**RISK ASSESSMENT**

**Risk Overview**

Risk: A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.

Regardless of the types of risk being considered, all risk assessments generally include the following elements. Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.

Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals. Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important

Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs. Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls. Documenting the results and developing an action plan.

A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on

(1) the likelihood that a damaging event will occur,

(2) the costs of potential losses, and

(3) the costs of mitigating actions that could be taken

**Risk Identification**

Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern. The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on the project's ability to achieve performance or capability outcome goals. They may come from within the project or from external sources.

There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty. Risk identification needs to match the type of assessment required to support risk informed decision making. For an acquisition program, the first step is to identify the program goals and objectives, thus fostering a common understanding across the team of what is needed for program success. This gives context and bounds the scope by which risks are identified and assessed.

There are multiple sources of risk. For risk identification, the project team should review the program scope, cost estimates, schedule (to include evaluation of the critical path), technical maturity, key

performance parameters, performance challenges, stakeholder expectations vs. current plan, external and internal dependencies, implementation challenges, integration, interoperability, supportability, supply-chain vulnerabilities, ability to handle threats, cost deviations, test event expectations, safety, security, and more. In addition, historical data from similar projects, stakeholder interviews, and risk lists provide valuable insight into areas for consideration of risk.

Risk identification is an iterative process. As the program progresses, more information will be gained about the program (e.g., specific design), and the risk statement will be adjusted to reflect the current understanding. New risks will be identified as the project progresses through the life cycle.

**Risk Analysis**

**Risk analysis steps:**

 Identify the scope of the analysis.

 Gather data.

 Identify and document potential threats and vulnerabilities.

 Assess current security measures.

 Determine the likelihood of threat occurrence.

 Determine the potential impact of threat occurrence.

 Determine the level of risk.

 Identify security measures and finalize documentation

**A risk analysis has four main goals:**

 Identify assets and their values

 Identify vulnerabilities and threats

 Quantify the probability and business impact of these potential threats

 Provide an economic balance between the impact of the threat and the cost of the Countermeasure

**Risk Evaluation**

The risk evaluation process receives as input the output of risk analysis process. It compares each risk level against the risk acceptance criteria and prioritise the risk list with risk treatment indications.

**Risk Treatment**

Risk treatment efforts should be undertaken to mitigate identified risks, using appropriate administrative, technical and physical controls. Control includes:

 applying appropriate controls to avoid, eliminate or reduce risks;

 transferring some risks to third parties as appropriate (e.g., by insurance);

 knowingly and objectively accepting some risks; and

 documenting the risk treatment choices made, and the reasons for them.

Risk treatments should take account of:

 legal-regulatory and private certificatory requirements;

 organizational objectives, operational requirements and constraints; and

 costs of implementation and operation relative to risks being reduced.

**Risk treatment strategies include:**

**Risk reduction**

Taking the mitigation steps necessary to reduce the overall risk to an asset. Often this will include selecting countermeasures that will either reduce the likelihood of occurrence or reduce the severity of loss, or achieve both objectives at the same time. Countermeasures can include technical or operational controls or changes to the physical environment

**Risk sharing/transference**

The organization shares its risk with third parties through insurance and/or service providers. Insurance is a post-event compensatory mechanism used to reduce the burden of loss if the event were to occur. Transference is the shifting of risk from one party to another

**Risk avoidance**

The practice of eliminating the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized. For example, an organization decides to discontinue a business process in order to avoid a situation that exposes the organization to risk.

**Risk acceptance**

An organization decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs. Risk acceptance is a viable strategy where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are accepted by default

**Risk Management Feedback Loops**

**Risk management is a comprehensive process that requires organizations to:**

 frame risk (i.e., establish the context for risk-based decisions);

 assess risk;

 respond to risk once determined; and

 monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

**The first component of risk management addresses establishing a realistic and credible risk frame required by an organization:**

 risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time);

 risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration);

 risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and

 priorities and trade-offs (e.g., the relative importance of missions/business functions, tradeoffs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses).

**The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify:**

 threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;

 vulnerabilities internal and external to organizations;

 the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and

 the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).

To support the risk assessment component, organizations identify:

 the tools, techniques, and methodologies that are used to assess risk;

 the assumptions related to risk assessments;

 the constraints that may affect risk assessments;

 roles and responsibilities;

 how risk assessment information is collected, processed, and communicated throughout organizations;

 how risk assessments are conducted within organizations;

 the frequency of risk assessments; and

 how threat information is obtained (i.e., sources and methods).

**The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments.**

The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by:

 developing alternative courses of action for responding to risk;

 evaluating the alternative courses of action;

 determining appropriate courses of action consistent with organizational risk tolerance; and

**The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to:**

verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational mission/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied;

 determine the ongoing effectiveness of risk response measures following implementation;

 identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

**Risk Monitoring**

**Risk monitoring provides organizations with the means to:**

 verify compliance;

 determine the ongoing effectiveness of risk response measures; and

 identify risk-impacting changes to organizational information systems and environments of operation.

Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation. Organizations can implement risk monitoring at any of the risk management tiers with different objectives and utility of information produced.

For example, Tier 1 monitoring activities might include ongoing threat assessments and how changes in the threat space may affect Tier 2 and Tier 3 activities, including enterprise architectures (with embedded information security architectures) and organizational information systems.

Tier 2 monitoring activities might include, for example, analyses of new or current technologies either in use or considered for future use by organizations to identify exploitable weaknesses and/or deficiencies in those technologies that may affect mission/business success.

Tier 3 monitoring activities focus on information systems and might include, for example, automated monitoring of standard configuration settings for information technology products, vulnerability scanning, and ongoing assessments of security controls.

In addition to deciding on appropriate monitoring activities across the risk management tiers, organizations also decide how monitoring is to be conducted (e.g., automated or manual approaches) and the frequency of monitoring activities based on, for example, the frequency with which deployed security controls change, critical items on plans of action and milestones, and risk tolerance.