



Australian Government

Comcover



Comcover Risk Management Benchmarking Survey 2010

Risk Management Capability Maturity Levels



Element One

Risk Management Policy and Objectives

Informal

There is no formal approach to determining the agency's risk management strategy, as a result there is inconsistency in the communication and understanding of the agency's risk management policy and objectives across the agency. Where a risk policy has been developed it has been done without consultation and therefore not aligned with the agency's objectives and/or business strategies.

The risk appetite of the agency is not understood by staff and varies from situation to situation. As staff are unaware of the context of the agency's appetite for risk tolerance levels are not documented.

The agency has no, or little, formal governance structures and processes around the assessment or approval of risks associated with the consideration and implementation of new policies, programs and/or services.

Basic

The agency's risk management strategy, including its risk management policy, has been considered at Senior Executive and/or the Board level but it is not linked into branch or business units' operations. It does not contain clear objectives or guidance against which to measure performance and communication to staff on the agency's approach to managing risk is limited.

While there is some understanding of the risk appetite at Senior Executive and/or the Board level this is not articulated into specific risk tolerance levels which can be applied or communicated throughout the agency. Risk limits are not fully understood or complied with across the agency.

The agency does have some formal governance structure and processes around the assessment and approval of risks associated with new policies, programs and/or services.

Top Down

The agency's risk management strategy, including its risk management policy, is established and understood across the agency. The agency's policy demonstrates clear links to the strategic objectives and operational/business plans of the agency, and articulates the accountability for managing risk at these levels.

The agency's risk appetite and tolerance level is clearly defined. Guidance on maintaining risks within acceptable levels of the agency's appetite and tolerance is communicated to all staff, enabling them to gain an understand of the agency's risk limits and the processes for assessing and managing risk.

There is a formal governance structure and process for the assessment and approval of the risks associated with the development of new policies, programs and/or services.

Structured

The agency's risk management strategy, including its risk management policy and procedures, is aligned with all classes of risk and consistently applied across the agency. It is linked to the agency's objectives, embedded in the agency's operating policies, can demonstrate return on investment and contains performance measures for both the accountability and management of risk.

The agency's risk appetite and tolerance levels are regularly reviewed. Reports provided to Senior Executive and/or the Board include the use of qualitative criteria to assess the agency's performance in managing risk against its agreed appetite and tolerance levels.

The agency has a risk rating model for all new policies, programs and/or services that contributes to the successful delivery of these activities by outlining the monitoring and assurance framework through planning and implementation phases.

Risk Intelligent

The agency's risk management strategy supported by its policy and procedures, clearly defines the relationship between the agency's management of risk, its risk appetite, the accountability for managing risk and the resources and processes dedicated to the management of risk. The risk management policy is embedded in business processes and is considered across all classes of risk.

The agency uses qualitative and quantitative analysis to define its risk appetite and this is consistently applied across the agency.

The agency has an integrated approach to strategic and operational planning with risk reporting provided to Senior Executive and/or the Board including information on the strategic risks of the agency as well as information on any new or emerging risks, large financial risks and risks identified as a result of the implementation of new policies, programs and/or services.



Element Two Accountability and Responsibility

Informal

Accountability and responsibility for managing risk is vague with roles and responsibilities across the agency not clearly defined. The agency does not have a risk manager or a risk management team responsible for implementing the agency's framework or policy.

There is a general lack of awareness to managing risk, demonstrated by individual branches or business units adopting an ad-hoc approach, with no evidence of reporting to the Executive.

The agency has no formal governance structure or processes around the assessment or the approval of risks associated with the agency's operations. Risk is not considered during implementation of new policies, programs and/or services.

Basic

The agency has a risk manager or team responsible for implementing the agency's risk management framework. Some risk management roles and responsibilities are defined within the agency, primarily at an Executive and/or Audit Committee level. The agency may have a risk committee but its role is one of information exchange. There remains some lack of clarity of roles and responsibilities at a branch or business unit level, evidenced by duplication or gaps in the reporting of risk.

