



Internal Controls

Risk Assessment & Control Activities Concepts and Template *Refresher*

January 2017



Agenda



- ✓ **Expectations and Themes**
- ✓ **Internal Control System Flow**
- ✓ **Assessing Risks**
- ✓ **Wording Discussions**



Template Expectations



- All organizations will need to complete a template
 - Includes attached agencies, etc
- SAO will be releasing a template with applicable cells completed for Shared Services
 - Organizations still responsible for their part of the process (such as initiating a transaction)
- Record tabs –all considerations related to recording items in your accounting records (be it in Teamworks or whatever method is used)

Common Themes



Common items from first round of templates:

- Risk justifications for inherent, likelihood and/or impact improperly consider control activities currently in place
- Items marked N/A with no further reasoning
- Risk justifications or control activities not applicable to specific risk example
- Control activities not detailed or significant controls not bolded
- Cells left blank with no further reasoning



Internal Control System Flow



Overview of the Process



- First start by establishing objectives
 - Today we will only be discussing the financial reporting objective (and compliance objectives relating only to financial reporting)
- Then consider risks getting in way of accomplishing those objectives – “identify risk”
 - Drive allocation of more resources to the areas of highest risk
- Consider how much risk are you willing to allow (risk tolerance) – “analyze risk”

Continuing On....



- Consider “risk responses”, which are control activities (common tasks – internal controls) already in place
- Do any of those activities offset the risk
 - If not, need to consider response (which could be doing nothing)
- Then repeat (it is a dynamic process)



Assessing Risks



“Risk Level Definitions” Tab



Contains:

- Definitions and instructions on filling out the various risk columns in the template

“Risk Level Definitions” Tab



Definition of Risks relating to financial reporting objectives		
(see Risk Assessment chapter in the Georgia Statewide Internal Control guidance for additional details)		
Instructions: for each of the specific risk examples noted on the following tabs, an analysis of risk tolerance has been performed:		
<i>Risk Tolerance Column (column D)</i>		
Level of risk willing to be accepted (but still maintain an appropriate internal control system)		
Listed in specific and measurable terms (such as acceptable error rates for the quality of financial data, timing of financial data, zero tolerance for certain errors, etc)		
Information on tabs is reported in column D in time periods, dollar variances, etc		
Instructions: for each of the specific risk examples noted on the following tabs, an analysis of inherent risk needs to be performed:		
<i>Inherent Risk Column (column E and F)</i>		
<u>Inherent</u> - risk relating to the each of the specific risk examples in the absence of management's response (internal controls), consider:		
- internal factor... of operations (level of judgment or		
	Start Here!!	Risk Level Definitions
		1-General Rcrd

“Risk Level Definitions” Tab



Inherent Risk

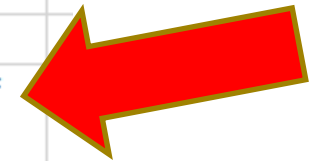
Instructions: for each of the specific risk examples noted on the following tabs, an analysis of inherent risk needs to be performed:

Inherent Risk Column (column E and F)

Inherent - risk relating to the each of the specific risk examples **in the absence** of management's response (internal controls), consider:

- internal factors such as complex nature of operations (level of judgment or special skills needed to determine financial numbers, number of transactions, etc.), organizational structure (extent of reliance on other areas or other systems, level of manual intervention, etc.), new personnel, new technologies, etc
- external factors such as new or amended laws, new Regulations, new Standards (including new Reporting requirements), economic instability, etc
- audit issues identified
- susceptibility to fraud

Information on tabs should detail a high, medium or low level (using chart below) in column E and a justification for that rating level in column F



“Risk Level Definitions” Tab



Risk Likelihood and Impact

Instructions: for each of the specific risk examples noted on the following tabs, an analysis of the likelihood and impact of the risk needs to be performed:

Likelihood and Impact Columns (column G, H, I and J)

Without considering the known control activities, analyze how big the specific risk would be.

