# TABLE OF CONTENTS

GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES ................................. 1
RISK ASSESSMENT AND CONTROL ACTIVITIES — INTRODUCTION .................. 3
EXPLAINING THE JARGON ........................................................................... 4
PLANNING FOR A RISK ASSESSMENT ................................................................ 7
PREPARING A RISK ASSESSMENT .................................................................. 9
1. DETERMINING WHAT NEEDS TO BE DONE (OBJECTIVES/GOALS) ................. 9
   Documenting the To-Do List ........................................................................ 10
   Grant Program Compliance .......................................................................... 10
   Financial Reporting ..................................................................................... 13
2. IDENTIFYING WHAT CAN GO WRONG (RISKS) ........................................... 15
3. PRIORITIZING WHAT CAN GO WRONG (RISK RANKING) ............................. 16
   Risk Ranking .............................................................................................. 16
   Risk Reactions ........................................................................................... 16
   Risk Acceptance ......................................................................................... 18
CONTROL ACTIVITIES – FORMULATING ACTIONS THAT WILL REDUCE THE CHANCE OF THINGS GOING WRONG .......................................................... 19
   Designing Control Activities ....................................................................... 20
   Control Activity Categories ......................................................................... 21
   Control Gaps and Redundancies .................................................................. 23
   Prioritizing Control Activities ..................................................................... 24
   Evaluating Key Controls ............................................................................. 24
UPDATING THE RISK ASSESSMENT AND IDENTIFIED CONTROL ACTIVITIES .... 27
BIBLIOGRAPHY ............................................................................................... 28
RISK ASSESSMENT AND CONTROL ACTIVITIES — INTRODUCTION

To many people, risk assessments (the second component of the COSO Framework) are a mystery. This is not because they do not understand risk—everyone thinks about and assesses risk every day—but rather because these everyday risk assessments are rarely written down or formalized.

There are many reasons why organizations perform risk assessments. They provide assurance that key business processes have appropriate control activities in place and provide a roadmap to guide management in developing standard policies and procedures. They help management identify control gaps and redundancies so that action plans can be formulated to plug control gaps, strengthen existing controls, or remove redundancies where applicable. Risk assessments also provide management with detailed documentation of the control activities in place, including process narratives, flowcharts, and risk grids. This information is useful for staff training and in cases of employee turnover.

For Minnesota state agencies, another reason to perform risk assessments is Minn. Stat. Section 16A.57 Sub. 8, which makes the head of each executive branch agency responsible for designing, implementing, and maintaining an effective internal control system within the agency. Because they are keys to an effective internal control system, completing risk assessments help agencies comply with Minn. Stat. Section 16A.57.

The COSO Framework defines risk assessment as “…the identification and analysis of relevant risks to achievement of the [entity’s] objectives, forming a basis for the determination of how the risks should be managed.” This means:

1. Determining what needs to be done (Objectives/Goals),
2. Identifying what can go wrong (Risks),
3. Prioritizing what can go wrong (Risk Ranking).

Once a risk assessment has been completed, actions that will reduce the chance of things going wrong must be formulated. These actions are called control activities (the third component of the COSO Framework). The COSO Framework defines control activities as “…the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risk to achievement of the entity’s objectives.”

The information in this guide is provided to help state agencies prepare risk assessments and implement effective control activities.

A word of caution: questionnaires and checklists

Many internal control questionnaires and checklists are available on the internet. These internal control questionnaires and checklists list common risks and control activities for various processes. However, because these questionnaires and checklists were prepared by people who lack knowledge of your specific organization’s operations, standard checklists are unlikely to be sufficient for documenting your organization’s risk assessment process. Nevertheless, these questionnaires and checklists may be useful in validating the completeness of a risk assessment once it has been prepared and provide users with common control activities.
EXPLAINING THE JARGON

Words can easily form a barrier to understanding. To avoid this, below are translations of technical terms often used when discussing risk assessments and control activities.

Compliance—The COSO Framework defines compliance as “…conforming with laws and regulations applicable to an entity.” This includes federal and state statutes, regulations, rules, policies and procedures.

Control Activities—The third component in the COSO Framework, referring to actions taken to reduce risk or to minimize obstacles to accomplishing goals. Examples of control activities include authorization and approval, reconciliations, and separation of duties.

Control Environment—The first component in the COSO Framework, and refers to the foundation of an effective internal control system which begins with the “tone at the top”—the words and actions of the agency’s leadership. Under an effective control environment, employees view internal control as essential and integral to performing their day-to-day job duties. See the Control Environment section on Minnesota Management & Budget’s Internal Control Unit website for a more detailed explanation.

Control Gap—When insufficient or no actions are taken to avoid or mitigate a significant risk.

Control Redundancy—When multiple control activities address the same risk. Redundancies often occur by design to provide additional assurance in high risk circumstances.

COSO Framework—In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a report titled Internal Control—Integrated Framework. This report is often referred to as the “COSO Framework.” The COSO Framework consists of five interrelated internal control components, including control environment, risk assessment, control activities, monitoring, and information/communication. The State of Minnesota has adopted the COSO Framework as its internal control standard.

Detective Control—A control designed to identify errors or irregularities that have already occurred and enable management to take prompt corrective action.

Financial Reporting—A financial report is any report containing financial data used to make informed decisions. Examples of financial reports include budget documents, comprehensive annual financial reports, and agency budget reports. In state government, responsibilities for financial reporting are often split between state agencies, which record day-to-day transactions and prepare reports for agency management, and a central service agency that compiles financial reports for external publication.

Function—An activity required to complete a process. Typically, a function is an activity performed by an individual employee, such as the review and approval of timesheets prior to payment of wages. A collection of related functions results in a process. A collection of related processes result in the delivery of a service by the agency.
GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES

Information and Communication—The fifth component of the COSO Framework. Information includes facts (i.e., data) and opinions. Communication refers to the flow of information from one person or organization to another. Information and communication are critical to the effective operation of an internal control system, flowing to, from, and through each of the other four components.

Inherent Risk—The risk associated with actions, activities or undertakings because of their nature, before steps have been taken to mitigate the riskiness. For example, having a lion as a pet is considered dangerous because the size and strength of the animal increases the chance that something will go wrong. The risk of having a lion as a pet remains inherently high even after steps have been taken to control the animal. On the other hand, having a domestic cat as a pet is not considered inherently risky and few actions need to be taken to control any danger posed by the cat. The same applies to business activities. For example, some assets, such as cash, have a higher inherent risk of theft than other assets, such as an office building.