There is generally no identification of accountability and responsibility specified in individuals performance agreements by linking the management of risk to the achievement of objectives or performance measures.

The agency has some formal governance structure and processes around the assessment and approval of risks associated with new policies, programs and/or services.

Top – Down

The agency does have a risk manager or risk management team responsible for implementing its risk framework and providing guidance to others on the agency's risk processes. The agency's risk management framework assigns responsibility with individual roles and responsibilities aligned and linked to performance appraisals.

The agency's Executive and/or Audit Committee make decisions on the management of individual risks based on input by branches or business units. The responsibility for managing risk across the agency is clear however the approach contains a degree of duplication between enterprise risks and specialist risk categories.

The agency has a clear definition of what constitutes a new policy, program and/or service and there is a formal

governance structure in place for the assessment of the risks associated with their development or implementation.

Structured

The agency's risk manager or team coordinates the implementation of the agency's framework, its risk profiles and action plans as well as evaluating risk planning to ensure consistency and accuracy of practice. The agency's framework assigns responsibility across the agency with individual roles and responsibilities aligned to the framework and linked to performance appraisals.

The agency's Executive and/or Audit Committee determine the agency's risk appetite and ensure continual improvement of the agency's framework. They review the agency risk profiles and the management of significant and critical risk areas.

Managers and Supervisors monitor the risks and risk profiles of their areas of responsibility and ensure staff are adopting the agency's risk management framework as developed and intended.

There is no duplication of risk management activities for different risk related functions across branches or business units, with the effective flow of information across the agency.

The agency has a clear definition of what constitutes a new policy program and/or service with a formal governance structure in place for the monitoring and assessment of the risks associated with their development or implementation.

Risk Intelligent

Senior Executive support the agency's risk manager or team to facilitate, challenge and drive risk management capability in the agency. A key responsibility of this role is to report to Senior Executive, the Audit Committee or the Board at regular intervals. Accountability and responsibility for risk is recognised as important for each of the following: the Chief Executive or Board; Senior Management Group; Audit Committee; Managers and Supervisors; the risk manager or risk management team, and staff at the branch or business unit level.

The agency's risks are clearly defined and aligned with individual branches or business units, specialist functions of the agency and specific risk classes. The management of risk is reflected in branch and business unit budgets, with the cost of risk being identified and managed effectively. The agency has a clear definition of what constitutes a new policy program and/or service with a formal governance structure in place for the monitoring and assessment of the risks associated with their development or implementation.



Element Three Integration

Informal

The agency's risk management framework is inconsistently defined and limited in its integration with its operations and overarching governance framework. Risk management is not a part of the agency's business planning, budgeting and reporting processes.

The cost of managing risk in the agency is high with the potential for duplication of resources, processes and individual risk treatments.

The definitions used to manage risk are inconsistently understood throughout the agency as there are no formal guidelines for identifying risk processes or differentiating between risk classes.

Basic

The agency has an established risk management framework however it may be applied or interpreted in an inconsistent manner, resulting in the creation of 'risk silos' across the agency. The definition of enterprise-wide risk and how it links to other categories of risk such as financial or strategic risk is not clear.

There is little evidence of embedding risk management into activities such as business planning, budgeting and reporting. The understanding of risk and how it can improve governance arrangements is not developed.

Top - Down

The framework for managing risk is understood and aligned with the agency's organisational structure. While the agency's risk processes (i.e. identification, assessment, monitoring, communicating and reporting) is consistent, the relationship between its risk management framework and specialist risk areas is not considered. This leads to an inconsistent approach in the reporting of risk to the Senior Executive and/or the Board.

There is little evidence of integration of the agency's enterprise wide risk management framework with business processes or its overarching governance framework.

Structured

The agency's risk management framework is embedded in its operational frameworks and processes ensuring: greater coordination across work areas; improved management reporting; and improved financial and operational viability.

