Insurance Commission of Western Australia

RiskCover

Risk Management Guidelines

Glossary of Terms

Business continuity management: A process that allows an organisation to recover from an event that significantly disrupts its activities. Business continuity management focuses on three post-event phases; disaster recover, business continuity (of essential functions) and full recovery.

Business continuity plan: The principle output of the business continuity management process. A business continuity plan is, in effect, a treatment plan for certain risks the consequences of which could disrupt core functions.

Cause (or trigger): The factors, either root or contributory, that may give rise to a risk event. A risk can have multiple causes.

Consequence: The impact or outcome of a risk eventuating. A risk can have multiple consequences.

Consequence categories: These are key impact areas, which if affected as a result of a particular risk event, could have a significant impact on the ability of an agency to deliver its outcomes. Consequence categories are agency specific, and should reflect the agency's economic, social and environmental responsibilities.

Control: A procedure, system, activity or process that reduces the likelihood and/or consequences of a risk. A risk may have more than one control, and a control may address more than one risk.

Controls rating: A qualitative, common-sense measure of the adequacy of controls in addressing a risk.

Controls assurance: The process whereby control ratings are verified through a series of questions regarding their relevance and effectiveness.

Critical success factors: A factor which is essential for the successful performance of a key activity.

Impact range: A measurement of how widespread the consequences of a risk may be. This measurement can assist in the assessment of controls and the formulation of treatments.

Implementation plan: A plan created to establish how the risk management process is to be implemented into an organisation.

Key activity: Any high level activity or function that is instrumental in an agency delivering required outcomes or performing its mission.

Key dependency: Relationship with or reliance upon another party essential to delivering outcomes or services. Key dependencies can be within the agency or external.

Likelihood: A measure of how likely it is that a certain consequence will eventuate, ranging from very unlikely to almost certain.

Monitoring: An ongoing process of surveillance of the internal and external environments to ensure that risks continue to be effectively and appropriately managed.

Operational (context): Deals with operational risks: those risks associated with normal, ongoing operations and activities.

Performance indicators: Clear, simple measures of performance over time used in the monitor and review process. Performance indicators can measure either processes or outcomes.

Project (context): Deals with project risks: those risks associated with defined projects and other discrete undertakings.

Review: Periodic assessment of a specific aspect of the risk management process or a particular group of risks to determine if there have been gradual changes over time.

Risk: Defined as "effect of uncertainty on objectives" by AS/NZS ISO 31000:2009 and an effect is a positive or negative deviation from what is expected.

Risk acceptance criteria: Agency specific standards that delineate under what conditions risks of a certain level can be accepted. The higher the risk rating, the higher the standard of controls, monitoring, and ownership required.

Risk assessment: Assignment values (risk ratings) to individual risks and deciding how to manage them.

Risk analysis: A process that assigns a risk rating to each risk by evaluating the effectiveness of existing controls and assigning values for likelihood and consequences for various scenarios.

Risk evaluation: A decision making process which evaluates the risk rating against the risk assessment criteria.

Risk categories: Categorisation of risks within the agency by type, often based on source of risk. This helps identify common risks in different functional areas.

Risk decision: The decision made after risk evaluation, balancing risk and reward.

Risk management: The practice of systematically identifying, understanding, and managing the risks encountered by an organisation.

Risk management process: The process of implementing, maintaining and embedding risk management in an organisation, as set out in these guidelines. The process consists of four sequential steps plus the overarching processes of communication and consultation and monitor and review.

Risk owner: The person specifically assigned to manage the risk, including monitoring the risk, its controls and any treatments that are implemented.

Risk rating: The value assigned to the risk which represents the product of consequences and likelihood.

Risk reference tables: Collective term for the various risk measurement and evaluation tools.

Risk tolerance (or risk appetite): The degree that an organisation is willing to accept risk in order to achieve its objectives. Risk tolerance is a product of mission, culture, policy and other factors that determine what an agency is and how it goes about its business.

Strategic (context): Risks which concern the whole agency and are associated with long term organisational objectives. Strategic risk management is most effective when conducted as an integral part of the strategic planning process.

Treatment: A measure that is designed and implemented to further reduce the consequences and/or likelihood of a risk. Once a treatment is fully implemented and effective, it becomes a control.

Treatment action plan: The plan formulated for selected treatments to ensure they are fully and properly implemented. Treatment action plans should identify owners, participants, resources, schedule, and performance indicators.