Key Control Activities—Key control activities address one or more significant risks to the organization or underlying business process. The Institute of Internal Auditors defines key control activities as “[those] that, if [they] fail, man there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. [K]ey control [activities are] required to provide reasonable assurance that material errors will be prevented or timely detected.”

Monitoring—The fourth component in the COSO Framework, which relates to actions taken to ensure that control activities are operating as intended. An example of monitoring activities is a periodic review by senior management of reconciliation files to ensure that reconciliations are in fact being prepared. In a grant program, monitoring activities include site visits and desk reviews both of which aim to ensure that grant funds are being properly spent.

Objectives/Goals—What needs to be done in any business process, including how it needs to be done (often referred to as the “to-do” list). A precondition to risk assessment is the establishment of clear, consistent agency objectives. To help identify control points, the to-do list should be expanded into a process narrative or flowchart.

Operations—Defined by the COSO Framework as “[dealing] with the effectiveness and efficiency of an entity’s operations, including performance and profitability goals…”

Preventive Control—A control designed to avoid errors or improprieties before a transaction is processed.

Process—A collection of business activities undertaken to complete a service. Typically, a process is a collection of functions performed by individual employees. For example, the payroll time entry process consists of activities including aggregation of employee time data, calculation of wages, calculation, collection, and remittance of taxes and other deductions, and payment of wages. A process can span more than one agency. For example, agencies collect employee time data in timesheets and pass the information to a central agency for payroll processing.
Reasonable Assurance—Management should design and implement internal controls based on the related costs and benefits. No matter how well designed and operated internal control cannot provide absolute assurance that all agency objectives will be met.

Risk—Any obstacle to getting things done or a negative event that prevents attainment of a goal.

Risk Acceptance—Where management determines that the control measures in place are, given the resources available, sufficient to address the identified risks.

Risk Assessment—Figuring out what needs to be done, how to decrease the chance of failure and increase the chance of successfully achieving desired goals.

Risk Ranking—Prioritizing obstacles that have the potential to prevent achievement of goals. Efforts should be focused on the most critical risks which, if they went wrong, could potentially disrupt or derail the entire process.

Safeguarding Assets—Having to do with safety, maintenance, retention of physical and intangible assets.

Services—A service is the output by which an agency or organization fulfills its objectives or goals. Most agencies are responsible for a collection of services. The delivery of each service is made possible by several processes, and each process is a collection of employee-level functions.
PLANNING FOR A RISK ASSESSMENT

A successful risk assessment project requires initial planning. First senior management must be involved. Second, the order in which risk assessments will be performed must be determined. Finally, participating staff must be chosen and adequately trained.

Senior management must be involved in preparing the risk assessment for three critical reasons: (a) the risk assessment process cannot succeed unless it is championed by senior management, (b) senior management’s broad overview of the organization places it in the best position to determine how a risk assessment should be completed, and finally (c) only senior management can allocate the time and resources necessary to ensure the success of the risk assessment process. Employees take their cues from senior management, and if risk assessments appear unimportant to their leaders, risk assessments will not be important to employees. Senior management must convey the message that every employee is responsible for internal controls.

Senior management will need to prioritize the order in which the risk assessments should be completed, taking into account materiality and the potential for error or fraud. While it is possible to perform a risk assessment on every agency activity, a targeted approach is much more efficient. Senior management must make priority decisions and also must determine which activities share similar processes and can be grouped together into a single, higher level risk assessment to save time and gain efficiency.

There are many ways to deploy risk assessments in an agency. For example, if processes are similar, it may be possible for an agency whose primary service is to issue grants to perform only two grant risk assessments—one for its grant making process and another for the support processes (e.g., financial reporting, payroll, administrative disbursements, and receipts). This process-based approach is likely to be more efficient because it groups related processes together and allows one risk assessment to cover several similar processes. It rarely makes sense to complete a risk assessment on an individual grant program.

Yet even within service areas, processes may be different enough to require separate risk assessments. While similar risks may be identified among the processes, the control activities used to manage the risks may be substantially different. For instance, both formula (flow-through) and competitive grants have eligibility risk. In both cases there is a chance that a grant will be made to an ineligible person or entity. However, the eligibility risk for competitive grants can be higher than that for formula grants for several reasons, such as a larger applicant pool, or more subjective selection criteria. The different levels of risk for each grant type call for differing actions. For a flow-through grant, these actions may be limited to confirming grantees to a predetermined list. For competitive grants, the actions may include implementing a rigorous Request for Proposal (RFP) process.

The types of assets within each agency may also be a factor. Each agency is responsible for tangible and intangible state assets (including money, computer software, etc.) used to achieve its objectives. For some agencies, these assets may be limited to furniture and computers while others may be responsible for high cost tangible assets like real estate. Preparing a list of the different types of assets may be helpful in deciding where to begin the risk assessment process, e.g., beginning with the most vulnerable assets (such as cash), and concluding with the least vulnerable assets (such as buildings).

There are two final considerations when planning for a risk assessment: training and timing. Once the risk areas have been prioritized, staff must be trained to enable them to effectively participate in the risk
assessment process. Staff training may occur through seminars or through the completion of pilot risk assessments on a small discrete process, providing staff with valuable hands-on experience. Management must also provide staff with sufficient time to complete a thorough risk assessment, and compile the supporting documentation.
GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES

PREPARING A RISK ASSESSMENT

1. DETERMINING WHAT NEEDS TO BE DONE (OBJECTIVES/GOALS)

A precondition to risk assessment is the establishment of clear, consistent agency and program objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving those objectives.

In the government sector, a legislative body usually decides “what” (i.e., service objective or goal) needs to be done by enacting statutes and budgets that reflect major goals and objectives. Broad goals are also found in each process within an agency because each process is dedicated to delivering a service. The executive branch determines “how” (i.e., the specific process steps to achieving that goal) the legislative goals will be implemented by establishing the processes that result in the delivery of the service.

Knowing what needs to be achieved and how it will be achieved allows for the creation of a “to-do” list. To avoid an unwieldy list, the list should be limited to the high-level, key steps needed to successfully accomplish the stated goals. To help ensure that the to-do list is both focused and complete, it may be helpful to consider the following questions:

- What triggers or initiates an activity? For example, what starts the process of making a grant or preparing the payroll?
- What reviews, approval, or monitoring does the activity undergo? For example, who reviews and approves grant applications? Who approves new employees before they are placed on the payroll?
- How are transactions recorded? For example, are grant applications recorded in a grants database? How are new employees recorded in SEMA4 or a similar payroll system?
- After initiating and approving the activity, what steps will it go through as it is processed? For example, once the grant application has been received, reviewed and approved, what happens from the moment of approval to the time a check is sent to the grant recipient? What happens from the time a new employee is entered in SEMA4 until the time the employee’s pay is deposited in his or her bank account?
- What are the reporting requirements for the activity or what must be communicated to whom and in what format? For example, does the agency have any financial or program effectiveness reporting obligations? Are time sheet reports for employees required?

