Developing a Risk-based Audit Plan

Session 121

May 7, 2012
1:30 – 5:00 pm

Philip E. Flora, CISA, CIA, CCSA, CFE
Principal
FloBiz & Associates, LLC
Phil Flora, CISA, is the principal/managing member for FloBiz & Associates LLC, a company that provides training, internal audit and consulting services. He was the chief audit executive (CAE) at a not-for-profit public corporation for over 16 years. His experience includes banking, public accounting and cost accounting. He also has over 30 years of auditing/management experience.

In his 16 years as the CAE for Texas Guaranteed Student Loan Corporation (TG) Flora was responsible for the maintenance/development of the internal audit function that included leadership, risk assessment/audit planning, communication with management/board, staff hiring/development and other administrative/operational activities. He transformed the function to enable audit coverage of the total organization. In cooperation with two other CAE’s he developed an internal audit leadership development program that assisted in the development of over 30 future audit leaders.
Session Objectives

• Identify standards related to risk assessment and audit planning

• Provide risk management framework examples for application/use in identifying organizational risks

• Determine ways that COBIT and Risk IT can be used to facilitate the risk assessment process
Session Objectives (Continued)

• Identify challenges & opportunities in the information gathering process

• Provide risk assessment/audit planning process/steps for the total audit universe

• Determine methods/approaches to communicate audit planning process results for review/approval

• Provide reference materials for future use
Today's Environment

Global Financial Challenges

Organizations asked to do More with Less!
High Unemployment
Information Security & Privacy continue as a focus
Should the Audit focus change from Compliance to Strategic Risks?

Control Changes to meet Business needs
Audit/IT Audit Role expanding
Ethical Environment Is a Must!

Risk Management Critical to Success
Pressures to meet Performance Expectations

© 2012 ISACA. All Rights Reserved
Follow us @ISACA News #NACACS

© FloBiz & Associates, LLC
Risk

What is it?
Risk

What Does it Look Like?
Risk

How do you Deal with It?
What is Your Organization’s Risk Appetite?
Risk Information Gathering

How much is enough information?
Risk Assessment Input

How can I get your input?

Training, Awareness, Relationships & Tone at the Top!
Information Gathering

Interviews

Open-Ended, Closed-Ended, Time Boxed, Leading?
Listening

It’s hard to learn while you are talking.

Unknown
Nuggets of Gold

What are they?  How do you get them?
Building Relationships

Gathering Valuable Risk Information!

We Appreciate Your Business!
Potential Risk Treatments

- **Risk Avoidance** - Includes not performing an activity that could carry risk.
- **Risk Mitigation/Reduction** - Involves methods that reduce the severity of the loss.
- **Risk Acceptance/Retention** - Involves accepting the loss when it occurs.
- **Risk Transfer** - Means causing another party to accept the risk, typically by *contract* or by *hedging*.

*Source: Wikipedia, the free encyclopedia*
Risk Assessment Process

Plan

Analysis

Support

Input

Understanding

Risk

Technical

Business
Audit Plan (Engagement)
1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.

Scope Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work.
2. A high-level description of the audit work to be performed in a certain period of time.

Source: ISACA Glossary – Knowledge Center
Annual Audit Plan

The plan that is developed annually (possibly updated more frequently based on significant business/organizational conditions). It is reviewed/discussed with Executive Management and approved by the Audit Committee/Board of Directors. The plan is based on the results of the annual Internal Audit risk assessment and the audit resources available (that includes co-sourcing or outsourcing) based on IA expertise and primary risks.
Risk

The combination of the probability of an event and its consequence. (ISO/IEC 73).

Source: ISACA Glossary – Knowledge Center

• Consider the Probability & Impact
Risk - Defined

• A probability or threat of a damage, injury, liability, loss or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through preemptive action.

Source: [http://www.businessdictionary.com/definition/risk.html](http://www.businessdictionary.com/definition/risk.html)
• Risk - The effect of uncertainty on objectives.

• Assurance – A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk.

Source: ISO 31000:2009
Risk Assessment
A process used to identify and evaluate risk and its potential effects.

**Scope Notes:** Includes assessing the critical functions necessary for an enterprise to continue business operations, defining the controls in place to reduce enterprise exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

*Source: ISACA Glossary – Knowledge Center*
Definitions (Continued)

Risk Culture
The set of shared values and beliefs that governs attitudes toward risk-taking, care and integrity, and determines how openly risk and losses are reported and discussed.

Risk Appetite
The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.

Source: ISACA Glossary – Knowledge Center
Risk Management
The coordinated activities to direct and control an enterprise with regard to risk. In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002).

Source: ISACA Glossary – Knowledge Center
Risk/Change - Quote

“Never be afraid to try, remember... Amateurs built the ark Professionals built the Titanic.”

---Unknown
• Enterprise Risk Management (ERM) – ERM is a term in common use. COSO has defined it as: ‘a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Source: ERM COSO - 2004
Risk Factor
A condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios.

Residual risk
The remaining risk after management has implemented a risk response (e.g. control applied).

