Risk Assessment is the identification, analysis, and management of risks or threats that could negatively affect the agency and prevent it from achieving its goals and objectives.

Risk Assessment Procedure*

1. Create an agency-specific risk assessment plan.
2. Identify individuals responsible and accountable for ensuring that the risk assessment plan is carried out, documented, accessible, regularly reviewed and updated.
3. Perform and document risk assessments as outlined in the risk assessment plan.
4. Ensure that control weaknesses and gaps identified through the risk assessment process are pursued and mitigation status is communicated to management.
5. Certify to the status of the risk assessment plan and progress toward implementation through the annual agency head internal control structure certification process, pursuant to M.S. 16A.057, Subd. 8.
6. Monitor progress on implementing and completing the risk assessment plan.
7. Revisit the plan to identify any new or existing processes to be added to the plan. Revise the plan annually.

Risk Assessment Phases

1. Coordinate the project
2. Document the business process
3. Identify risks
4. Prioritize risks
5. Identify and evaluate control activities
6. Create action plans to address control gaps and redundancies
7. Communicate results to management

Source: MMB Statewide Procedure 0102-01.2, Risk Assessment

Control Activities are the actions taken to reduce risk or to minimize obstacles to accomplishing goals.

Control Activity Categories

- **Documentation** preserves evidence to substantiate a decision, event, transaction, or system. All documentation should be complete, accurate, and recorded timely.
- **Authorization** is the power granted to an employee to perform a task (e.g. delegation of duties).
- **Approval** is the confirmation or sanction of employee decisions, events or transactions, based on an independent review.
- **Verification/Reconciliation** involves the comparison of an internally prepared document (e.g. purchase order) to an independent source (e.g. vendor invoice) to determine the completeness, accuracy, authenticity, and/or validity of transactions, events, or information.
- **Separation of Duties** is the division or segregation of key duties and responsibilities among different people to reduce the opportunities for any individual to be in a position to commit and conceal errors (intentional or unintentional), or perpetrate fraud in the normal course of their duties.
- **Access Security** involves securing access to resources and information to reduce the risk of unauthorized use or loss. Access controls are set based on the employee's need to access data files and information necessary to perform his or her specific job duties while maintaining acceptable separation of duties.
- **Supervision** is the ongoing oversight, management, and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives.
- **Reporting** is a means of conveying information. Effective and accurate reporting control activities provide information on issues such as timely achievement of goals, accurate financial position, and payroll irregularities.

Control Activity Design

A control activity must have all of the following characteristics to be valid:

1. It addresses the risk in question
2. It is mandatory (not optional)
3. It is currently in operation or has occurred in the last 12 months

Key controls address significant and/or multiple high-level risks. Consideration should be given to include these key control activities in policies and procedures and in the position descriptions of those responsible for carrying them out.

Control Activity Classifications

Control activities can be classified as **preventive** or **detective; hard** or **soft**; **manual** or **automated**; or **IT-dependent**.

- **Preventive controls** are designed to avoid errors or improprieties before a transaction is processed (documentation, authorization, approvals, segregation of duties, access security, supervision, etc.)
- **Detective controls** are designed to identify errors or irregularities that have already occurred and enable management to take prompt corrective action (verification, reconciliation, reporting, etc.)
- **Soft controls** provide notice of a requirement but do not by themselves immediately terminate a transaction for failing to meet that requirement (statutes, policies, rules, etc.)
- **Hard controls** terminate a transaction for failing to meet a requirement (passwords, authorization codes, approvals, etc.)
- **Manual controls** are performed by individuals (authorizations, approvals, reconciliations, etc.)
- **Automated controls** are incorporated into application systems (access security, system activity and exception reports, etc.)
- **IT-dependent controls** are manually performed by required input based on computer-produced information (access security, etc.)

Definitions

- **Risk** is the possibility of an event occurring that will have a negative impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
- **Inherent Risk** is the probability of a loss arising out of a negative event or existing in the current environment before mitigating steps (i.e. control activities) are taken to reduce the possibility of occurrence.
- **Residual Risk** is the risk remaining after management takes action to prevent or reduce the impact and/or likelihood of a negative event occurring.

Risk Response and Mitigation Strategies

- **Control/Reduce/Mitigate** – Risk can be reduced by putting control activities into place to ensure that all significant risks have been addressed.
- **Transfer** – Risk can be transferred by having someone else assume it. However, the entity transferring the risk often remains ultimately responsible for the final outcome.
- **Avoid** – Risk can be avoided by choosing not to engage in the activity. However, in government it is impossible to avoid activities mandated by the legislature.
- **Accept** – Significant risks can be reduced, mitigated, or transferred. Low or residual risks can be accepted. This occurs when the agency chooses to deal with the consequences of the risk if it occurs.

Some Questions to Ask When Attempting to Identify Risks:

1. What can go wrong?
2. How could we fail?
3. What must go right for us to succeed?
4. Where are we vulnerable?
5. What activities are most complex?
6. What is our greatest legal exposure?

MS 16A.057 INTERNAL CONTROLS AND INTERNAL AUDITING

Subd. 8. **Agency head responsibilities.**
The head of each executive agency is responsible for designing, implementing, and maintaining an effective internal control system within the agency. The head of each executive agency must annually certify that the agency head has reviewed the agency's internal control systems, and that these systems are in compliance with standards and policies established by the commissioner. The agency head must submit the signed certification form to the commissioner of management and budget, in a form specified by the commissioner.

MMB Statewide Procedure 0102-01.2 Risk Assessment

Risk assessment is one component of the COSO Internal Control Integrated Framework and is vital to an effective internal control system. Risk assessments must be performed on all high profile key processes in order to support the agency head's annual certification of internal control structure, pursuant to MS 16A.057, Subd.8. The agency's risk assessment plan identifies the specific processes for which risk assessments must be performed and documented. The plan must be comprehensive and sufficient enough in scope to support the agency's certification of internal control structure. This procedure is applicable to all cabinet level agencies and other executive branch agencies, based on size and inherent business risk.

For more information about risk assessment and control activities go to:

https://www.mn.gov/mmb/internalcontrol/

MINNESOTA Management & Budget

Risk Assessment: A Quick Reference Guide

A Key to an Effective Internal Control System

A publication of Minnesota Management & Budget
Internal Control and Accountability
Unit http://mn.gov/mmb/internalcontrol/