Transforming a high-level to-do list into comprehensive process documentation (e.g., a flow chart or process narrative) can be a daunting task. Fortunately, there are several resources to help with this process such as the Office of Management and Budget Circular A-133, Audits of States, Local Governments and Non-Profit Organizations, Compliance Supplement, Part 6 – Internal Controls (hereafter referred to as OMB Circular A-133 Compliance Supplement, Part 6 or Part 6 of the Compliance Supplement) and the Office of Management and Budget Circular A-123, Management’s Responsibility for Internal Control, Appendix A —Implementation Guide (hereafter referred to as OMB Circular A-123 Appendix A Implementation Guide). It may be helpful to group these resources along the three categories highlighted in the COSO Framework model, i.e., financial reporting, compliance, and operations. For government entities, a fourth category—safeguarding assets—should also be considered. Most entities begin their risk assessment process by focusing on the financial reporting and compliance areas.
GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES

Documenting the To-Do List

Documenting the processes by which the agency achieves its goals is essential to demonstrating that senior management has identified and addressed major risks. There are many ways to document the processes within an agency, including to-do lists, process narratives, and flow charts. The documentation style will depend on the size of the agency, resources available, and the complexity of the agency’s processes.

A to-do list is a high-level outline of a process narrative or flow chart, and is therefore insufficient on its own to demonstrate an understanding of the activity under review. Expanding the to-do list makes it easier to identify control points—those actions management is taking to achieve its objectives. For instance, if one of the items on the to-do list is to determine who is eligible for program funds, it will be easier to identify steps management is taking to ensure effective screening if these steps are presented in a narrative or flow-diagram form.

The process narrative or flow chart documentation should be detailed enough to identify control points but not so detailed as to overwhelm a reader. To make efficient use of resources, process narratives and flow charts should focus on key actions, rather than on every action that management takes to control risk.

Finally, the risk assessment should be documented in a form that allows for easy periodic review and updating.

Grant Program Compliance

A to-do list for grant programs will depend on what is significant for these programs. The federal Office of Management and Budget (OMB) has identified 13 risk areas common to most federal grant programs. A discussion of these risk areas can be found in OMB Circular A-133 Compliance Supplement, Part 6. Although this guidance is aimed at federal grants and programs, it can be applied to any grant program.

While Part 6 of the Compliance Supplement has a helpful list of objectives and risks that should be considered for all grants, this list is very generic. Relying solely on Part 6 of the Compliance Supplement can result in an incomplete list of objectives and risks. On the other hand, not every area addressed by Part 6 of the Compliance Supplement is applicable to every grant program. A comprehensive list of objectives and risks for a grant is best developed independently, with Part 6 forming a backstop to the risk identification process.

The risk areas addressed by Part 6 of the Compliance Supplement include the following objectives which can be thought of as the “what” needs to be done. To prepare a to-do list (and later the process narrative or flowchart), list or describe “how” each applicable objective will be achieved, e.g., how does the agency ensure funds are spent only on allowable activities?

A. Activities Allowed or Unallowed—Ensuring that awards are expended only for allowable activities,
B. Allowable Costs/Cost Principles—Ensuring the costs of goods and services charged to awards are allowable and in accordance with the applicable cost principles,
C. Cash Management—Ensuring that the (1) drawdown of federal cash is only for immediate needs, (2) reimbursement is requested only after costs have been incurred, (3) states comply with applicable treasury agreements, and (4) recipients limit payments to sub-recipients to immediate cash needs,

D. Davis-Bacon Act—Ensuring that contractors and subcontractors were properly notified of the Davis-Bacon Act requirements and the required certified payrolls were submitted to the non-Federal entity,

E. Eligibility—Ensuring that only eligible individuals and organizations receive assistance under award programs, that sub-awards are made only to eligible sub-recipients, and that amounts provided to or on behalf of eligible individuals or groups of individuals were calculated in accordance with program requirements,

F. Equipment and Real Property Management—Ensuring that proper records are maintained for equipment acquired with awards, equipment is adequately safeguarded and maintained, disposition or encumbrance of any equipment or real property is in accordance with award requirements, and the awarding agency is appropriately compensated for its share of any property sold or converted to non-federal use,

G. Matching, Level of Effort, Earmarking—Ensuring that matching, level of effort, or earmarking requirements are met using only allowable funds or costs which are properly calculated and valued,

H. Period of Availability of Funds—Ensuring that funds are used only during the authorized period of availability,

I. Procurement and Suspension and Debarment—Ensuring that procurement of goods and services are made in compliance with the provisions of the A-102 Common Rule or OMB Circular A-110, as applicable, and that covered transactions (as defined in the suspension and debarment common rule) are not made with a debarred or suspended party,

J. Program Income—Ensuring that program income is correctly earned, recorded, and used in accordance with the program requirements,

K. Real Property Acquisition and Relocation Assistance—Ensuring compliance with the real property acquisition, appraisal, negotiation, and relocation requirements,

L. Reporting—Ensuring that reports of awards submitted to the awarding agency or pass-through entity include all activity of the reporting period, are supported by underlying accounting or performance records, and are fairly presented in accordance with program requirements, and

M. Sub-recipient Monitoring—Ensuring that award information and compliance requirements are identified to sub-recipients, sub-recipient activities are monitored, sub-recipient audit findings are resolved, and the impact of any sub-recipient noncompliance on the pass-through entity is evaluated. Also, the pass-through entity should perform procedures to provide reasonable assurance that the sub-recipient obtained required audits and takes appropriate corrective action on audit findings.

It may be helpful to review the suggested controls in the control activities section for each of the (A through M) areas above.

