Risks – Identifying, Assessing and Managing Them

By Torpey White, CPA/CITP, CISA, CGEIT, CGMA
And Karen Johnston, CIA, CFE, CISA
Our Agenda

• How do you define risk, risk management and internal control?
• How do you go about managing risk?
• What are the pitfalls to effective risk management?
• What is the maturity of your organization’s Risk Management process?
• How can you more effectively leverage Risk Management and Internal Controls?
• How can you be a champion for effective Risk Management?
Today’s Objective

• Enable you to become adept at defining risk and a champion of effective Risk Management in your agency.

• During this conference session, you will:
  – Share your experiences
  – Learn from each other
  – Hear current thinking on Risk Management and Internal Controls
Risks are conditions, impediments or obstacles to the achievement of the agency’s goals or objectives…

Have you established articulated goals, missions or objectives for the agency?

- Risk can be “The effect of uncertainty on (setting and achieving) the organization’s objectives” (ISO 31000)

- Thus, always assess risk in light of (setting and achieving) your organization’s objectives!

No Objectives = No Risk
Events/Impediments

What are they?
How do you identify them?
What are they in relation to your agency?
Can you do anything about them?
RISKS

What are they?
How do you identify them?
Where are they in your agency?
Can you do anything about them?
The Definition of Risk*

**NOUN:** The possibility of suffering harm or loss; danger.

A factor, thing, element, or course involving uncertain danger; a hazard: "the usual risks of the desert: rattlesnakes, the heat, and lack of water" (Frank Clancy).

- The danger or probability of loss to an insurer
- The probability of interruption of service
- The amount that an insurance company stands to lose
- The variability of returns from an investment
- The chance of nonpayment of a debt

One considered with respect to the possibility of loss: a poor risk.

**TRANSITIVE VERB:** risked, risking, risks

To expose to a chance of loss or damage; hazard.

To incur the risk of: His action risked a sharp reprisal.

* - definition from Webster’s Dictionary
The Definition of Risk

- It means different things to meet different objectives:

  It Could be this to Some

  And This to Others
RISKS

Entity level items

Program specific level items

Community involvement
The Levels of Assessment

Entity Level (involves executive management)

**Business Processes**
- Entity level for each subsidiary or division
- All identified financial statement categories
- Capturing details of agency activities
- Examination of financial transactions

**IT Processes**
- General Controls for the IT environment
- Application Controls for all significant financial applications
- Spreadsheets used in financial reporting
RISKS

Entity level items

Threats, vulnerabilities and opportunities that pertain to the agency as a whole.
Risk Concepts

❖ RISKS

Program specific level items

Threats, vulnerabilities and opportunities that pertain to the individual programs and activities of the agency.

These can be very narrowly focused and unique
Group Exercise #1
Group Exercise #1

Write down between 5 and 10 events/items that you feel can affect your agency and place them in the envelopes at your tables.
The safest place for a ship...

... is to stay in the harbor

But that’s not what ships were made for...
… Instead, ships were made to transport people & goods to other destinations…

… And that involves risk…

So, what is risk?
- The ship may not reach its destination.
- Insurance may not cover the loss.

No Objectives = No Risk
Risk Assessment is the basis for determining how risks will be managed.

The Risk Assessment needs to be performed with management in a realistic fashion.
Group Exercise #2
Group Exercise #2

Thinking about your agency, rank the ten items on the lists at your table in order of importance from 1 to 10.

Rank the items individually and do not add any items to the list.
Management should assess how “the nature and characteristics of an entity’s activities” affect the entity’s internal control process and the achievement of its business objectives.

“The five components of an internal control process:
  > Control Environment,
  > Risk Assessment,
  > Control Activities,
  > Information and Communication,
  > Monitoring
are applicable to every entity.”*

* - Committee of Sponsoring Organizations of the Treadway Commission.
2013 COSO Internal Control Framework*

* - Committee of Sponsoring Organizations of the Treadway Commission.
2004 COSO ERM Framework*

* - Committee of Sponsoring Organizations of the Treadway Commission.
COSO ICIF vs. ERM*

* - Committee of Sponsoring Organizations of the Treadway Commission.
Other Control Frameworks

PA Management Directive 325.12 - effective July 1, 2015

PURPOSE -
To establish policy, responsibilities, and procedures for implementing effective internal control systems within commonwealth agencies.