Source: ISACA Glossary – Knowledge Center
Definitions (Continued)

Risk Analysis
1. A process by which frequency and magnitude of IT risk scenarios are estimated.

2. The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.

Scope Notes: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.

Source: ISACA Glossary – Knowledge Center
Definitions (Continued)

Risk Indicator
A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.

Risk tolerance
The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives.

Source: ISACA Glossary – Knowledge Center
Definitions (Continued)

Threat
Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.

Scope Notes: A potential cause of an unwanted incident (ISO/IEC 13335)

Vulnerability
A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Source: ISACA Glossary – Knowledge Center
COBIT
A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. COBIT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices.

Source: ISACA Glossary – Knowledge Center
Standards – Risk Related

• ISACA
  ➢ S4 – Competence
  ➢ S5 – Planning (Risk-based)
  ➢ S6 – Performance of Audit Work
  ➢ S7 - Reporting

Source: ISACA® - IT Audit & Assurance Standards, Guidelines, & Tools/Techniques
Standards/Guidelines (Continued)

- S9 – Irregularities & Illegal Acts
- S10 - IT Governance
- S11 - Use of Risk Assessment in Audit Planning
- S15 - IT Controls

Guidelines
- G2 - Audit Evidence Requirements
- G3 – Use of Computer Assisted Audit Techniques (CAATS)

Source: ISACA®
Standards/Guidelines (Continued)

ISACA

- G4 – Outsourcing of IS Activities to Other Organisations
- G6 – Materiality Concepts for Auditing Information Systems
- G8 – Audit Documentation
- G9 – Audit Considerations for Irregularities & Illegal Acts

Source: ISACA®
Standards/Guidelines (Continued)

ISACA

- G10 - Audit Sampling
- G11 – Effect of Pervasive IS Controls
- G13 - Use of Risk Assessment in Audit Planning
- G14 – Application Systems Review
- G15 - Audit Planning Revised (Risk based)

Source: ISACA®
ISACA

- G18 - IT Governance
- G20 – Reporting
- G21 – Enterprise Resource Planning (ERP) Systems Review
- G23 – System Development Life Cycle (SDLC) Review Reviews

Source: ISACA®
Standards/Guidance (Continued)

ISACA

- G30 – Competence
- G32 – Business Continuity Plan (BCP) From IT Perspective
- G34 – Responsibility, Authority and Accountability
- G38 - Access Controls

Source: ISACA®
Standards/Guidance (Continued)

ISACA

➢ G39 – IT Organisation
➢ P1 - IS Risk Assessment
➢ P5 - Control Risk Self-assessment

Source: ISACA®
ISACA

- P7 – Irregularities and Illegal Acts
- P8 – Security Assessment - Penetration Testing and Vulnerability Analysis
- P10 – Business Application Change Control

Source: ISACA®
Primary Focus
P1 – IS Risk Assessment Measurement Procedure
This procedure is designed to provide

• A definition of IS audit risk assessment
• Guidance on the use of an IS audit risk assessment methodology for use by internal audit functions
• Guidance on the selection of risk ranking criteria and the use of weightings

Source: ISACA®
Thought for the Day

If it's there and you can see it — it's real.
If it's not there and you can see it — it's virtual.
If it's there and you can't see it — it's transparent.
If it's not there and you can't see it — you erased it!
IIA Standard

• 2000 - Managing the Internal Audit Activity
  – 2010 – Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Source: IIA - International Professional Practices Framework (IPPF)
IIA Standard

• 2000 - Managing the Internal Audit Activity

  The internal audit activity’s plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

Source: IIA - International Professional Practices Framework (IPPF)
IIA Practice Advisory

• 2120-2 – Managing the Risk of the Internal Audit Activity
  - Considerations (not all encompassing)
    • Periodic review of the Audit Universe
    • Periodic review of the Audit Plan
    • Effective planning
    • Relevant risk information is captured & communicated appropriately across the organization

Source: IIA - International Professional Practices Framework (IPPF)
Risk & Consequences

It doesn't work to leap a twenty-foot chasm in two ten-foot jumps.

American Proverb
Frameworks - Examples

COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
Frameworks, Standards & Guidance

Risk IT – Three Domains

Risk Governance
- Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

Risk Evaluation
- Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Risk Response
- Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Business Objectives
- Integrate With ERM
- Establish and Maintain a Common Risk View
- Make Risk-Aware Business Decisions

Risk Management Cycle
- Manage Risk
- React to Events
- Collect Data
- Maintain Risk Profile
- Analyse Risk

Communication

© FloBiz & Associates, LLC

Follow us @ISACANews
#NACACS
Risk IT, Val IT & COBIT®
Has your organization adopted COSO as their risk framework?
Frameworks (Continued)

Global Technology Audit Guides (GTAG 1-16)


Guide to the Assessment of IT Risk (GAIT)


Source: IIA – IPPF – Practice Guides

• Enterprise Architecture Standards (TOGAF) - http://www3.opengroup.org/standards/ea

Frameworks (Continued)