Information on tabs should assign a level (from the chart below) for likelihood and impact of each risk in columns G and I and a justification in column H and J for that rating level.

Likelihood - level of possibility that a risk will occur, consider:

- ease of access to asset, liquidity of the asset, manual processing, etc

Impact - scale of the deficiency that could result from the risk, consider:

- size, pace, duration, etc of the risk



“Risk Level Definitions” Tab



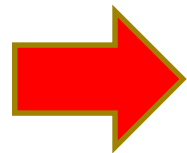
Risk Rating Levels

Rating Level		
High	Medium	Low
Poses a significant financial reporting risk.	Poses a moderate financial reporting risk.	Poses a minimal financial reporting risk.
Likely to require ongoing and continued resource commitment.	Likely to require moderate resource commitment.	Likely to require a low level of resource commitment.
Likely to involve complex control and accounting issues.	Likely to involve less complex control and accounting issues.	Likely to involve routine control and accounting issues.

“Risk Level Definitions” Tab



Residual Risk



<u>Residual Risk Column (column N and O)</u>	
<u>Residual</u> - risk that remains after management's response to inherent risk	
Considering the known control activities actually occurring, analyze the level of the remaining risk for each of the specific risk examples.	
Information on tabs should detail a high, medium or low level (using chart below) in column N and a justification in column O for that rating level.	

Now What?

- ✓ Use that guidance to fill out the risk columns in the template
- ✓ Remember depending on which risk – will determine if you do not or do consider control activities currently in place



Key Terminology – Risks



- Consider what risks will get in the way of accomplishing the objective
 - Break down in to specific risks, as necessary
- Need to consider for service organizations (outside third parties) too! (ex: Teamworks infrastructure is outsourced but SAO is still responsible for internal controls relating to that outsourced work)
- Consider fraud and Information System related risks throughout

Now Apply the Concept



Note that the risks are driven by the objectives:

Statewide Guidance Attribute	7.1	
Financial Reporting Obj.	Risk	Specific Risk Examples
A	B	C
The accounting records comply with Standards and are complete and accurate	Key assets are not all recorded at the proper amount, in the proper fund, in the proper account code or in the proper basis of accounting.	Cash is not all included or not recorded at the correct amounts in the accounting records
The financial reports are complete and accurate	Information provided on year end forms does not agree with accounting records and/or supporting documentation.	Allowance for Doubtful Accounts: - appropriate research not performed to include all needed items
The financial reports are available on a timely basis	Reports are not available timely	Not submitting forms to SAO based on due dates noted in year end calendar

Key Terminology - Risk Tolerance



- **Definition:**
 - Essentially how much risk an organization is willing to accept
 - What is the acceptable level of variation in performance compared to the achievement of objectives
- **Guidance:**
 - Establish an acceptable error rate
 - List in specific and measurable terms (such as acceptable error rates for the quality of financial data, timing of financial data, zero tolerance for certain errors, etc)

Now Apply the Concept



Risk Tolerance Examples:

- Establishing a low risk tolerance relating to financial reporting for such things as: timeliness, transparency, GAAP, etc.
- Establishing a zero tolerance for violating standards of conduct

Note: in the template this has been pre-established as de minimis

Key Terminology – Inherent Risk



Risk to the organization in the *absence of management's response* (internal controls), consider:

- Internal factors such as:
 - Complex nature of operations (level of judgment or special skills needed to determine financial numbers, number of transactions, etc.)
 - Organizational structure (extent of reliance on other areas or other systems, level of manual intervention, etc.)
 - New personnel
 - New technologies
 - Etc

Key Terminology – Inherent Risk



Risk to the organization in the absence of management's response (internal controls), also consider:

- External factors such as:
 - New or amended laws
 - New Regulations
 - New Standards (including new Reporting requirements)
 - Economic instability
 - Etc
- Audit issues identified
- Susceptibility to fraud

Now Apply the Concept



Inherent risk would be rated high, medium, or low, with a justification added.