SCOPE -
a. Applies to all departments, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction.
b. Applies to all aspects of an agency’s operations, reporting, and compliance with applicable laws and regulations.

OBJECTIVE -
To adopt and implement the internal control framework outlined in Standards for Internal Control in the Federal Government (Green Book) and ensure agencies use the components, principles, and attributes to design, implement, operate, and assess an effective internal control system. The Federal “Green Book.”
What is the Green Book and how is it used?

**Important facts and concepts related to the Green Book and internal control**

**Internal control and the Green Book**

**What is internal control?**
Internal control is a process used by management to help an entity achieve its objectives.

**How does internal control work?**
- Run its operations efficiently and effectively
- Report reliable information about its operations
- Comply with applicable laws and regulations

**How is the Green Book related to internal control?**
Standards for Internal Control in the Federal Government, known as the Green Book, sets internal control standards for federal entities.

**Principles**
Each of the five components of internal control contains several principles. Principles are the requirements of each component.

**Attributes**
Each principle has important characteristics, called attributes, which explain principles in greater detail.
Other Control Frameworks

Look Familiar?

The standards in the Green Book are organized by the five components of internal control shown in the cube below. The five components apply to staff at all organizational levels and to all categories of objectives.
Other Control Frameworks

• While the PA Management Directive is not specifically aimed at your Agency, it will have an effect.
  – Requires these Agencies to perform a Risk Assessment
  – The Commonwealth Agencies will be looking to document their internal controls and indirectly “trickling down” to their funding recipients
  – They will be using an Internal Control Assessment Template that we will see later on
  – You can “help” them by utilizing the same format they are using
Your operating environment poses specific **risks** to an entity’s objectives, including:

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data.
- Unauthorized changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data.
- Humans
- Changes in regulations
What are the Risks?

How do you begin Event Identification?

Where do the risks occur?
• Globally or locally
• Seasonal or on-going?

An example: Retention and Storage of data
• Where is the data?
• What form is it in?
• Who can access it?
• How long is it being retained?

Another example: Compliance and Regulation
• Are you up to date on the latest regulations?
• Are compliance reports/requirements being met?
• Who is in charge?
## Risk Identification

### Identification and Measurement of Risks

<table>
<thead>
<tr>
<th>Risk #1</th>
<th>Risk #2</th>
<th>Risk #3</th>
<th>Risk #4</th>
<th>Risk #5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>Loss of Data</td>
<td>Culture</td>
<td>Data</td>
<td>Employee Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Breaches</td>
<td></td>
</tr>
</tbody>
</table>
Main Objective of Risk Management

- Is *not* to have effective controls…
- Is *not* to effectively manage risk…

It is to:
- Properly set & achieve your objectives
- Avoid too many surprises along the way
- Identify appropriate risks
- And create sustainable value
Risk Management Maturity Levels

- **Level 1:** Non-existent or ad hoc
  - Crisis management

- **Level 2:** Internal control only
  - Formal internal control, mainly focused on external financial reporting

- **Level 3:** RM/IC as a silo
  - Internal control complemented by risk management but still being seen as separate

- **Level 4:** Integrated RM/IC
  - Risk management, including internal control, integrated in organization’s system of management
Group Exercise #3
Group Exercise #3

What are the pitfalls to effective risk management in your agency?
Serious Risk Management Flaws

• Having a compliance-only mentality
• Treating risk as only negative
• Overly focused on one aspect of the agency’s operations
• Regarding Risk Management as a separate function or stand alone process
• Viewing risk management as predominantly important for operations
• Time
Who is involved in Risk Management?

• **Essentially EVERYONE!**
  
  – All levels within the agency should be incorporated in the Risk Management process during the course of your fiscal year.
Who is involved in Risk Management?

• **How can you do that?**
  
  – Get Organized
    • Scheduled meetings
    • Agendas and To-Do lists
  – Treat the process with Respect
  – Don’t get caught in a rut
  – Always ask “What could go wrong?”
Why Worry About Internal Controls?