**State Programs**—The Minnesota Department of Administration’s Office of Grants Management has collected various statutes, policies, and procedures that are applicable to state grants. There is considerable overlap between the objectives and risks noted in OMB Circular A-133 Compliance Supplement, Part 6 and the state statutes, policies, and procedures listed by the Office of Grants Management. Both aim to improve the administration of grant programs by suggesting or requiring best practices in grant administration. The list of policies referenced by the Office of Grants Management includes:
1. Grants Conflict of Interest—Avoid both actual and perceived conflicts of interest related to grant-making at both the individual and organizational levels,

2. Rating Criteria for Competitive Grant Review—Ensuring fairness, precision and consistency in competitive grant awards, including having review criteria published in the request for proposal or notice of grant opportunity,

3. Publicizing Grant Notices and Requests for Proposals—Ensuring sufficient information is included in notices of grant opportunities and requests for proposal (RFPs) so that potential applicants may make informed decisions about applying for and managing state grants,

4. Use of Grant Agreements—Ensuring Minnesota state agencies have written grant agreements for all grants made by the agency, that conform to Minnesota Statute 16 B.98 subd. 5, "Creation and Validity of Grant Agreements."

5. Public Comments Concerning Fraud and Waste in State Grants—Ensuring the Office of Grants Management (OGM) serves as the central point of contact for questions and comments about fraud and waste in state grants and about the violation of statewide grants policies,

6. Financial Review of Non-governmental Organizations—Ensuring that grants are made to nongovernmental organizations that are financially stable enough to carry out the purpose of the grant, including (a) assessing a recent financial statement from any non-governmental organization awarded a grant of over $25,000, (b) discussing any significant concerns with the grant applicant and (c) ensuring such concerns are resolved to the satisfaction of state agency staff before a grant is awarded,

7. Single and Sole Source Grants—Ensuring that grants are competitively awarded as much as possible and that single and sole source grants are to be used when only one entity is reasonably able to meet a grant’s intended purpose and objectives, due to their geographic location, specialized knowledge, relationships or specialized equipment,

8. Grant Payments—Ensuring that grant agreements (a) specify the method and schedule of payments for each grant in the grant agreement, (b) grant payments are not issued until the funds are encumbered and the grant agreement is fully executed, and (c) reimbursement is the preferred method for making grant payments,

9. Grant Progress Reports—Ensuring (a) state agencies monitor progress on state grants by requiring grantees to submit written progress reports at least annually until all grant funds have been expended and all of the terms in the grant agreement have been met, and (b) grant payments are not made on grants with past due progress reports unless the state agency has given the grantee a written extension,

10. Grant Monitoring—Ensuring the state agency (a) conducts at least one monitoring visit per grant period on all state grants of over $50,000 and at least annual monitoring visits on grants of over $250,000, and (b) conducts a financial reconciliation of grantees' expenditures at least once during the grant period on grants of over $50,000,

11. Legislatively Mandated Grants—Ensuring agencies manage legislatively mandated grants with the same level of oversight (including monitoring activities) applied to other state grants, while respecting and maintaining the legislative intent,

12. Policy on Grant Amendments—Ensure any changes to grant agreements are made using fully executed grant agreement amendments,

13. Grant Closeout Evaluation—Ensuring that state agencies consider a grant applicant’s past performance before awarding subsequent grants of over $5,000 to them.

As with the suggested control objectives in OMB Circular A-133 Compliance Supplement, Part 6, when using the Department of Administration policies, the grant risk assessment should describe how the required objective is being achieved.
**Department Policies**—Many departments have policies that were formulated to facilitate important goals or prevent undesired activities from occurring. Departmental policies should be reviewed where applicable.

**Financial Reporting**

Financial reporting includes annual financial statements, budgets, and reports used to monitor specific activities. The audience for these reports includes the general public, legislative bodies, and agency management.

The federal Office of Management and Budget (OMB) published *OMB Circular A-123—Management’s Responsibility for Internal Control* (OMB Circular A-123) which defines management’s responsibility for internal control in federal agencies. Although aimed at federal agencies, OMB Circular A-123 provides guidance that is useful to all governmental entities.

Once the agency has identified the financial reports within the scope of the risk assessment, the OMB Circular A-123 Appendix A Implementation Guide suggests a series of steps including the following three that may be helpful in preparing a to-do list for each financial report:

1. Determine significant accounts or groups of accounts. This involves identifying accounts or groups of accounts that are material to the financial report in question.

2. Identify and evaluate the major classes of transactions. For each significant account or group of accounts, identify the major classes of transactions associated with the accounts. Typically, these classes of transactions will fall along service or process lines such as payroll and accounts receivable.

3. Understand the financial reporting process. This involves obtaining an understanding of the process steps that link the accounting system to the financial report. It is rare that information will go directly from an accounting system to the financial report. The information from the accounting system is usually subject to intervening calculations and summarizations carried out by agency staff or a central financial reporting group.

Once the relevant accounts have been identified and appropriately grouped together, and there is an understanding of how these accounts are translated into financial reports, the question of how to prepare process documentation for financial reporting can be tackled. It may be helpful to envision the financial reporting process as following these three steps: (a) collection of data on transactions and events, (b) accumulation of balances, and (c) presentation and disclosure of information.

The American Institute of Certified Public Accountants (AICPA) has identified management assertions (i.e., management goals or objectives) under each of these three steps that are aimed at ensuring financial reports are accurate. These management assertions can be found in the AICPA’s *Statement of Auditing Standards (SAS) 106 Audit Evidence* (AU §326 paras. .14 and .15). A to-do list and a comprehensive process narrative or flowchart can be created by asking how each of these assertions is being achieved. These assertions are as follows:

A. For transactions and events, how does management ensure that:
A transaction or event occurred (Occurrence)?
All transactions or events have been captured (Completeness)?
All transactions or events are accurately recorded (Accuracy)?
The transactions or events are recorded in the correct accounting period (Cut-off)?
The transactions and events are correctly classified (Classification)?

B. Once transactions or events have been recorded, they are then accumulated in account balances. For account balances, how does management ensure that:

- The account balances represent transactions or events that really occurred (Existence)?
- The account balances properly reflect amounts owed to the agency or amounts the agency owes to others (Rights and Obligations)?
- The account balances represent all transactions or events (Completeness)?
- The account balances reflect what the state can reasonably hope to receive or pay (Valuation and Allocation)?

C. Finally, the accumulated account balances must be translated into a report. This creates the need for proper presentation and disclosure. How does management ensure that:

- The transactions or events summarized in the report happened and correctly reflect what is owed to the organization or what amount it owes (Occurrence/Rights and Obligations)?
- All transactions or events are reflected in the report (Completeness)?
- The transactions or events are correctly classified and the classifications are understandable to the intended reader of the report (Classification/Understandability)?
- The transactions or events are accurately summarized in the report and correctly represent amounts owed to the agency or amounts the agency owes to others (Accuracy and Valuation)?

