



INTERNAL AUDIT

Risk Assessment Procedure

Issued: April 22, 2016

Number: FMR-0102-01

Revised:

Objective

The Department of Administration (Admin) is subject to Minnesota Management and Budget's (MMB) Statewide Operating Procedure number 0102-01.2: Risk Assessment. Risk assessment is the second component of the *Standards for Internal Control in the Federal Government*, also known as the *Green Book*. Admin completes risk assessments for the purpose of documenting potential negative events and assessing the likelihood of occurrence and severity if it did occur so that the agency can decide whether or not to establish internal controls to mitigate the risk. Risk assessment is the precursor to designing, implementing, documenting and periodically assessing internal controls, because internal controls should support risk analysis decisions. In other words, first you understand the risks, and then you establish the controls.

State Operating Procedure 0102-01.2 requires Admin to:

- Conduct a high level, but comprehensive, review of the most significant, high profile business processes
- Create or update a formal agency-specific risk assessment plan. The plan must include the most significant, high profile processes or sub-processes
- Document decisions for why some processes/sub-processes are included in the risk assessment plan and why others are not
- Assign responsibility for ensuring the risk assessment plan is implemented. Projects identified in the risk assessment plan must meet the following criteria:
 - Performed within the timeframe specified;
 - Sufficiently documented;
 - Results and corrective action plans for control gaps/weaknesses are communicated to management;
 - Are periodically reviewed and updated; and,
 - Documentation is readily accessible for third party (e.g., auditor) review.

The objective of this procedure is to document Admin's risk assessment processes, define the annual risk assessment plan and demonstrate compliance with State Operating Procedure 0102-01.2.

General Procedures

Financial Profile

All risk assessments must consider both qualitative and quantitative factors. The financial profile is the agency's risk measure using purely quantitative factors: financial results.

Step	Action	Responsible Party	Timeline								
1.	Review the previous year's agency financial profile. Determine that the financial results measured are still relevant and useful for analysis. Determine that all Admin divisions are represented.	Internal Audit	October Annually								
2.	Initiate the financial profile with Financial Management and Reporting (FMR). Prepare and send a blank profile spreadsheet for FMR's completion. Request values as of the close of the previous fiscal year. The previous fiscal year is used for ease and availability of results and the data is still considered relevant and timely for the purpose of risk analysis.	Internal Audit	November Annually								
3.	Complete the financial profile spreadsheet.	FMR	November – December Annually								
4.	Calculate the percentage of the agency total for each financial measure. Assign a risk assessment to each result as follows: <table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Percentage of the agency total</td> <td style="width: 50%;">Risk rating</td> </tr> <tr> <td><i>0% to 5%</i></td> <td><i>Low</i></td> </tr> <tr> <td><i>5% to 25%</i></td> <td><i>Medium</i></td> </tr> <tr> <td><i>25% and higher</i></td> <td><i>High</i></td> </tr> </table>	Percentage of the agency total	Risk rating	<i>0% to 5%</i>	<i>Low</i>	<i>5% to 25%</i>	<i>Medium</i>	<i>25% and higher</i>	<i>High</i>	Internal Audit	January - February Annually
Percentage of the agency total	Risk rating										
<i>0% to 5%</i>	<i>Low</i>										
<i>5% to 25%</i>	<i>Medium</i>										
<i>25% and higher</i>	<i>High</i>										
5.	Summarize the results and concentrations of financial risk for the final report.	Internal Audit	March Annually								
6.	Calculate the changes from year-to-year in the financial profile. Identify the largest changes from year-to-year in terms of both dollars and percentage.	Internal Audit	March Annually								

Step	Action	Responsible Party	Timeline
7.	Analyze the reason for the changes, with the assistance of FMR, as needed.	Internal Audit & FMR	March - April Annually
8.	Include a summary of the significant changes in the final report.	Internal Audit	June Annually

Agency-wide risk assessment survey

Together with the financial profile, the risk assessment survey is the comprehensive overview of agency risks. The risk assessment survey is a qualitative measure of risk. The purpose of the survey is to help the Senior Leadership Team (SLT) analyze Admin’s functions from a risk based perspective. A survey method is utilized for measuring risk on an agency-wide basis for a several reasons:

- Involves as many members of management as possible;
- Spreads the burden of gathering information to the Admin’s management team;
- Minimizes the time commitment required of any one individual;
- Measures risk in a broader sense than purely financial; and,
- Leverages technology for ease of survey taking and results compilation.