Lowe's TV Spot, 'Valspar Reserve Video Call' - iSpot.tv.url
Emerging Trends

- Big Data and Analysis
- 3-D Printing
- Biometrics
- Other Competing Agencies
- Political Climates
- Smart devices (other than phones)
Example Key Priority: Breach Notifications

- What Breach of Data Processes does your Agency have in place?
- Are they well-known?
- How often are they updated?
- Are you insured?
- Who is the “face” of the organization?
- Has your staff been trained?
Understanding Key Priorities: Operations

• What software are you using?
• What changes have taken place in your industry?
• What organizational changes have you experienced?
  • Personnel
  • Technology advancements
  • Third-parties
  • Expansion
• How complex are the transaction flows you use?
• Did you experience any problems or incidents during the year?
• Have you remediated audit findings?
Understanding Key Priorities: IT Hardware

• **Portals**
  - How are you using them?
  - How is access granted and controlled?

• **CyberSecurity**
  - Are you using encryption?
  - Have you performed a vulnerability assessment?
  - Who’s minding the mint?

• **Email**
  - What is being sent?
  - Is a filtering mechanism in place?
  - How are you controlling the other parties?

• **Staff and Client education**
  - Continuous and never too much
Understanding Key Priorities: Vendors

• Who are they and what do they do for the Agency?
• How often do you communicate with them about their viability?
• Do they provide you with any type of assurance report?
• Would you know if they had an incident or were on the verge of folding?
Getting the Risk Assessment Done

Let’s explore how we do this
• What is a Risk Inventory?

Is it Animal?

Is it Mineral?

Is it vegetable?
Building a Risk Inventory

- Why are Risk Inventories Important?
  - Reflect the current control environment
  - Can be used as a roadmap for action
  - Provide good governance
  - Keeps employees aware of themselves and others
Building a Risk Inventory

Do We Really Need One?
Building a Risk Inventory

How Can We Use One Once it is Built?
Building a Risk Inventory

What are the Building Blocks to Formulating a Good Risk Inventory?

Do You want Yours to Look like this?

Or This?
The Components of a Risk Inventory

- Define who the Agency’s stakeholders are
- Interviews of stakeholders
- Compilation and categorization of responses
- Organization and prioritization
- Creation of the inventory
- Refinement of the inventory
The Components of a Risk Inventory

• Interviews of Stakeholders
  – Start at the Top
    • Board of Directors
    • Executive Management
  – Ask the time honored question
    • What keeps you awake at night?
    • Or better yet – When you are alone what worries you about your Agency?
  – Ask open-ended questions (and wait for an answer)
  – To do it thoroughly you need to drill down to the lowest level in the Agency.
Compilation and Categorization of Responses

- Compile the answers and look for common themes.
- Begin to put the responses into Categories such as Operational, Financial, Marketing, etc.
- Review the list with the Key Stakeholders
- Refine it after the secondary review
  - This step may require some follow-up
The Components of a Risk Inventory

Organization and Prioritization

- Building on the Categorization phase, decide how the Agency “views” the risks within departments, types or some other measure.
- Begin to assign a prioritization and likelihood rating to each risk
- Using the prioritization and likelihood rating, generate a “score” for each risk or category of risks.
- Begin to quantify the “scores”
Creating the Risk Inventory

– The format is irrelevant!!
– Make it available to the Key Stakeholders for:
  • Review
  • Additional Input
  • Transparency
– Involve your auditors (internal & external)
– Keep all aspects of the agency in mind
Refinement of the Inventory

– This is not a “Once and Done” exercise
– Determine when you will revisit the process (keep it current)
– Any impactful change will require you to look at the Inventory again:
  • Regulatory changes
  • Operational changes
  • Merges/Divestitures
  • Change in Personnel
Risk Assessment

• Risks are measured against each item:
  – Likelihood
  – Impact
  – Velocity
  – Frequency

RISK RATING TABLE

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPACT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>2</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>3</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>4</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>5</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

H = High Risk
M = Moderate Risk
L = Low Risk
Considerations for Likelihood:

- The surrounding environment
- The operating environment
- History of occurrences
- Social conditions
- Financial conditions

Begin with your instinct and expand from that point
Considerations for Impact:

- The surrounding environment
- The operating environment
- History of occurrences
- Social conditions
- Financial conditions
- Mix of programs (concentrations)
- Recovery period

Begin with your known facts and expand from that point
Considerations for Velocity:

- The operating environment
- Social conditions
- Financial conditions
- World events
- Preparedness

Begin with your current incident plans and expand from that point
Considerations for Frequency:

- History of occurrences
- Social conditions
- Financial conditions
- Incident response plans
- Previous mitigation

Begin with your historical knowledge and expand from that point
Group Exercise #4
Group Exercise #4

Using a blank piece of paper, list your top 10 events, incidents, opportunities or conditions that may affect your agency. (Don’t share – yet!)