As discussed above, in state government the first two steps (the transaction/event and the accumulation of balances) typically occur at the agency level. The summarization, presentation, and disclosure are typically overseen by a central financial reporting entity.
2. IDENTIFYING WHAT CAN GO WRONG (RISKS)

Simply stated, a risk is anything that can go wrong and prevent the achievement of a desired objective. Once a to-do list, process narratives, and/or flow charts (see the Determining What Needs to be Done section) have been prepared, brainstorm about what could go wrong in each step of the process. Given time and a little imagination, countless risks can be identified. Make sure the list includes risks relating to compliance, financial reporting, operations, and safeguarding of assets. See the Explaining the Jargon section for descriptions of these categories.

For each item on the to-do list, ask these questions:

- What can go wrong?
- What problem are we trying to prevent?
- How can we identify or detect errors?
- Could fraud or abuse occur?
- Does this activity depend on inputs or support from outside the process and what happens if those outside functions fail?

It is also important to consider “intangible” risks. Examples of this type of risk include a tarnished reputation, loss of public confidence, and low employee morale. These types of risks typically arise from a failure of internal controls in one or more of the other risk categories: compliance, financial reporting, operations, and asset safeguarding.

It is important for the risk identification to be performed by a multi-dimensional team of employees familiar with the business process for which the risk assessment is being performed. For example, grant managers and administrators should be involved in the risk assessment for grants, as should the accountants who make payments to grantees. Similarly, the payroll risk assessment should be prepared by a team consisting of human resource, payroll, and accounting staff.

Some risks, such as those in the human resource and payroll processes, are shared because responsibility for the underlying activities crosses state agency lines. For example, while state agencies are typically responsible for their own staff recruitment; the central payroll services unit is responsible for ensuring employees receive proper wage and salary payment. Consequently, some risks, such as staff hiring and training, reside with the agency while other risks, such as accurate calculation of wages, and deduction of appropriate taxes and union dues, etc., reside with the central payroll unit. Other examples of shared operational risks can be found in information technology, vendor contract management, and financial reporting. When documenting the risk assessment, the point at which responsibility is passed from one agency or department to another should be clearly identified.
3. PRIORITIZING WHAT CAN GO WRONG (RISK RANKING)

Risk Ranking

It is impossible and unwise to attempt to address all that might go wrong. Actions taken to minimize risk (referred to as control activities) can be expensive and labor intensive. Efforts should be focused on the most critical risks which, if they went wrong, could potentially disrupt or derail the entire process.

The risk being assessed is the inherent risk—the chance of something going wrong BEFORE steps (i.e., control activities) are in place to reduce that chance of failure. For instance, when you think of physical security of assets (before any control measures are taken), cash is inherently more risky than a building. It is much easier to lose cash through theft (it is highly mobile and transferable) than it is to lose a building (very immobile and hard to transfer).

Risk ranking should take into consideration three elements: (a) occurrence (i.e., could it happen?), (b) probability (i.e., how likely it is to happen?), and (c) the materiality or magnitude of the event (i.e., what is the seriousness of the consequences if it happens?). Using the cash example above, the risk of loss from theft easily meets the first two criteria—the cash can be stolen, and if there are no control activities in place, the probability of theft is high. The materiality or magnitude requires more analysis. The risk grows with the size of the potential loss. In addition, small repeated losses could become material if unchecked. Hence the risk of loss of cash really depends on the circumstances, taking into account occurrence, probability, and magnitude of the potential loss.

There are many ways to rank risk. Whatever method is selected, it should include the following:

a. A ranking scale such as high, medium, low, or 1, 2, 3, etc. The ranking scale should be simple enough to allow the quick communication of the severity of the risk associated with an activity.

b. Written criteria that distinguishes the different levels of risk. For example, if the failure to meet a requirement would lead to a program being shut down, the risk of failure may be ranked high. On the other hand, if the consequence of a failure to comply is a minor inconvenience (e.g., a short time delay), then the risk of failure may be ranked low.

Risk Reactions

In theory, there are at least four potential reactions to the possibility of things going wrong: (a) transfer the risk, (b) avoid the risk, (c) reduce or mitigate the risk, or (d) accept the risk.

Risk can be transferred by having someone else assume it. However, the entity transferring the risk often remains ultimately responsible for the final outcome. A typical example is outsourcing a task. Although the task is being performed by some other entity, the transferring entity is still ultimately responsible for ensuring the outsourced task is completed.

Risk can be avoided by choosing not to engage in the activity. However, in government it may be impossible to avoid a mandate from the legislature.

In many cases, actions are taken to reduce or mitigate the risk. Because of the difficulty in anticipating every possible outcome or circumstance, it is usually difficult and very expensive to completely
 eliminate risk. A common reaction is to reduce the risk to a point where the remaining risk is acceptable to the decision maker, thus providing reasonable assurance of meeting the agency’s goals and objectives.

Commuting to work provides an everyday example of risk reactions. There is a risk of being involved in a car accident if you drive your car to work. The risk may be high because (1) car accidents happen, (2) they happen often, and (3) they can result in bodily harm. However, depending on where you live, car accidents may be so infrequent that the risk is reduced to medium.

You can try to transfer the risk of a car accident to the public transportation system by taking a bus. However taking a bus does not completely eliminate the risk of an accident; it just transfers some of the risk of an accident to the public transportation system. There is still a chance for an accident involving the bus, and you remain ultimately responsible for getting to work.

Alternatively, you can avoid the risk of a car accident by staying at home or traveling only on foot. However, staying at home and not showing up at work may lead to the loss of a job. Doing all your travel on foot greatly reduces your mobility and may be very inconvenient.

If you choose to drive, you can reduce the chance of getting into an accident by paying attention to other cars and obeying traffic regulations, such as the speed limit. But careful driving alone does not eliminate the chance that you will be involved in a car accident. As a result, at some point you must conclude that you have taken sufficient precautions and are going to drive the car regardless of the remaining risks.

Risk reduction and acceptance often go hand-in-hand for the reason discussed above—it is impossible and prohibitively expensive to eliminate all risk.

The same principle can be demonstrated in a grant-related example. Most grant programs have an eligibility risk—the chance that funds will be paid to an ineligible person or organization. A program can transfer the eligibility risk by outsourcing the eligibility determination. However this will have a limited effect because the program remains ultimately responsible for ensuring grants are made to eligible grantees.

The program may attempt to avoid that risk by not engaging in any grant activity—a course of action that may not be acceptable to the legislature or the public. Management may take certain actions to reduce the eligibility risk, for example, instituting a review process for all applications and requiring supervisory review of payments before they are made. If management is confident of the control measures in place and decides that the cost of additional measures outweighs any potential benefits, it may accept the remaining risk of paying an ineligible grantee.