Note that the risk rating and justification is driven by the specific risk examples *before consideration of control activities* actually in place.

Wording Discussion.....



Inherent Risk – Justification Example (original wording)

Person completing the form reviews the question with appropriate senior management to answer the questions appropriately, we are a small agency and Director is aware of most things in which the agency is involved

Does that wording seem like it is assessing risks before consideration of control activities

Wording Discussion.....



Inherent Risk – Justification Example (original wording) - continued

Person completing the form reviews the question with appropriate senior management to answer the questions appropriately, we are a small agency and Director is aware of most things in which the agency is involved

These items underlined are actually listing control activities.

Wording Discussion.....



Inherent Risk – Justification Example (original wording)

N/A

Explain why is it not applicable:

- That form does not apply to you?
- That form does apply to you but is blank?
- You do not have any of that item in your accounting records?

Wording Discussion.....



Inherent Risk – Justification Example (suggested revisions)

- high susceptibility to fraud, has a lot of transactions and requires manual entry of deposit
- not inherently risky because accounting standards have not recently changed
- requires manual entry of billing - and there are numerous types of different billings done
- This is a complex process that involves numerous other Departments recording their data

This wording is assessing risks before consideration of control activities

Key Terminology – Likelihood



Level of possibility that a risk will occur:

Without considering the **known control activities** (internal controls) actually occurring, analyze how *likely* the specific risk would be.

Certain factors to contemplate could be:

- Ease of access to asset
- Liquidity of the asset
- Manual vs automated processing
- Etc

Wording Discussion.....



Risk Likelihood – Justification Examples (original wording)

- The account is reconciled monthly. Any differences are identify and researched.
- Receivable analysis is done quarterly

Does that wording seem like it is assessing risks before consideration of control activities or is it listing control activities

Wording Discussion.....



Risk Likelihood – Justification Example (original wording)

N/A

Explain why is it not applicable:

- That form does not apply to you?
- That form does apply to you but is blank?
- You do not have any of that item in your accounting records?

Wording Discussion.....



Risk Likelihood – Justification Examples (suggested revisions)

- there are a lot of transactions to be recorded
- only receivable relates to Federal government which has minimal activity
- billing system is not integrated in to accounting system so a lot of manual entry is required

This wording is assessing risks *before consideration of control activities*

Key Terminology – Impact



Scale of the deficiency that could result from the risk

Without considering the **known control activities** (internal controls) actually occurring, analyze what the *scale* of the specific risk would be.

Certain factors to contemplate could be:

- Size
- Pace
- Duration
- Etc

Wording Discussion.....



Risk Impact – Justification Examples (original wording)

- The form is submitted by Director who is familiar with the reconciliation of the staff preparing it
- Information is being pulled directly from Teamwork's to complete CAFR Forms

Does that wording seem like it is assessing risks before consideration of control activities or is it listing control activities

Wording Discussion.....



Risk Impact – Justification Example (original wording)

N/A

Explain why is it not applicable:

- That form does not apply to you?
- That form does apply to you but is blank?
- You do not have any of that item in your accounting records?

Wording Discussion.....



Risk Impact – Justification Examples (suggested revisions)

- minimal cash comes in at the pool offsite
- the overall dollar amount is not material
- receivable balance is minimal (less than 1% of total revenue received)
- Dollar amounts reported are high. Information is publicly reported and could be relied upon by numerous users (such as the Federal Government, Legislators, Bond Rating Agencies or citizens).