You can list more than 10 if you like.
Risk Assessment

- Traditional methods employ scaling (1-5).
- This is very objective and the results reflect the “raters” attitudes, knowledge and impact of the risks in their departments.
Risk Assessment

An optional approach is:

– Creating the risks as a “top-ten” list

– The “raters” list their risks in critical order.

– While objectiveness is still part of the process, each individual has listed “their” risks from the perspective of department and company.

– The “top ten” lists can be compared and contrasted to develop a list for the entire organization.
Group Exercise #5
Group Exercise #5

Taking the lists that you have written (earlier and just now) work in your group and list your top 10 events, incidents, opportunities or conditions that may affect your agency.

You can list more than 10 if you like.
## Key Implementation Factors

<table>
<thead>
<tr>
<th>Kickoff Process:</th>
<th>Risk Identification, Analysis &amp; Prioritization</th>
<th>Validate Risk Assessment &amp; Responses</th>
<th>Risk Inventory Maintenance &amp; Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Executive Endorsement</td>
<td>• Identify risks</td>
<td>• Review and validate risk assessment</td>
<td>• Continuously monitor and assess risks</td>
</tr>
<tr>
<td>• Determine what is right for You / Create the Process</td>
<td>• Evaluate and assess impact and likelihood</td>
<td>• Develop strategy to mitigate /action plan</td>
<td>• Ensure accountability</td>
</tr>
<tr>
<td>• Leverage existing risk functions (i.e., Audits, SSAE16)</td>
<td>• Link to strategic objectives</td>
<td>• Identify &amp; Evaluate response to risks</td>
<td></td>
</tr>
<tr>
<td>• Risk Health Check</td>
<td>• Develop risk inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prioritize key risks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Inventory Implementation Factors

- Build awareness and establish a “risk and control” mindset across the organization.
- Leverage all existing functions and assessments to date (SSAE16, Annual Audit Planning, IT Governance)
- Ensure strategic objectives and goals are aligned within the Risk Inventory process
You should take full benefit of all risk functions and internal assessments previously performed, including:

- **Annual Audit Planning**
  - Includes risks and controls identified across the organization
- **Third-Party Vendors and SSAE 16 Reports**
  - Includes risks and controls related to operations and services provided by outside organizations (i.e., Contractors, etc.)
- **IT Governance**
- **Departmental Function Review**
  - Addresses operational and strategic risks through process improvement
Risk Inventory Implementation Factors

- Success Factors Include:
  - Support from Board and Senior Management
  - Encouraging constructive feedback and open discussions
  - Making it clear who owns the process
  - Risk management is everybody’s job (even if you establish a Risk Committee)
Risk Inventory Implementation Factors

• Additional Success Factors
  – View it as a “Process” - not a “Project”
  – Select the right people and approach
  – Learn from losses and successes
  – Strategize on emerging risks
  – Measure and report progress
## Leveraging Best Practices

<table>
<thead>
<tr>
<th>COSO</th>
<th>Moody’s</th>
<th>A.M. Best</th>
<th>S&amp;P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Environment;</td>
<td>Risk Governance</td>
<td>Culture</td>
<td>Risk Management Culture</td>
</tr>
<tr>
<td>Objective Setting;</td>
<td></td>
<td>• Tone at the Top</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment;</td>
<td></td>
<td>• Risk Management Objectives</td>
<td></td>
</tr>
<tr>
<td>Risk Response</td>
<td></td>
<td>• Roles &amp; Responsibilities</td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td>• Strategic Decision Making Process</td>
<td></td>
</tr>
<tr>
<td>Risk Analysis &amp; Quantification</td>
<td></td>
<td>Identification and Management</td>
<td>Risk Controls</td>
</tr>
<tr>
<td>Risk Infrastructure &amp;</td>
<td></td>
<td>Measurement</td>
<td>Emerging Risk Management</td>
</tr>
<tr>
<td>Intelligence</td>
<td></td>
<td></td>
<td>Strategic Risk Management</td>
</tr>
<tr>
<td>Risk Analysis &amp; Quantification</td>
<td></td>
<td></td>
<td>Risk &amp; Economic Capital Models</td>
</tr>
<tr>
<td>Risk Infrastructure &amp;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intelligence</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Leveraging Best Practices