The agency's approach to managing risk is a part of its overarching governance framework and recognised as key to effective business planning.

The agency's risk appetite has been defined and communicated to all staff to ensure an appropriate level of risk identification is undertaken when developing strategic and operational plans.

Specialist risk programs are documented and included in regular reports to Senior Executive and/or the Board.

Risk Intelligent

Implementation of the agency's risk framework is achieved through the use of clearly articulated risk processes and systems applied consistently across the agency to planning and decision making. The agency uses risk information to identify its risks and allocate responsibility for the management of these, as well as to recognise opportunities that arise as a result of good risk management.

The agency's framework is integrated with its overall approach to governance and planning and considers risks at all levels including specialist risks such as Occupational Health and Safety or Fraud.

The process of managing risk occurs at the policy, program and/or service delivery level and is evident in the collation and analysis of management information.



Element Four Review and Evaluation

Informal

There is little evidence to suggest ongoing monitoring of compliance with the agency's risk management framework occurs, ensuring the agency's approach to managing risk is consistent with its organisational goals and objectives.

Risk is not considered as part of the agency's annual audit program, and its risk management function is not separate to that of Internal Audit, leading to a lack of independence.

There is not a formal or co-ordinated approach to the collection of risk data to inform Senior Executive and/or the Board on how effectively risk is being identified, analysed, managed or communicated.

Basic

Review of the risk management framework is undertaken by the agency's Internal Audit function on an ad hoc basis. Risk is considered as an element to be discussed in the course of an internal audit but there is no formal process in place to review all elements of the agency's framework on an annual basis.

Risk information is used for historical analysis. The collection of data is not consistent across the agency, with the level of information recorded varying across branches or business units.

There is no process of moderating risk information from an agency wide perspective to: ensure a degree of accuracy or completion of an agency's risk register; determine whether the consequence and impact levels of individual risks are still relevant; and to reassess the effectiveness of current controls.

Top - Down

Internal audit performs regular reviews of all material risks and provides formal assurance to the Senior Executive and/or the Board of the validity of the framework. These reviews also consider those responsible and accountable for managing specific risks and a process has been implemented where individuals certify the performance of their responsibilities.

Staff responsible for implementing a specific policy, program or project review these risk profiles on a regular basis, to ensure that no new risks have emerged and treatment strategies are still appropriate and effective.

Structured

The agency evaluates its risk management framework annually. Senior Executive and Audit Committee undertake reviews using both qualitative and quantitative information to assess the soundness of the agency's risk management framework going forward. These reviews include reporting on compliance with the agency's framework as well as the oversight and monitoring of specific risk functions.

The validation process from Internal Audit becomes more forward-looking with data used to inform new initiatives, reflecting a move away from historical analysis to future predictions.

Those responsible for implementing a specific policy, program or project use performance measures to assess the effectiveness of treatments and controls. They also conduct regular reviews of their risk profiles ensuring that no new risks have emerged and that treatment strategies remain appropriate and effective.

Risk Intelligent

Regular communication of risk issues with the Senior Executive and/or the Board has ensured that the agency's risk management policy is aligned with its organisational objectives. The agency's context for managing risk is clearly established, its risk appetite is understood and the responsibilities for managing risk are consistent with the strategic direction of the agency.

The agency's framework contains validation and assurance processes on a real-time basis with weaknesses or deficiencies identified and addressed as they arise.

Risk information from data collected is consistent, fully retained and readily retrievable. Analysis is undertaken on the correlation of key risk indicators and quantitative measures of risk are used.



Element Five Positive Risk Culture

Informal

The culture of the agency does not reflect an understanding of the value that may be obtained by improving the risk management capability of the agency. There is little evidence that the agency understands, manages and accepts its risks and staff are unaware of the benefits of considering risk when undertaking their day to day responsibility. There is limited communication in the agency on the benefits of managing risk to staff or stakeholders.