The payroll process provides another example. There is always a risk that a non-employee will be paid. The larger an organization’s head count, the harder and more expensive it is to ensure this does not happen. The risk can be transferred by out-sourcing the payroll process, but the agency still retains the risk of inappropriate payment. Avoidance is also an unlikely option unless the organization decides to cease operations.

The risk of paying a non-employee can be reduced by taking several actions such as restricting access to the payroll application, requiring written approval for additions and removals from the payroll, and a management review of the payroll before it is paid. At some point, management may be confident enough of existing controls to accept any remaining risk.
Risk Acceptance

One of the most confusing tasks management faces in completing a risk assessment is how to document risk acceptance. Risk acceptance occurs where management determines that the control measures in place are, given the resources available, sufficient to address the identified risks. In accepting risk, management acknowledges that it is impossible to completely eliminate risk, and at the same time asserts that it has made the best use of existing resources to address its most critical risks.

A risk acceptance document therefore contains at least two elements: (i) a list of risks, and (ii) management’s justification for not addressing some non-critical risks (i.e., how management gained confidence that it had minimized the potential negative outcomes from these risks).

A thorough risk assessment documents management’s acceptance of risk. The risk assessment documentation, especially the risk grid, includes a list of risks, how management has addressed them, and if applicable, control gaps. Because of resource limitations, a risk assessment cannot list all risks. Rather, it should list all critical risks, thereby providing the first element of a risk acceptance document.

A risk assessment’s risk rankings and control activities demonstrate how management has gained confidence that it has minimized the potential negative outcomes from the risks. The risk rankings help management allocate resources by identifying the most critical risks. It would be expected that the most resources would be directed at addressing the most critical risks.

Using the risk assessment to document management’s risk acceptance avoids the time consuming and resource draining alternative of having to perform a cost-benefit analysis to justify why management has not addressed non-critical risks. However, to successfully document risk acceptance, the risk assessment must be thorough in identifying critical risks.

Finally, there may be instances where a risk remains so significant even after steps have been taken to mitigate it, a separate risk acceptance approval by management would be appropriate. In such cases, management should separately document the risk and steps it has to minimize it. This separate risk assessment should be approved in writing by management.
GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES

CONTROL ACTIVITIES – FORMULATING ACTIONS THAT WILL REDUCE THE CHANCE OF THINGS GOING WRONG

Once the risk assessment has been completed, management must take steps to ensure that all significant risks are addressed. Control activities are tools, including policies, procedures, actions and other mechanisms, that help ensure actions are taken to address risks (“what can go wrong?”). They are essential for proper stewardship and accountability of government resources and for achieving program goals and objectives. Control activities should be recognized as an integral part of each business process, rather than as a separate system. Strong control activities reduce the risk of:

- Failure to meet organizational goals and objectives,
- Business breakdowns or unexpected results,
- Excessive re-work to correct errors,
- Erroneous management decisions based on inaccurate, inadequate or misleading information, and
- Fraud, embezzlement and theft.

No one control activity provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity may be sufficient in reducing one or more risks.

Control activities encompass a wide array of actions, from simple steps such as locking a filing cabinet, to more complex measures like analyzing and approving grant applications. Control activities occur at all levels and functions of an organization, from data entry to management reviews. In short, control activities represent sound business practices.

Control activities benefit, rather than hinder, the agency by helping to achieve organizational goals. They are not intended to limit or interfere with an agency’s duly granted authority related to legislation, rule-making or other discretionary policy-making. Instead, control activities can actually help ensure the agency is acting within their authority and complying with legislative requirements.

The implementation of control activities must always consider costs and benefits, especially since most agencies struggle with limited resources, such as staffing, funding, and time. Excessive or duplicative control activities should be avoided; attempting to completely eliminate a risk is generally not achievable, would be prohibitively expensive and would most likely slow down productivity. As a general rule, the cost of implementing and sustaining a control activity should not exceed the benefits derived from that control activity. For example, purchasing an expensive locked cabinet to limit access to basic office supplies may not be considered cost effective. Alternatively, using a locked cabinet to secure highly negotiable assets such as daily cash receipts would be considered cost effective.

The concepts underlying control activities are likely to be similar across all agencies, but the form and formality with which they operate will vary. Smaller agencies rely on highly effective management controls instead of other types of control. For example, management’s retention of authority for approving significant purchases can provide strong control over this activity, lessening the need for more detailed or redundant control activities. Setting up an appropriate segregation of duties can also be challenging in a smaller agency. However, even agencies with only a few employees can assign responsibilities to achieve appropriate segregation, or use management oversight of the incompatible activities to achieve a strong control structure.
Designing Control Activities

An ideal control activity has three features: a carefully thought-out design, effective operation, and frequent updates. A good understanding of the underlying business process, obtained by performing a risk assessment, and the participation of staff directly involved in the business process, are critical to the creation of a well-designed control activity that addresses the risk in question. Control activities, especially those dependent on human actions, are effective only if they are operated when they should, as they should. This means the control activities are in operation and are a requirement. Finally, subjecting business processes to periodic risk assessments keeps the related control activities updated for changing circumstances. Positive results, including fewer errors, and less rework, fraud, waste, and abuse, allow management and staff to focus resources on the organization’s primary goals. In summary, a control activity has the following characteristics:

1) It addresses the risk in question;
2) It is mandatory; and
3) It is currently in operation.

Control activities that stray from the ideal often disrupt the underlying business process and cause operational bottlenecks. A poorly designed control activity is particularly dangerous because it can lull management and staff into a false sense of security.

Control activities can be classified as preventive or detective. Preventive control activities (also known as front-end control activities) are designed to avoid errors or improprieties before a transaction is processed. Examples of preventive controls are authorization lists, security access restrictions, system edit checks and requiring supervisor approval prior to processing. Detective control activities (also known as back-end control activities) are designed to identify errors or irregularities that have already occurred and enable management to take prompt corrective action. Examples of detective controls are reconciliations and exception report reviews.

Control activities can also be manual, automated, or IT-dependent manual. It is not unusual for a business process to include a combination of these three classes of control activities. Manual control activities are performed by individuals, such as preparing a bank deposit or performing a reconciliation. Automated controls are incorporated into application systems. Automated controls are considered more reliable, due to their ability to prevent errors from being entered into the system (e.g., inaccurate vendor id) and by detecting/correcting errors within the system (e.g., exception reports). Additionally, automated controls occur consistently with every transaction, whereas manual controls are more susceptible to human error. IT-dependent manual control activities are manually performed but require input based on the results of computer-produced information. Examples of IT-dependent manual controls include management’s review and follow up of a monthly variance report. Management relies on the information system to identify variances and produce the variance report.