The survey presents a series of high risk scenarios and asks participants to rate their exposure to that risk on a scale of one to five; five being the highest risk exposure and one being minimal or no risk exposure. Survey participants are asked to rate their risk exposure absent internal controls. In other words, survey participants are asked to rate the chances the negative event described would occur if there were no controls.

The risk assessment survey is divided into five elements:

1. Financial
2. Compliance
3. Operational
4. Information Technology (IT), and
5. Strategic

After answering a series of questions within each element, each participant is asked to rate their exposure to that element as Low, Medium or High. The following methodology is used to assign a total risk rating to each business risk unit:

Risk Element	# of questions	Weight	Low Risk	Medium Risk	High Risk	Total Risk Score
Financial	16	40	0.3	0.6	1.0	Weight x Risk Rating
Compliance	5	10	0.3	0.6	1.0	Weight x Risk Rating
Operational	16	25	0.3	0.6	1.0	Weight x Risk Rating

Risk Element	# of questions	Weight	Low Risk	Medium Risk	High Risk	Total Risk Score
IT	9	15	0.3	0.6	1.0	Weight x Risk Rating
Strategic	5	10	0.3	0.6	1.0	Weight x Risk Rating
Total	51	100				Total

The total risk score is used to assign an overall risk rating to each business risk unit follows:

Total Risk Score	Overall Risk Rating
30 – 45	Low
46 – 70	Medium
71 - 100	High

For example, a business risk unit with the following risk profile would receive a total risk score of 64 and an overall risk rating of *Medium*:

Risk Element	Risk Rating	Risk Rating score	Weight	Total Risk Score
Financial	Medium	0.6	40	24
Compliance	High	1.0	10	10
Operational	Medium	0.6	25	15
IT	Medium	0.6	15	9
Strategic	Medium	0.6	10	6
Total				64

Step	Action	Responsible Party	Timeline ¹
1.	Review and update the risk assessment survey. <ul style="list-style-type: none"> • Determine that questions asked are still relevant for Admin from a risk based perspective. • Consider emerging risks relevant to Admin when considering adding new questions. • Consider the format of the survey: <ul style="list-style-type: none"> ○ The survey should be accessible. ○ Preferably, the survey should be formatted so that it can be completed online. 	Internal Audit	April Annually
2.	Define the Admin universe:	Internal Audit and the	April Annually

¹ Preferably, the risk assessment survey should be completed annually. However, State Operating Procedure 0102-01.2 requires risk assessment activities at a minimum of once every three years.

Step	Action	Responsible Party	Timeline ¹
	<ul style="list-style-type: none"> • There were 26 defined business risk units in 2014 and 2015. • At a minimum, there should be a one-to-one relationship between divisions and business risk units. The exception is the Commissioner’s office which includes internal audit, communications, legislative and any other miscellaneous functions completed by the Commissioner’s staff. • Larger divisions may be divided into multiple business risk units, but the final decision of the number of units each division will be divided resides with the SLT member. <ul style="list-style-type: none"> ○ For example, the Plant Management Division is divided into four business risk units: <ul style="list-style-type: none"> ▪ Plant Management ▪ Parking Operations ▪ Central Mail ▪ Minnesota Bookstore 	Deputy Commissioner of Finance and Administration	
3.	Finalize the risk assessment survey.	Internal Audit	April Annually
4.	Train the Agency Leadership Team (ALT) on completing the survey. At a minimum, train new members of management and new participants. <ul style="list-style-type: none"> • Emphasize that management should complete the survey from an inherent risk perspective: assume there are no internal controls in place to mitigate the risk. 	Internal Audit	April Annually
5.	Issue the survey. <ul style="list-style-type: none"> • Error check the survey before issuing. • E-mail survey hyperlinks to each participant. 	Internal Audit	May Annually
6.	Complete the survey questionnaire.	ALT and other selected participants	May Annually
7.	Compile survey results <ul style="list-style-type: none"> • Ensure that each business risk unit has completed a survey. • Download and save each survey as a PDF. (Optionally, print and save in a 3-ring binder.) Files should be saved in the Risk Assessment – Agency folder of the Internal Audit file folder. 	Internal Audit	June Annually