The agency quickly puts unpleasant experiences and loss situations behind it without review, creating a culture that is risk adverse, ignorant of risk or overconfident with risk taking.

Basic

Senior managers and line managers across the agency, need to be encouraged to demonstrate their awareness of risk management when undertaking their day to day responsibilities. This includes, acknowledging good risk management practice and speaking with staff regularly about opportunities to better manage risk.

The agency avoids the mention of unpleasant experiences with its response to a loss situation being short term to ensure it does not repeat the mistake. This could be improved by ensuring lessons learnt are communicated to staff, to influence behaviour and shape internal attitudes towards risk.

The management of risk is considered to be an additional task and the engagement and acknowledgement of stakeholders' views is limited.

Top – Down

The agency has defined its approach to managing risk through its risk management policy. With formal governance structures and processes in place for the assessment and reporting of risk staff are aware of their responsibility. Senior Executives monitor the key risks of the agency and encourage staff to demonstrate a level of awareness when undertaking their day to day responsibilities.

Staff acknowledge stakeholders views and engage with stakeholders from a compliance perspective but this process is limited and not considered essential when assessing or determining the level or impact of specific risks.

The agency analyses loss incidents and identifies areas for improvement. However, feed-back into policies, procedures and related communication can be improved.

Structured

The agency has a risk management framework that is integrated with its overarching governance framework so that the task of managing risk is not regarded as an additional responsibility or burden. The importance of the management of risk is communicated by Senior Executive and rewarded when individuals excel in demonstrating this in their day to day responsibilities.

There is a sponsor at the Senior Executive level of the agency that leads and promotes risk management, and staff have adopted a risk based approach to the implementation of policies, programs, and/or services.

The agency learns from negative (loss) and positive situations so that policy and procedural changes are made to improve the management of risk in the future.

Risk Intelligent

The culture of the agency is one that demonstrates that risk is appropriately identified, assessed, communicated and managed, with this approach modelled and articulated by Senior Executive. The commitment to managing risk is displayed at all levels so that understanding, and accepting appropriate levels of risk is part of the agency's every day decision making processes.

The agency continuously improves its risk and business activities based on the outcome of both negative (loss) and positive situations. Continuous learning is highly integrated in the operations of the agency with its culture for managing risk measured as part of the agency's staff survey.



Element Six Resourcing

Informal

The cost of treating risk is not considered at a business or project level. As a result there may be a shortfall in the allocation of resources to the management of risk in the agency.

Individual Branches or Business units consider varying aspects of managing risk, but this is undertaken in a disjointed and un-coordinated manner across the agency.

The communication of risk issues with Senior Executive and/or the Board is on an ad-hoc basis and the roles and responsibilities of staff to manage risk is not defined or clearly allocated.

While there may be an understanding of managing risk in the agency it is not possible to determine the level of relevant skills, as a result, there may be a general lack of awareness as to how risk relates to an individual's day to day responsibilities.

Basic

Informal communications between Branches and Business Units has contributed to an inconsistent approach to managing risk across the agency. There is generally no link to the management of risk and an agency's budget, or the performance measures of an individual.

Risk management roles are generally filled by individuals with an understanding of risk but there is a general shortage of risk management expertise, with little training being offered to support the development of these skills.

Roles and responsibilities for the management of risk are communicated in a co-ordinated manner. However, the focus is primarily communicating to Senior Executive and/or the Board the oversight and management of specialist risk categories, such as Occupational Health and Safety and Business Continuity.

The role of co-ordinating risk management in the agency is shared with other responsibilities such as audit, security or facilities management.

There is a informal process in place to exchange risk information between the Senior Executive and/or the Board with individual Branches or Business Units. This approach leads to a lack of clarity in regards to those accountable for managing risk and those responsible for managing risk.

Top Down

The agency recognises the importance of fostering better risk management by ensuring suitable allocation of resources, including budget, at the Branch and or Business

Unit level. These resources can be used to manage and treat individual risks as well as develop an appropriate level of skill across the agency.

