Enterprise Risk Management (ERM) Self-assessment

Source: Texas State University.

This self-assessment was developed by Lynn Altemeyer as part of a research project. For further information refer to Altemeyer, Lynn, "An Assessment of Texas State Government: Implementation of Enterprise Risk Management Principles" (2004). Applied Research Projects. Paper 14. http://ecommons.txstate.edu/arp/14.

How the self-assessment can help BPIR members…

This self-assessment tool will help you to assess your current Enterprise Risk Management framework in order to consider where improvements might be made. The assessment could be carried out by different departments to highlight variations in understanding/application.

Assessment Questions (Mark one box per question with an 'x')	Don't Know	Disagree, or No Plans	Planned	Partly In Place	Implemented enterprise wide
A - Internal Environment					
A1 - The organisation views risk management as a means of preserving and creating value					
A2 - There is an overall risk management policy set out in a board-approved statement					
A3 - The board considers risk management a regular part of its oversight agenda					
A4 - The board constructively engages management on plans and performance					
A5 - The organisations attitude and approach to risk is clear and consistent with the level of risk (appetite) it is prepared to take					
A6 - Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks					
A7 - There is a senior management committee that oversees risk management					
A8 - There is a senior executive responsible for risk management					
B- Objective Setting					
B1- The organisation defines goals and objectives for the enterprise as a whole.					
B2 - An effective strategic planning process is in place to formulate strategies that will enable the organisation to achieve its business objective.					
B3 - Business strategies are clearly articulated with objectives linked					
B4 - The risk identification process is designed to make a clear link between the organisation's objectives and the associated risks.					
B5- Risk to the achievement of objectives is evaluated to ensure it does not exceed the levels of risk determined by the Board as acceptable.					
B6- Acceptable tolerance limits on the risk to the achievement of key objectives have been determined					
B7 - Management uses meaningful performance measures in monitoring results against other set tolerances					

Assessment Questions (Mark one box per question with an 'x')	Don't Know	Disagree, or No Plans	Planned	Partly In Place	Implemented enterprise wide
C – Event Identification					
C1 - Data on the business operating environment – political, economic, etc., events is captured and regularly evaluated in terms of their potential impact upon the organisation's business objectives					
C2 - A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared					
C3 - Events are linked to and risk evaluated for each individual objective.					
C4 - Goals and objectives for identifying events and the related risks exist and are communicated to all segments of the organisation					
C5- Responsibilities and accountabilities for risk identification are clearly defined and understood.					
C6 - Risk is considered in terms of not just isolated events but also inter-related events					
C7 - Events are categorized into useful groups to facilitate the aggregation of information for purposes of assessing risks					
C8 - The organisation evaluates events in the context of the potential upsides (opportunities) as well as the downside (risks).					
D – Risk Assessment					
D1 - Prior to assessing risks, management examines the impact of potential future events relevant to its business (i.e. entity size, complexity of operation, degree of regulation, etc.)					
D2 - Risk is considered in terms of both inherent and residual risk					
D3- Key risks are considered within a standard framework, e.g. likelihood and consequences of risk occurring					
D4 - Risk assessment criteria, e.g. likelihood, are articulated and applied consistently					
D5 - Management gives consideration to both near term risk impacts as well as those that are further out in time which impact strategic direction					
D6 - Appropriate methodologies are in place to allow the organisation to measure the impact of identified risks on objectives with some degree of accuracy					
D7 - The costs (including resources allocated) and benefits of risk mitigation are taken into account in the evaluation of risk acceptability					
D8 - There is a periodic review process to ensure that the organisation's risk assessments remain current					
D9 - Scenario analysis techniques are used to assess the potential impact of events combining					
E – Risk Response					
E1 - The full range of available risk management options – avoid, reduce, share, accept – is considered when formulating risk responses					
E2 - When considering alternative responses, management considers the impact on risk significance and likelihood					
E3 - Alternative responses are evaluated in terms of the resulting costs and benefits					
E4 - There are clear guidelines as to how decisions following on from risk assessment are to be made and at what level					
E5 - The organisation measures risk management outcomes or results					
F – Control Activities					
F1 - There is an appropriate balance of preventative and detective controls in place, with emphasis on preventative controls when appropriate					
F2- Controls are considered in terms of efficiency as well as effectiveness					
F3 - Control activities include effective controls over information technology management, information technology infrastructure, security management, software development and maintenance					

Assessment Questions (Mark one box per question with an 'x')	Don't Know	Disagree, or No Plans	Planned	Partly In Place	Implemented enterprise wide
F4 - Controls are effective in ensuring the completeness, accuracy and validity of data processed					
F5 - Management considers the impact of significant organisational, structural or managerial changes on risk, risk responses and the related control activities before implementing them					
G – Information/Communication					
G1 - Appropriate information is identified and captured to identify, assess and respond to risk and manage the business, obtained from appropriate internal and external sources, generated manually and electronically and is in appropriate formal and informal formats.					
G2 - Information is provided for decision making at the appropriate depth and with the appropriate timeliness					
G3 - Information quality is evaluated in terms of e.g., level of detail of the content – Timeliness, Currency, Reliability, Accessibility, and Level of Detail					
G4 - There are clear upward lines of communication to report risk incidents					
G5 - Communications in the organisation, both formal and informal, are effective in raising the risk awareness					
H – Monitoring					
H1 - The required information is available to allow for proper monitoring of risk throughout the company					
H2 - Appropriate real time ongoing monitoring processes are in place to measure performance and provide early warning or detect and report deviations from established norms immediately to the appropriate managers					
H3 - A monitoring process is built into the execution of the business process					
H4 - Day-to-day monitoring takes place daily through ongoing supervision and oversight					
H5 - Process and risk owners periodically self assess their performance and report the results of their self-assessment upward to appropriate managers					

Scoring Key

The Enterprise Risk Management (ERM) framework enables the maturity of enterprise wide risk management implementations to be gauged and for actions to be taken in order to make improvements as appropriate.

Scoring instructions: Take note of where the boxes have been crossed, particularly in the first two columns where no action has been taken, or further information is required. Brainstorm what actions are required to improve performance.