Risk Governance & Policy

**Business Units**
- Take & Manage risks at a department level

**Risk Management Function**
- Identify, Measure, Aggregate, Monitor & Report

**Internal Audit**
- Validate

**Executive Risk Committee**
- Oversee overall risk profile; set risk appetite; create and adjust strategy based on overall risk

**Board of Directors**
- Approve

Various activities to be undertaken within each area of risk governance
## Example Risk Categories

<table>
<thead>
<tr>
<th>Human Actions</th>
<th>Competitive Pressures</th>
<th>Economic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism</td>
<td>Community Involvement</td>
<td>Inflation</td>
</tr>
<tr>
<td>Regulation</td>
<td>Other Agencies</td>
<td>Interest Rates</td>
</tr>
<tr>
<td>Social Priorities (greening)</td>
<td>Insufficient Insurance Coverage</td>
<td>Loss of Funding</td>
</tr>
<tr>
<td>Workforce Demographics (aging)</td>
<td>Federal Regulations</td>
<td>Increases in Funding</td>
</tr>
<tr>
<td>Labor Supply / Demand</td>
<td>Availability of Qualified Personnel</td>
<td>Corporate Fundamentals</td>
</tr>
<tr>
<td>Error from Insufficient Training / Expertise</td>
<td>Catastrophic Event(s)</td>
<td>Municipal Performance</td>
</tr>
<tr>
<td>Error in processing</td>
<td>Regional / local catastrophe</td>
<td>Taxation Policy</td>
</tr>
<tr>
<td>Organizational influence</td>
<td>Change in Frequency of Events</td>
<td></td>
</tr>
<tr>
<td>Lack of Staff</td>
<td>Loss of Employee(s)</td>
<td></td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>Loss of Key Employee(s)</td>
<td>Cost of Losses</td>
</tr>
<tr>
<td>Unauthorized activities</td>
<td></td>
<td>Change in Litigation</td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Internal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- External</td>
<td>New Risks / Loss mitigation needs identified</td>
<td>Dislocation / Market Disruption</td>
</tr>
<tr>
<td>System Failures</td>
<td>New buyers</td>
<td>New Services and Products</td>
</tr>
<tr>
<td>Processing Systems</td>
<td>New buying pressures</td>
<td>Availability of Return</td>
</tr>
<tr>
<td>Communication Systems</td>
<td>Change in regulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consolidation</td>
<td></td>
</tr>
</tbody>
</table>
## Example – Risk Definitions and Mapping

### Regulatory Risks

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Definition</th>
<th>Events (Scorable)</th>
<th>Ultimate Owner</th>
<th>Operational Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance - Business Conduct Laws/Regulations</td>
<td>The risk of non-compliance with insurance and business conduct laws and regulations that could impair the Agency's ability to do business or affect its business model</td>
<td>Ability to do business is impaired</td>
<td>CFO</td>
<td>VP Finance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fines</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Employment Law (E.G. ERISA, HIPAA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Investment Regulations (E.G. FCPA, AML)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Accounting Regulations (E.G. GAAP &amp; STAT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance - Insurance Regulations</td>
<td>The risk of non-compliance with federal/state and business conduct regulations</td>
<td>Public Censure</td>
<td>General Counsel</td>
<td>VP Regulatory Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Employment Law (E.G. ERISA, HIPAA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Data Breaches</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Example Risk Inventory Matrix

<table>
<thead>
<tr>
<th>Company Process / Business Goal</th>
<th>Operational Risk</th>
<th>Risk Profile</th>
<th>Key Performance Indicators</th>
<th>Risk</th>
<th>Risk Monitoring &amp; Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Loss events; 2. Annual client acceptance process reviews conducted by internal audit; 3. Periodic review of employee portfolios; 4. Periodic awareness training.</td>
<td>Mgmt</td>
<td>Internal Audit Monitoring Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Executive Committee</td>
<td>External Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Senior Executive Committee</td>
<td>Other Exposures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COO / CFO</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COO / CIO</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CFO / COO</td>
<td>N/A</td>
</tr>
<tr>
<td>COSO - Operations:</td>
<td></td>
<td></td>
<td></td>
<td>CFO / COO</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Ensure that significant operational risks are identified and integrated into the risk management & monitoring program. |}

1. Insider Trading
   - 1. Reputational risk exposure;
   - 2. Ability to meet regulatory guidelines;
   - 3. Inadequate documentation of insider training policy.