Staff responsible for implementing the agency's risk management framework are a dedicated resource to the risk management function with a well developed understanding of the agency and its operations.

Communication of risk issues with Senior Executive and/or the Board is as requested. As a result this may lead to duplication of information across the agency.

Structured

The risk manager or risk management team is responsible for assisting Branches or Business Units to identify and evaluate risk, ensuring a consistent and structured approach is applied. They also support the Senior Executive and/or the Board by providing clear and concise risk information that can be used to inform decision making.

There is an effective flow of information through the agency with a structured approach to the provision of information to Senior Executive and/or the Board that consolidates all risk data including that of specialist risks such as Occupational Health and Safety and Business Continuity.

There is a high degree of awareness and understanding of the cost of managing risk. This is also considered in the preparation of Branch and Business Unit budgets by allocating sufficient to train and inform staff on the agency's approach to managing risk, as well as fund the development of new systems and processes to identify, analyse and treat risk.

Risk Intelligent

The accountability and management of risk is clearly defined with Senior Executive and/or the Board receiving regular reports on the status and cost of managing risk from a single source of risk data.

The ongoing costs associated with the implementation of an agency's risk management framework, such as risk treatment, resourcing, education and communication, are identified and managed within an agency's operational budget.

The agency demonstrates an effective allocation and use of risk resources by focusing on priority areas for improvement, addressing underlying issues, and utilising the skill of existing resources.



Element Seven Communications and Training

Informal

The communication of risk internally and externally is limited. The processes of identifying, assessing and monitoring risk is not co-ordinated across the agency and relies heavily on the effectiveness of internal controls. Methods for measuring risk exposures are not formally documented and communicated and the impact of risk on external stakeholders is not defined.

There is limited discussion of risk in the agency with Senior Executive and/or the Board becoming aware of the impact of a specific risk once it has occurred. Risk information is communicated on an ad-hoc or need-to-know basis so staff are not informed of the processes for managing risk in a consistent manner.

Training of staff in either the risk management process or the agency's approach to managing risk is limited with no opportunity for staff to develop their expertise further.

Basic

The communication of risk within specialist risk areas demonstrates the development of a basic understanding of the principles of risk management in the agency.

While communication with the Executive and/or the Board may occur on an ad-hoc basis it only includes information on the specialist risks such as Occupational Health and Safety or Fraud. Branches and or Business Units may communicate with their stakeholders but this information is not shared across the agency.

Discussions of potential risks focus on a historical understanding of their previous impact and are not considered in setting future direction or decision making. There is limited evidence of sharing of skills and knowledge across the agency.

A training needs analysis has not been undertaken however awareness training may be provided for new staff as part of induction but it does not extend to the competency level required of their role.

Top – Down

The agency acknowledges the importance of communicating risk in a timely manner by providing information on the management of key risks and the effectiveness of the agency's risk management framework to line managers, Senior Executive and/or the Board at regular intervals. While the agency analyses incidents and identifies areas for improvement feed-back is not commonly used to improve policies, procedures and related communications.

External communication occurs to inform stakeholders of the management of key risks and to assist them in understanding the agency's approach to managing risk.

A training needs analysis has not been completed but communication of the agency's approach to managing risk is provided to staff through a variety of channels including staff newsletters and the agency's intranet site. Access to external training is provided if required.

Structured

Communication of risk is considered in the day to day activities of staff which contributes to the development of a basic understanding of the principles of managing risk across the agency. This level of communication ensures there is a shared understanding of risk and supports a consistent approach across all Branches and Business Units. It also assists to promote a greater understanding of how risk management can contribute to achieving an agency's objectives.

A training needs analysis has been undertaken and training is provided in accordance with the current level of awareness and the competency level required of staff to undertake their role. Internal and external training is promoted by the agency and induction training is undertaken by all new starters, regardless of level. Managers and Executive are encouraged to continue to develop their knowledge and skills through training programs and self development.

