audit plan (feed-back).

f) The follow-up is aimed at checking the actual implementation of response actions related to any remarks or recommendations.
Q. With reference to risk management, internal controls and internal audit system within your organization, please detail the connection/integration between these ones

R. “Strategic Internal Audit Plan is consistent with the objectives contained in the Strategic Plan”.

(Source: Croatia Bureau of Statistics, In-depth survey on risk management practices)

R. “Once the key strategic/operational areas have been reviewed, the internal audit program will be prioritized on the agreed assessment and the risk rankings”

(Source: Australian Bureau of Statistics, In-depth survey on risk management practices)