Step	Action	Responsible Party	Timeline ¹
	<ul style="list-style-type: none"> Download results into an Excel spreadsheet to facilitate analysis. 		
8.	<p>Calculate the risk assessment scores and resulting risk rating based on the methodology.</p> <ul style="list-style-type: none"> Prepare the Agency risk profile; a table presenting the results for each business risk unit by risk element. Prepare a table presenting business risk units in descending order by total risk score. 	Internal Audit	June Annually
9.	<p>Analyze other risk data as needed.</p> <ul style="list-style-type: none"> Highest and lowest scoring questions. Highest and lowest average risk elements. Changes year-over-year; Identify emerging or declining risks. 	Internal Audit	June Annually
10.	<p>Based on the results of the survey and the agency financial profile, identify Admin divisions/business processes which are the riskiest for Admin and should be analyzed further from a risk and control perspective. Analyzing divisions/business processes from a risk and control perspective includes defining business risks in plain language, assessing those risks, and documenting the internal controls intended to mitigate those risks. This process is described in detail in the Risk Assessment Plan below.</p> <ul style="list-style-type: none"> Divide business processes into agency-wide (E.g. Payroll) and division specific (E.g. Parking). As of June 30, 2015, there were 20 business processes identified. The number of processes could grow or shrink based on changing conditions. 	Internal Audit and the Deputy Commissioner of Finance and Administration	June Annually
11.	<p>Compile the agency financial profile and risk assessment survey into a final report.</p> <ul style="list-style-type: none"> Include the final report in the annual internal control submission to MMB pursuant to MN Statute Section 16A.057, Subdivision 8. Distribute the report to the ALT. 	Internal Audit	July Annually

Risk Assessment Plan

The Admin risk assessment plan can vary from year-to-year based on changing conditions and available resources for risk assessment activities. However, on an annual basis, the risk assessment plan will consist of the following:

Step	Action	Responsible Party	Timeline
1.	Prepare an agency Financial Profile using results from the most recently completed fiscal year.	FMR and Internal Audit	Annually (but no less often than every three years)
2.	Complete the agency Risk Assessment Survey .	Internal Audit and Division Management	Annually (but no less often than every three years)
3.	For each Admin division/business process identified in Risk Assessment Survey step 10, prepare or update a Risk and Control Matrix.	Internal Audit	Annually; updates occurring in the first fiscal quarter, or when an audit occurs, whichever is sooner.
	a. Use the Risk and Control Matrix template (MS Excel file) and customize for the division/business process being reviewed.	Internal Audit	
	b. Brainstorm business risks and document them on the matrix. For example: <ul style="list-style-type: none"> • Overpayment • Non-payment • Non-compliance 	Internal Audit and Division Management	
	c. Assess business risks in terms of likelihood and severity. <ul style="list-style-type: none"> • Likelihood is the probability that a negative event will occur absent internal controls. • Severity is the relative damage (reputational, legal, financial, or operational) a negative event would impair management’s ability to achieve objectives. 	Internal Audit and Division Management	
	d. Document the risk mitigation strategy (Control, Share or Accept).	Division Management	
e. Document the management control objectives. Management control objectives are management’s high level objectives implementing internal controls. Definitions of management	Internal Audit		

Step	Action	Responsible Party	Timeline
	control objectives can be found in the Green Book.		
	<p>f. Document internal controls in place to mitigate the risk.</p> <ul style="list-style-type: none"> • Internal controls can be listed more than once: <ul style="list-style-type: none"> i. One internal control can mitigate multiple risks. The internal control number is in red when it appears under multiple risks. ii. One internal control can be listed more than once under the same risk when it satisfies multiple Green Book Components or Principles. • Internal audit should help division management identify controls that exist on an entity-wide basis. e.g. Code of Conduct certification or background investigations before employment. 	Internal Audit and Division Management	
	<p>g. Document the control type.</p> <p>Preventive controls are strongest because they are designed to prevent the negative event from occurring.</p> <p>Detective controls are designed to detect a negative event after it has occurred so it can be corrected and prevented from occurring again.</p> <p>Administrative controls document policies, procedures and practices.</p>	Internal Audit	
	<p>h. Select Key Controls. Key controls are the most critical to mitigating the risk. Key controls assist auditors plan their test work, as all key controls should be tested.</p>	Internal Audit and Division Management	
	<p>i. Select the Green Book Component(s) and Principle(s) the control satisfies.</p>	Internal Audit	
	<p>j. Determine that the controls documented satisfy all applicable Green Book Components and Principles.</p>	Internal Audit	