Control activities can also be considered soft or hard. Soft control activities are those that provide notice of a requirement but do not themselves immediately terminate a transaction for failing to meet that requirement. Examples of soft controls include statutes, rules, policies and procedures all of which tell people what should and should not be done. Soft control activities are less effective if not paired up with hard control activities to enforce them. Hard control activities are those that terminate a transaction for failing to meet a requirement. Examples of hard control activities include passwords and
authorization codes. Hard control activities can be preventative, such as passwords, or detective, such as audits.

**Control Activity Categories**

The following are categories of commonly used control activities. This is by no means an exhaustive list.

**Documentation**

Documentation is perhaps the most critical control activity because it preserves evidence to substantiate a decision, event, transaction, or system. All documentation should be complete, accurate, and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the agency. Examples of areas where documentation is important include:

- **Critical decisions and significant events** generally involve senior management. These decisions and events usually result in the use, commitment, exchange or transfer of resources, such as in strategic plans, budgets and executive policies. By recording the information related to such events, management creates an agency-wide history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

- **Transactions** should be traceable from inception through completion to demonstrate how agency resources were utilized and control activities were applied to ensure compliance with agency objectives. This means the entire life cycle of a transaction should be documented, including: (1) its initiation and authorization; (2) its progress through all stages of processing; and, (3) its final classification in summary records (e.g., accounting records, inventory records, program management records, etc.).

- **Policies and procedures** are critical to the daily operations of a department. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction and help form the basis for decisions made every day by employees. Without this framework of understanding by employees, conflict or inconsistencies can occur, poor decisions can be made and serious harm can be done to the department’s reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

**Authorization and Approval**

Authorization is the power granted to an employee to perform a task. It is a delegation of duties. Management defines the terms of the authorization and ensures that those terms are documented and clearly communicated. Approval is the confirmation or sanction of employee decisions, events or transactions, based on an independent review. It signifies that the approver has reviewed the supporting documentation and is satisfied that the transaction is accurate and complies with applicable laws and regulations. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority.

**Verification / Reconciliation**

Verification (or reconciliation) typically 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. It is a control activity that
enables management to ensure that other control activities are being performed in accordance with directives. Management should determine what needs to be verified or reconciled, based on the inherent risk of the underlying process. Management should clearly communicate and document these decisions to those responsible for conducting the verifications. The list below offers some examples of verification and reconciliation.

- Reviewing vendor invoices for accuracy by comparing to purchase orders and contracts
- Reviewing grantee documentation prior to making grant payments
- Comparing cash receipts transactions to a cash receipts log and tracing to bank deposit records
- Reviewing and verifying a participant’s eligibility for state program services
- Reconciling a department’s cash records to bank statements

**Separation of Duties**
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. The fundamental premise of segregated duties is to prevent any one individual from controlling and performing all key functions of a transaction or event: initiation, authorization, record keeping, and custody. A combination of two or more of these functions performed by the same employee is called incompatible duties. The list below offers some examples of incompatible duties:

- Individuals responsible for data entry of invoices should not be responsible for approving these documents (record keeping and authorization)
- Individuals responsible for acknowledging the receipt of goods or services should not also be responsible for purchasing or payment activities (custody and record keeping)
- Individuals doing personnel onboarding (i.e., direct deposit, update/correct and personal data/job data updates) should not have access to mass time entry, business expenses or payroll adjustments (initiation and record keeping)
- Managers should review and approve payroll expenses and time sheets before data entry, but should not be involved in preparing payroll transactions (authorization and record keeping)
- Individuals performing physical inventory counts should not be involved in maintaining inventory records nor authorize withdrawals of items maintained in inventory
- Individuals receiving cash into the office should not be involved in authorizing and recording bank deposits in the accounting records (custody, authorization and record keeping)
- Individuals receiving revenue or making deposits should not be involved in reconciling the bank accounts (custody and record keeping)

In cases where duties cannot be effectively separated, management can substitute increased review or supervision as an alternative control activity (i.e., a compensating control) to help reduce the risks. In an environment with a very limited number of employees, management needs to be involved in reviewing and approving transactions, reports, and reconciliations.

**Access Security**
Securing access to resources and information reduces the risk of unauthorized use or loss. Management should protect the department's equipment, information, cash receipts, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals only. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.
The list below offers some examples of control activities used to safeguard physical assets.

- Securing mobile items within locked facilities
- Locking up cash receipts
- Utilizing key cards to limit access to agency facilities
- Performing periodic physical inventories of assets for verification of values, location, and appropriate utilization

Access controls restrict access and safeguard data files and information maintained in information systems. 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. Access controls include the use of multilevel security, user identification along with regularly changed passwords, call backs and dial-up systems, firewalls, limited access to not public data, and encryption of confidential information. Periodic management reviews of system access should occur to ensure employee access is appropriate based on any new or changed job duties.

**Supervision**
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. Those with the responsibility for supervision should:

- Assign tasks and establish written procedures for completing assignments
- Systematically review each staff member's work
- Approve work at critical points to ensure quality and accuracy
- Provide guidance and training when necessary
- Document supervisory reviews (for example, initialing examined work)

**Reporting**
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. Reporting also helps promote accountability for actions and decisions. The list below offers some examples of effective and accurate reporting.

- Project status reports to alert management to potential cost or time overruns
- Payroll Register reports to confirm accuracy of current and prior pay period adjustments, salary increase adjustments, special payments, earnings codes, hours, pay rates, salary amounts, and amounts of any lump-sum payments
- The State’s Comprehensive Annual Financial Report (CAFR) issued for the public’s review of Minnesota’s financial performance and position

**Control Gaps and Redundancies**

Once all the control activities within a process are identified, it may become apparent that control gaps and redundancies exist. A control gap occurs when there are either insufficient or no actions taken to avoid or mitigate a significant risk. For example, in a process that involves the collection of large amounts of cash, there is a control gap if no effort is made to secure the cash before depositing it. A redundancy occurs when multiple control activities address the same risk. Control redundancies often occur by design provide additional assurance in high risk circumstances. As explained below, the removal of a redundant control should occur only after careful consideration of the consequences.
Control gaps should be clearly documented in the risk assessment in a manner that draws them to the attention of management. Each control gap should be reviewed to confirm that there is a control gap and to evaluate potential steps to address that risk. Where possible, a plan should be formulated to address the gap and assign a target resolution date. Risk assessments with control gaps should be reviewed more frequently so that management can ensure corrective action is being taken where necessary.