A lessons learnt approach, that considers mistakes and loss situations, exists to determine if internal processes need improvement. The agency actively shares the outcomes of this approach to improve staff awareness across Branches and Business Units.

Risk Intelligent

Communication of risk is considered across the agency with a high level of importance placed on ensuring a basic understanding of the principles for managing risk and the need to communicate or inform stakeholders in a timely manner.

There is a consistent approach to communicating and discussing risk, enabling staff to develop an understanding of how risk management contributes to achieving an agency's objectives.

Staff are informed of the agency's risk appetite and processes through a variety of communication and information channels. Each are regularly reviewed and updated as the agency's context for managing risk changes.



Element Seven **Communications and Training *continued***

A training needs analysis has been undertaken and attendance at both internal and external training is promoted to ensure that staff are educated on the aspects of managing risk that relate to their role. The agency has adopted a philosophy of 'continuous improvement' by providing the opportunity for staff to learn from the outcomes of both negative (loss) and positive situations by sharing of information through a lessons learnt approach with all staff.

Induction training is completed with all new starters, regardless of level, and managers are encouraged to develop their knowledge and skills through training and self development. The agency identifies and trains risk experts that are relied on to develop awareness and assist others to improve the risk management processes of the agency.



Element Eight Risk Assessment

Informal

The method for identifying, analysing, evaluating and treating risks is not formally documented, resulting in a strong reliance on traditional internal controls and an inconsistent approach to the identification of risk.

The agency does not collect risk data and there are no processes in place to identify gaps in assessment. Guidance for identifying the difference between various classes of risk does not exist therefore the benefits of aggregating risk, either by category or operational function, is not understood within the agency.

Methods for measuring risk exposures are not formally documented and are inconsistent throughout the agency.

Inconsistency or the absence of risk data prevents the identification of Branches or Business Units that may require assistance as well as not capturing the risk priorities of the agency.

Basic

The agency views the identification of risk as a corporate obligation but does not recognise value in the process. The agency may have established a simple process of risk identification and assessment but it is inconsistently applied across the agency and may not be applicable to all risks identified.

There is a lack of robustness in the process (e.g. no full coverage of hotspots, aggregation, or interdependencies) and the approach is not tailored or consistent in application. The understanding of individual risk and how they link to particular risk categories such as financial and strategic is not clear.

There is a lack of consistency in the level of risk data collected with information only being used for historical analysis. Whilst there may be some aggregation of risk data it does not include any analysis or correlation to support the efficient use of resources for the treatment of specific risks.

While there may be some tracking of risk data the data collected is not complete for all branches or business units. It also does not include controls and treatments for specific risks or indicate those responsible for managing these risks.

Top Down

The agency has methodologies and tools for risk identification and assessment (i.e. identification, assessment, monitoring, communicating and reporting) which are consistently applied by individual branches and business units. Branches and business units recognise the value of the risk process to inform decision making, so these processes are updated periodically.

The methodologies used identify specialist risk categories in the agency and these are aligned to the agency's structure. Some quantitative measurement is attempted using basic calculations based on judgemental estimates of impact and likelihood.

There are procedures for the retention of records and information relating to risk identification, measurement and monitoring undertaken previously.

Aggregation of the agency's operational risks occurs allowing the correlation of these risks to determine the financial impact or the cost of managing specific categories of risk.

Structured

The agency has developed a suite of integrated tools and methodologies to cover each aspect of the risk assessment process and this approach is embedded in branches and business units.

The tools developed are consistently applied and updated and there is an appropriate balance of controls (entity- vs. process-level, preventive vs. detective, manual vs. automated).

The agency uses a quantitative and qualitative model for measuring risk data using this information for future predictions, as well as completing analysis of historical precedence. Analysis of risk aggregation data is undertaken to develop a portfolio risk matrix that can be considered when determining the exposure to specific categories of risk, as identifying and developing appropriate controls.