Step	Action	Responsible Party	Timeline
	<ul style="list-style-type: none"> • Continue documenting and/or adding internal controls until all applicable Green Book Components and Principles are satisfied. 		
	<p>k. Review each risk and determine whether documented controls mitigate that risk to an acceptable level. Document whether controls listed are “adequate”, “needs improvement”, or “excessive.”</p> <ul style="list-style-type: none"> • Internal audit should work with division management to develop and implement internal controls to mitigate control gaps noted. • If internal controls cannot mitigate the risk to a satisfactory level, use the Matrix form to document division management’s alternative risk mitigation strategy. (Share or Accept the risk) 	Internal Audit and Division Management	
4.	Retain the most recently completed risk and control matrices as an integral part of Admin’s documentation of internal controls. Internal control documentation should be available upon request from an authorized requester (e.g. Legislative Auditor)	Internal Audit and Division Management	Ongoing
5	<p>Update each risk and control matrix annually with division management.</p> <ul style="list-style-type: none"> • Highly recommended that internal audit and division management update each matrix prior to any announced internal or external audit. The auditor will rely on the accuracy of the matrix and likely test documented controls. 	Internal Audit and Division Management	Once Annually; recommended during the 1 st calendar (3 rd fiscal) quarter, but the timeline is not critical.
6	If resources do not permit completion of steps 1 – 5, Internal Audit should complete, and agency senior management should review and approve an analysis of significant changes since the last risk assessment was completed. This analysis (if completed) should be submitted to MMB’s internal control and accountability unit annually each July, along with the Internal Control System Certification Form and the Control Environment review.	Internal Audit and Agency Senior Management	June – July annually ONLY IF no other risk assessment activity completed during the fiscal year.

Step	Action	Responsible Party	Timeline
	<ul style="list-style-type: none"> To facilitate the analysis, consider using MMB’s “Ongoing Change Indicators for Completed Risk Assessments Questionnaire.” 		

Forms

[Internal Control System Certification Form](http://mn.gov/mmb/internalcontrol/executivebranchagencyrequirements/annualinternalcontrolsystemcertification/)

(<http://mn.gov/mmb/internalcontrol/executivebranchagencyrequirements/annualinternalcontrolsystemcertification/>)

Risk and Control Matrix template

(To be placed on an Admin website. MS excel document)

[Ongoing Change Indicators for Completed Risk Assessments Questionnaire](http://mn.gov/mmb/images/2014%2520RA%2520Ongoing%2520Change%2520Indicators%2520Wksht.docx)

(<http://mn.gov/mmb/images/2014%2520RA%2520Ongoing%2520Change%2520Indicators%2520Wksht.docx>)

Related Policies and Procedures

[MMB Statewide Operating Policy 0102-01 Internal Control System](http://mn.gov/mmb-stat/documents/accounting/fin-policies/chapter-1/0102-01-internal-control-policy.pdf)

(<http://mn.gov/mmb-stat/documents/accounting/fin-policies/chapter-1/0102-01-internal-control-policy.pdf>)

[MMB Statewide Operating Procedure 0102-01.2](http://mn.gov/mmb-stat/documents/accounting/fin-policies/chapter-1/0102-01-2-risk-assessment-procedure.pdf)

(<http://mn.gov/mmb-stat/documents/accounting/fin-policies/chapter-1/0102-01-2-risk-assessment-procedure.pdf>)

[MMB Risk & Control Activities](http://mn.gov/mmb/internalcontrol/internalcontrolframeworkandtools/riskassessment/)

(<http://mn.gov/mmb/internalcontrol/internalcontrolframeworkandtools/riskassessment/>)

Related Resources

[Standards for Internal Control in the Federal Government \(Green Book\)](http://www.gao.gov/greenbook/overview)

(<http://www.gao.gov/greenbook/overview>)