2. Confidentiality
   - 1. Reputational risk if exposed in the media;
   - 2. Exposing critical client data;
   - 3. IT processes and procedures are not aligned with risk and strategy.

3. Conflicts of Interest
   - 1. Accepting a new engagement where a conflict exists within the organization.
Leveraging Best Practices

- Risk Health Check Example:
  - To what extent is the “culture” supportive of advancing an enterprise view of risk management?
  - How has the significance of risk governance been communicated? (i.e., regular communications and documentation)
  - How comfortable are our people in discussing risk? Are they afraid to raise difficult issues? How quickly do they raise issues?
  - Is risk management built into decisions about capital allocation, acquisition, succession planning, and other strategic initiatives?
  - Would you describe the organization’s approach to risk management as:
    - Reactive to risks that occur
    - Proactive about risk possibilities
Leveraging Best Practices

• Now that you have built the Risk Inventory – What do you do to build a risk response for each one?
  ▫ Risk Responses can be categorized as follows:
    ▫ **Mitigate the risk** – with internal controls and management oversight
    ▫ **Insure the risk** – discuss with insurance brokers and others
    ▫ **Transfer the risk** – develop strategies to move or divert actions to other locations or organizations
    ▫ **Accept the risk** – based on your analysis, decide you can “live” with it
    ▫ **Ignore the risk** – not your best option but you may decide to do this based on your analysis
Internal controls are a process. It is a means to an end, not an end in itself.”

COSO defines internal control as:

“A process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives”.

© Wipfli LLP
“Internal control is **effected by people.** It is not merely policy manuals and forms, but people at every level of an organization.”
Internal control can be expected to provide only *reasonable assurance, not absolute assurance*…”
Internal Control involves methods, policies and procedures adopted by an organization to ensure:

- Safeguarding of information
- Accuracy and reliability of information and financial records
- Promotion of administrative efficiency
- Adherence to Information Security standards
The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data”
What Internal Controls can be designed to do:

- Assist the agency in achieving performance and funding targets.
- Help ensure reliable financial reporting.
- Help ensure compliance with laws and regulations.
- Assist in avoiding damage to the agency’s reputation.
What Internal Controls are NOT designed to do:

- Change poor management.
- Prevent errors in judgment.
- Avoid mistakes or errors.
- Prevent collusion.
- Makeup for a lack of resources.
- Align personnel in positions.
Why Incorporate Internal Controls?

- Growing access to and use of computers
- Growing concern for data security and privacy
- Fosters good processes
- Good people do bad things
Risk Management is not a “One Size Fits All” approach. The key is to remember this is a PROCESS!
## Identified Risks

- Access rights to financial adjustment changes are not restricted.
- Use of paper forms creates duplication of effort.
- Power outages are common in the area.

## Business Process

- Certain office employees can order supplies and receive them.
- The Office Admin prepares a census report and sends it to the billing department.
- Personnel must go home when no power.

## Internal Controls

- Establish access restrictions in the IT system to limit duties.
- Train and permit first-line case workers to enter census data directly in your IT system.
- Look at installing a generator or equipping personnel to work from home.
Taking the Next Steps

Set Expectations:

– Executive endorsement

– Direct reporting is critical

– Leverage existing risk functions

– Develop a risk mindset, starting at the top
Risk Identification:

– In general, there are three kinds of risks your agency faces:
  
  – Risks you know of and are working to resolve (Low Concern)
  
  – Risks you know of and are not yet working to resolve (Medium Concern)
  
  – Risks you are not yet aware of but will find out via complaints, litigation, regulators and/or media attention (High Concern)

– Map risks to agreed-upon categories
Taking the Next Steps

Risk Compilation and Categorization:
– Compile all results of the risk identification process
– Quantification of risk exposure
– Options available:
  – Accept = monitor
  – Mitigate = establish internal controls
  – Insure = institute appropriate coverage
  – Share = partner with someone (e.g. other agencies)
– Link Risk Assessment to the Strategic Objectives
# Impact vs. Probability: Example Agency