Loss data is considered in the risk identification and assessment process however, analysis of this data is generally historical and assists 'after the event' reporting. The aggregation of risk occurs for all risk categories across the agency providing the opportunity to evaluate the agency's portfolio of risks, its volatility and any potential variables.

Risk Intelligent

The agency has a fully integrated approach to the assessment of risk underpinned by a suite of tools and methodologies that address each aspect of its risk assessment process.

The approach supports both the positive and negative outcomes from assessing risk. Ensuring that controls and treatments are included in risk management plans confirms there is no excessive use, or duplication, while also providing a cost vs. benefit analysis of the risk methodologies employed.

The agency captures risk data that identifies responsibility for the management and treatment of risks as well as analysis of key risk indicators, loss data modelling and quantitative/



Element Eight

Risk Assessment *continued*

qualitative measures. Sources of risk are analysed to identify common or shared risk drivers and resources are allocated to treat these. The model incentivises behaviour to ensure there are measurable benefits for improving the management of risk at a business level.

The agency has a complete set of loss data including internal and external losses and near miss experiences. Risk information from data collected is consistent and readily retrievable.

There is a robust and dynamic risk aggregation process at the enterprise level across all risk categories which supports the active management of the agency's portfolio risk matrix.



Element Nine

Risk Profiling and Reporting

Informal

Roles and responsibilities across the agency are not defined or clearly articulated in regards to the management or accountability of risk. Therefore the reporting and consideration of risk issues is performed in a disjointed and uncoordinated manner.

As access to Senior Executive and/or the Board is on an ad-hoc basis the risk appetite and the tolerance levels for managing risk are not communicated to staff. This leads to limited understanding of the agency's risk appetite at the branch and business unit level. There are no risk limits documented so the risk appetite and risk tolerance level of the agency may vary from situation to situation.

As a result of informal reporting processes the available risk information does not allocate clear responsibility for the management of risks at the branch or business unit level. Information may be disseminated on a need-to-know basis, however the Senior Executive and/or the Board are not engaged in the process of considering risk. At the operational level there is no ability to identify poor performing branches or business units or identify priorities for the management of risk.

The agency is not able to consider the cost of managing risk due to a lack of risk data. As a result, the allocation of resources may not be reflected in the agency's operating budget.

Basic

While there is a level of agreement of the risk appetite of the agency at the Senior Executive and/or the Board level this is not clearly articulated in the agency's risk management policy. Therefore specific risk tolerance levels are difficult to apply at the Branch or Business unit level.

Risk reports provided to the Senior Executive and/or the Board enable them to gain an historical understanding of risk but do not assist decision-making or action. There is limited oversight of the effectiveness of an agency's risk management framework. Internal Audit includes elements of the agency's risk management framework in their audit plan.

The agency considers the cost of managing risk although informally due to the quality and availability of data from branches and business units. As a result the allocation of resources to the treatment of risk is not reflected in the agency's operating budget.

Top – Down

The agency has articulated its risk appetite with the processes for the management of risk widely understood by staff at all levels of the agency. As a result the agency's appetite for risk, and how the agency manages its risks in line with its objectives, is clearly defined. Reporting of risk occurs on a regular basis enabling the consideration of key issues in a timely manner by the Senior Executive and/or the Board.

Internal Audit undertake regular reviews of all material risks and provide formal assurance to Senior Executive and/or the Board on the validity of all aspects of the framework. The risk management framework includes a process by which individuals certify the performance of their responsibilities.

The agency considers the cost of managing risk as a result there is a component of the agency's budget allocated to the costs associated with employing risk management resources. It does not reflect the costs of treatment strategies in the agency or activities such as education and training of staff in risk management.

Structured

Risk reporting to the Senior Executive and/or the Board includes the use of qualitative and quantitative criteria to assess performance against appetite and tolerance levels. Risk limits and processes are frequently communicated so that they are embedded in the agency's policies. The agencies risk appetite and tolerance form an integral part of reporting and these combined with the agency's approach to managing risk are also regularly reviewed by Senior Executive and/or the Board.