This wording is assessing risks before consideration of control activities

Key Terminology – Risk Response



Management designs risk responses to respond to the analyzed risks. Responses could include:

- Acceptance - no action is taken
- Avoidance - action is taken to stop the operational process (for example, stop allowing cash to be collected offsite or stop collecting cash at all)
- Reduction - action is taken to reduce the likelihood or magnitude of the risk (for example, segregate duties, have more oversight, etc)

Key Terminology – Control Activities



Actions management establishes through policies and procedures to achieve objectives and respond to risks (including fraud risks) in the internal control system

- Essentially, these are the tasks already being performed
- Remember this also includes information systems considerations

Control activities are generally in these common categories

- Segregation of duties
- Accurate and timely recording of transactions
- Proper execution of transactions
- Reconciliations
- Controls over information processing
- Physical controls over vulnerable assets
- Access restrictions to and accountability for resources and records

Control activities are generally in these common categories (continued):

- Appropriate documentation of transactions and internal controls
- Establishment and review of performance measures and indicators
- Reviews by management at the functional or activity level
- Top-level reviews of actual performance
- Management of personnel

Wording Discussion.....



Controls Activities Example - Allowance for Doubtful Accounts specific risks:

- not completely filling out all of the required information
- not properly calculating uncollectible percentages based on past history
- not properly reporting uncollectible percentages to applicable accounts receivable

Controls activities answer (original wording)

The staff preparing the report form has a Bachelor Degree in Accounting and more than 20 years experience in financial reporting, including SAO FYE financial reporting procedures, GASB and State Accounting Policies and Procedures policies and Guidelines. Reconciliations are performed prior to final approval from the Director and CFO.

Wording Discussion.....



Controls Activities Examples - Allowance for Doubtful Accounts (original wording) - continued:

Does that answer wording seem like it is detailed with significant controls **bolded** and applicable to the specific risk example

The staff preparing the report form has a Bachelor Degree in Accounting and more than 20 years experience in financial reporting, including SAO FYE financial reporting procedures, GASB and State Accounting Policies and Procedures policies and Guidelines. Reconciliations are performed prior to final approval from the Director and CFO.

Wording Discussion.....



Controls Activities Example - Allowance for Doubtful Accounts: (suggested revisions)

- 1. Accounts receivable clerk fills out the form - they have an Associates and three years of related experience.
- ***2. The accounts receivable clerk followed instructions/guidance on forms carefully:***
 - 2 a. ran query in Teamworks (excluding receivables with other State organizations), pasted information from pivot on to form by three digit revenue account
 - 2b. determined uncollectible percentage based on trends from last 3 years

Wording Discussion.....



Controls Activities Example - Allowance for Doubtful Accounts: (suggested revisions) - continued

- 2 c. entered and applied percentages to applicable amounts outstanding
- 3. AR clerk then compares amounts recorded on form to amounts on June 30th general ledger, and follows up on any discrepancies.
- 4. ***Accounting supervisor verified calculations performed and the form completed by accounts receivable clerk prior to submission to SAO.*** Accounting supervisor has bachelor's degree and five years of experience.

Wording Discussion.....



Controls Activities Example (original wording)

N/A

Explain why is it not applicable:

- Likelihood and impact are both rated as low?
- You do not have any of that item in your accounting records?

Key Terminology – Residual Risk



Risk that remains after management’s response to inherent risk

Considering the **known control activities** (internal controls) actually occurring, analyze the ***level of the remaining risk*** for each of the specific risk examples.

Submission Expectations



- Mark N/A if not applicable (leave no blanks)
- Submit to SAO:
 - Via compliance@sao.ga.gov or paper mail
 - Include the organization code in the file name
 - Specify, in the email or document, if it also covers an attached agency or related organization
- **The completed template and any related documentation relating to the recording tabs (highlighted orange) are due to SAO by February 28, 2017 (1 – General Rcrd, 2 – Rev Collec Rcrd, and 5 – BCR Rcrd)**

Where to Find Information



The Green Book is available on GAO's website at:

www.gao.gov/greenbook

SAO's website:

<http://sao.georgia.gov/internal-controls>

Information will be added when available

My Contact Information:

Rachael.Krizanek@sao.ga.gov