On the other hand, redundant controls should only be removed where a written determination has been made that eliminating the control does not jeopardize the process. Redundancy should not be the only factor leading to elimination of the control. Seemingly redundant controls may themselves address multiple risks within other processes.

**Prioritizing Control Activities**

When going through the initial exercise of identifying control activities within a particular process, the list of control activities can become quite extensive. Even though it may be beneficial, in certain situations, to have back-up controls in case a main control activity fails, managing a large number of redundant control activities can reduce business process effectiveness and waste time and resources. Control activities are only as important as the risks they address, and management cannot devote the same amount of resources to all control activities. At this point, the judgment of management and subject matter experts is needed to determine which individual controls are key to addressing one or more significant risks in the event that all other controls fail.

A key control activity is (1) one that addresses one or more significant risks to an organization or business process, or (2) one that addresses multiple lesser risks that cumulatively are significant. However, even if the control activity meets one or both these criteria, whether it is a key control activity is a management decision.

Once the key control activities have been identified, documentation of the key control activities is essential to showing that key control activities actually exist and are effectively designed. The documentation also provides management with a clear picture of critical points requiring special attention when proposing modifications to the existing process. Documented details about each key control include identifying who is performing the control, when the control occurs and at what frequency, how the control is performed, what evidence exists that the control was performed, and which reports, if any, are used in the operation of the control activity. It may be helpful to bold the description of the key control activity in the process narrative or highlight it in the flowchart to make it more visible.

**Evaluating Key Controls**

To ensure a key control activity operates as intended, a two-step evaluation is performed: (1) determining whether the control activity is properly designed, and (2) assessing whether the control activity is operating effectively.

To determine whether a key control activity is properly designed, a reviewer, independent of the activity, evaluates the design of the control by answering the following questions:
GUIDE TO RISK ASSESSMENT AND CONTROL ACTIVITIES

- Does the control activity occur at the right point in the process?
- Does the control activity occur at the right frequency?
- Would the control activity prevent or detect the intended error or nonconforming circumstance (e.g., ineligible recipient, inaccurate amount, etc.)?
- Is the control activity the most cost effective way to address the risk?

To assess whether a key control activity is operating effectively, an independent reviewer performs a “walkthrough” of the process to ensure the employee or application performing the key control activity is in fact doing the tasks described in the narrative or flowchart. A walkthrough is normally performed using documents that are typical of the process being reviewed. It is recommended to perform a walkthrough for at least one transaction, event or activity. During the walkthrough, employees performing the tasks should be questioned at each point where key processing controls are indicated. The questions should focus on the employee’s understanding of what is required and whether the processing procedures and controls are performed on a regular basis.

To corroborate information obtained at various points in the walkthrough, employees should be asked about their understanding of the control activities and to demonstrate what they do. Exceptions to the prescribed processing procedures and controls should be identified as well as any differences between what the narrative or flowchart indicates and what is actually done. For example, if the control activity is an employee review, and the employee is required to initial a document as evidence of having reviewed it, it is recommended to inquire about the nature of the review performed and ascertaining whether the reviewer initials or otherwise documents their review. Furthermore, it is important to ask what the person does if the review process reveals an error or other discrepancy in the document, and if appropriate, examine documents where problems were detected to confirm that appropriate actions were taken. If the control consists of the preparation and analysis of a periodic reconciliation, the following steps are recommended:

- Review one or more of the reconciliations to determine whether all the relevant data are accurately and promptly included
- Note the explanation and disposition of any unusual items
- Inquire about the actions taken when actual or potential errors are indicated on the reconciliation
- Inquire how the errors occurred
- Whenever practical, obtain evidence of the correction of the errors that were noted during the reconciliation process
- Ensure timely completion of the reconciliation and clearing of reconciling items

In addition to walking through the physical flow of documents and forms, the flow of data and information through the automated processes should be followed. These steps may include inquiry of independent and knowledgeable personnel, review of user manuals, observation of a user processing transactions at a terminal in the case of an online application, and review of documentation such as output reports.

Two outcomes are possible upon completion of a walkthrough:

1. The process outlined in the narrative/flowchart matches the actual process, and the key control activities are documented and operating as intended.
2. The process outlined in the narrative/flowchart does not match the actual process, and some key control activities are not operating as intended. Action steps should be developed to revise the narrative/flowchart and improve the effectiveness of these control activities. At a later point in
time, the revised control activities should be re-evaluated to ensure they are operating effectively.

Walkthroughs of processes and related control activities should be documented (i.e., brief memos) describing the procedures performed. This documentation provides proof that management determined whether the key control activities were effectively operating to mitigate risks.
UPDATING THE RISK ASSESSMENT AND IDENTIFIED CONTROL ACTIVITIES

Preparing a risk assessment is not a one-time exercise—Each risk assessment should be updated at least annually or whenever there are significant changes to the related agency, department, program, or process (e.g., from new legislation). Remember, organizations constantly change (e.g., changes in staff or technology), and the risks and control activities related to processes change with them.

New and existing risks—Because the services, processes and functions within an agency constantly change, new risks will arise and existing risks will change in their effect on each process. New risks need to be evaluated to determine what control activities currently exist or need to be developed to manage these risks. Existing risks could become more or less critical, affecting management reaction to them. Because of this unavoidable change to the circumstances affecting each service, process, and function, each risk assessment must be reviewed at least once a year.

Effectiveness of control activities—Control activities used to address significant risks should be periodically assessed to verify that they are cost beneficial and continue to operate effectively. Management should reconfirm that individual controls identified as key controls are continuing to operate as designed.

Senior management involvement remains critical to the on-going risk assessment process—Senior management directs the allocation of time and resources, and are uniquely placed to identify changes to the services, processes, or functions within an agency. Without senior management’s involvement as champions, it is difficult to get the participation of other employees.

Updating a risk assessment is usually easier than creating one—The update process is easier because the initial compilation of information and documents is completed when the risk assessment is created. Unless there are significant changes to the agency, department, program or process, updating the risk assessment will involve making tweaks to the documentation and therefore takes less time. An annual walkthrough is recommended as part of the annual update process. Performing a walkthrough confirms the process is functioning as intended and control activities continue to operate effectively.
BIBLIOGRAPHY


7. Minnesota Statute 16A.057 Internal Controls and Internal Auditing