The agency considers the cost of managing risk at all levels to ensure a consistent approach resulting in a reduction in the duplication of management activities and an increased understanding of related risks across the agency. Also the allocation of resources reflected in the agency's operating budget, includes the treatment of key risks and the program costs associated with employing a risk management resource or team.

Regular reviews of compliance with the risk framework is undertaken by Internal Audit. Ongoing oversight and monitoring of the risk function also occurs on a regular basis so as to identify opportunities for improvement in the framework and processes of the agency.



Element Nine

Risk Profiling and Reporting *continued*

Risk Intelligent

The agency has developed their risk profile so it is able to translate the operational risks of the agency into a statement that reflects its risk context and risk appetite. This risk profile is reviewed and monitored regularly. The agency's risk appetite is consistently applied considering both qualitative and quantitative data at all levels of the agency.

Risk reporting is undertaken in real time, include specific risk categories and is used by staff at all levels of the agency. Reporting formats have been agreed and are tailored to target audiences.

As all roles and responsibilities for risk are clearly defined including: the alignment of specific risk categories; branches and business units; specialist functions; and internal audit, risk is embedded in a cost-efficient manner across the agency. Reporting on the total cost of managing risk is provided at both the operational level and the Senior Executive and/or the Board level.

Risk information from data collected is consistent, fully retained and readily retrievable with the agency being able to access loss data, including internal and external loss and near miss experiences.

The agency considers the cost of managing risk at all levels. As a result, the allocation of resources for managing risk is considered in the agency's operating budget. This includes the treatment of key risks and the costing of opportunities for improved processes or additional programs as a result of the identification of opportunities from the risk management process. It also includes program costs associated with employing a risk management resource or team and the delivery of an integrated risk management program, including activities such as education and communication and the development of additional tools such as a risk information system.



Element Ten

Business Continuity and Disaster Recovery

Informal

The agency has developed a Business Continuity framework however, it is not integrated with its overarching risk or governance framework.

Training and raising awareness of Business Continuity processes in the agency has commenced although there is not a clear understanding of the allocation of roles and responsibilities.

There is a limited level of documentation been approved by Senior Management and/or the Board.

Basic

The agency's Business Continuity framework is in place and raising staff's awareness of the agency's response to a business interruption event has commenced.

The agency's Senior Executive and/or the Board are yet to endorse the agency's framework and reporting of the performance of the agency's framework is ad-hoc. Testing of the framework has not been scheduled and regular performance reviews are not yet included in the agency's internal audit program.

Top – Down

The agency's Business Continuity framework is established and is linked with the agency's risk assessment and management strategy. Accountability and responsibility for key areas are defined.

Training and awareness of the agency's response to a business interruption event has been undertaken.

The activity of undertaking a Business Impact Analysis has been completed with all Branches and Business Units ensuring that preparatory controls are in place. Limited testing has occurred across the agency.

The agency's Executive and/or the Board has endorsed the agency's framework, and they receive regular reports on implementation of effectiveness of the agency's Business Continuity framework. However reporting of the performance of the agency's framework is not integrated with other aspects of the agency's overarching risk management framework.

Structured

The agency's Business Continuity framework has been endorsed by Senior Executive and/or the Board and is integrated with its governance and risk frameworks. The agency demonstrates an approach to Business Continuity Management which indicates that its policies are developed, implemented and maintained so that it is well placed to manage a business disruption event, as well as build agency resilience.

Business continuity testing and exercises are conducted on a scheduled basis and performance is reported to the agency's executive at regular intervals.

Risk Intelligent

The agency's Business Continuity framework a element of the agency's risk and governance framework. The agency's Senior Executive and/or the Board demonstrate support for building a resilient agency which is reflected in its approach to managing risk where incident management, emergency response management and IT disaster recovery are all considered and integrated with other management activities.

Senior Executive also recognise that an effective business continuity plan can deliver business improvements through the processes of regular testing and review.