<table>
<thead>
<tr>
<th>HIGH IMPACT</th>
<th>PROBABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Medium Risk</strong></td>
<td><strong>High Risk</strong></td>
</tr>
<tr>
<td>✓ Client Loss Risk</td>
<td>✓ Regulatory Violations and Fines</td>
</tr>
<tr>
<td>✓ The Authorization Process</td>
<td>✓ System Outages</td>
</tr>
<tr>
<td><strong>Share</strong></td>
<td><strong>Mitigate &amp; Control</strong></td>
</tr>
<tr>
<td>✓ Loss of Facility</td>
<td></td>
</tr>
<tr>
<td><strong>Low Risk</strong></td>
<td><strong>Medium Risk</strong></td>
</tr>
<tr>
<td>✓ Client Complaints</td>
<td>✓ Accounts Receivable</td>
</tr>
<tr>
<td>✓ Accounts Receivable</td>
<td>✓ Case Management Errors</td>
</tr>
<tr>
<td><strong>Accept</strong></td>
<td><strong>Control</strong></td>
</tr>
</tbody>
</table>
Objectives provide the context for the risk assessment

**Example Objectives**

**Strategic Objectives**
*Increase case closures by 10% over the next 3 years.*

**Supporting Objectives**
*Deploy new line of business by May 20XX.*

**Functional Objectives**
*Improve availability and continuity of IT core software by June 20XX.*

**Risk Management Objectives**
*Maintain break-even results (Billing, collections, etc.)*
Taking the Next Steps

• Establish accountability for risks
• Summarize a Risk Inventory report
• Create risk dashboards for high-level board reporting
• Develop a continuous monitoring program
  • Ensure updates are reflected (i.e., changes in risks, systems or processes)
Taking the Next Steps

The Federal Internal Control Template

## Internal Control Assessment Template for the Fiscal Year Ended June 30, 20xx

- **Agency ______________________**
- **Assessable Unit_____________**
- **Updated 07/18/2016**

<table>
<thead>
<tr>
<th>Control Factor Statement</th>
<th>Control Factor Question</th>
<th>Corrective Action Plan</th>
<th>Responsible Party</th>
<th>Target Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle #1 – Demonstrate Commitment to Integrity and Ethical Values</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Executive management has established a “tone at the top” that has been communicated to and is practiced by executives and management throughout the agency.</td>
<td>Does your Agency/Assessable Unit effectively communicate its Mission, Vision, Goals, and Objectives to all employees? Where are these principles located? How often are these principles reemphasized to the employees (i.e. annually, change of administration)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Management enforces a formal code or codes of conduct communicating appropriate ethical and moral behavioral standards; through policy, training and address unacceptable operational practices and conflicts of interest. Appropriate disciplinary action is taken in response to departures from such. (Management Directive 205.9)</td>
<td>Does your Agency/Assessable Unit maintain a code of conduct and comply with Management Directive 205.9? How is the code of conduct communicated to employees? Where is it maintained? How is it enforced?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle #2 – Exercise Oversight Responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Management has established an oversight body to oversee the implementation and continued monitoring of Green Book (Management Directive 125.12)</td>
<td>Has your Agency/Assessable Unit established an oversight body to oversee the implementation and continued monitoring of Green Book? If yes, who is on the oversight body?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 The oversight body oversees management’s design, implementation, and operation of the agency’s internal control system.</td>
<td>Does the oversight body oversee management’s design, implementation, and operation of the internal control system? How often do they meet to review and discuss the internal controls?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Taking the Next Steps

In Summary:

- Be brutally honest with your self assessment
- Select the right people and approach
- Encourage constructive feedback
- Make it clear who owns the process
- Risk management is everybody’s job
- Learn from losses
- Ask for help if you need it
Top Things you should do next

When you return, begin your process and ask:

1. Who are our stakeholders?
2. What are our objectives and goals?
3. Have we started any type of risk assessment activities?
4. How do we get the right personnel involved?
5. What can we do right away?
6. Do we need help?
7. What involvement does the Board desire?
8. What are your responsibilities to outside parties?
9. How do we manage third-parties?
Contact Information

Torpey White, CPA/CITP, CISA, CGEIT  
Wipfli LLP  
Three Logan Square  
1717 Arch Street, Suite 750  
Philadelphia, PA 19103  
610-368-7337 (cell)  
twhite@wipfli.com

Karen Johnston, CIA, CFE, CISA  
Wipfli LLP  
Three Logan Square  
1717 Arch Street, Suite 750  
Philadelphia, PA 19103  
610-220-8154 (cell)  
kjohnston@wipfli.com