  
- Committee of Sponsoring Organizations (COSO) - http://www.coso.org/guidance.htm
Exercise # 1
Risk Assessment/Audit Planning Process

• Please refer to slides 3 – 86 & 101 - 110 for Exercise 1
• This will be a group exercise with participants working in groups of 4-6
• Upon conclusion of the exercise each group will briefly report out or share our group’s ideas/comments
• Please share your knowledge, experience & ideas
How Can You Use COBIT and Risk IT in the Risk Assessment Process

What are your ideas, approaches & opinions?
Using COBIT & Risk IT

•

•

•

•

•

•
Using COBIT & Risk IT

- 
- 
- 
- 
- 
- 
- 
-
Risk Management Basics

- Common language – Definitions
- Define what is needed for your organization
- Identify who is responsible
Risk Assessment

Art ?  Science ?
Risk Factors (Continued)

• Financial impact – 20%
• Management – 15%
• Audits/Past performance – 13%
• Internal controls – 12%
• Compliance/Regulatory issues – 10%
Risk Factors (Continued)

- Customer service/satisfaction – 10%
- Operational changes/complexity – 5%
- Special requests – 5%
- Public/Customer/Regulator perception – 5%
- Other – 5%
Risk Factors (Continued)

Other Examples

• Environmental factors

• Reporting

• Strategic

• Resource
P1 - IS Risk Measurement Procedure

• Financial Risk

• Strategic Risk

• Operational Risk

• Legal/Compliance Risk

Source: ISACA – IT Audit & Assurance Tools and Techniques
Risk Factors (Continued)

Other Examples

• Reputation
• Fraud
• Social Media
• Outsourcing/Vendor
• Change/Change Management
Risk Factors (Continued)

Other Examples

- _______________________________________
- _______________________________________
- _______________________________________
- _______________________________________

Please share your ideas & experiences!
Risk Quote

Behold the turtle. He makes progress only when he sticks his neck out.”

James Bryant Conant
Educator, diplomat & chemist (1893 – 1978)
Where Do We Go From Here?
Risk Assessment / Management

- Identify & value assets
- Conduct threat assessment
- Perform a vulnerability assessment
- Calculate impact
- Evaluate controls & impact

Source: Wikipedia, the free encyclopedia
Risk Management

Does your organization have a mature risk management process?
Which Animal Poses a Greater Risk?
What to Audit?

Auditable Areas

Audit Universe & Audit Plan

Organization
Risk Assessment
Gathering Information

Where do you go from here?
Audit Planning

- Perform RA
- Gap Analysis
- Annual Plan
- Compile Analyze
- List Audits
Risk Assessment Process to Facilitate Audit Planning

- Identify the timelines and estimated hours/resources to complete
- Establish the risk factors
- Receive input/buy-in from the senior leadership/board
Process (Continued)

• Develop the process
• Establish an audit universe (confirm through input)
• Determine who, how & when input will be requested received
• Identify how the information gathered will be summarized
Analyzing the Risk Data Collected

Combine & Focus

Different People Say the Same Thing Differently!
• Determine the reporting format
• Communicate key aspects of the process to board, management, key staff
• Identify who will gather the information
• Gather risk information (all sources)
• Develop a list of potential audit/review activities (include estimated hours to complete)
Process (Continued)

• Receive input on areas of expertise from IA team members

• Calculate the initial risk rating for each item in the universe

• Perform gap analysis on the universe risk ratings – follow-up on significant items
Process (Continued)

- Compare audit risk assessments results with ERM – follow-up on differences
- Compare/use the risk assessment results in development of the audit plan
- Communicate the risk assessment results in the audit plan
- Gather/update risk information on a continuing basis
Risks are not Always Evident

How to Identify Key Risks?
Awareness, Relationships, Research, Business Acumen!
Who to Survey? Interview?
Overwhelming Information

How to make the information gathered manageable?
Consider Strategic & Reputation risks equally or with greater emphasis than Operational & Compliance risks!
Business Shark

Be Careful of People that Share Info about all other Areas than the one where they have **Responsibility**!
Value of Information
Information

What?  Why?  When?
Tips

Please refer to the handouts identified as Risk Assessment information/examples!
Handouts

Risk Assessment Process
1) Risk Assessment/Audit Planning Schedule
2) Risk Assessment Overview
3) Risk Assessment – Risk Factors
4) Risk Assessment Audit Committee/Board of Directors Input Letter Request
Risk Assessment Process

5) Risk Assessment Input Form - Board

6) Risk Assessment Management/Staff Input Letter Request

7) Risk Assessment Input Form – Management
Exercise # 2
Risk Assessment/Information Gathering

• Please refer to slides 3 – 86 & 101 - 110 for Exercise 2

• This will be a group exercise with participants working in groups of 4-6

• Upon conclusion of the exercise each group will briefly report out or share our group’s ideas/comments

• Please share your knowledge, experience & ideas
Preparation

Involve the audit team as much as possible to increase the plan quality input & promote buy-in!
Annual Audit Plan

• Team based development
• Addresses the top areas in the risk universe
• Objective
• Subjective
• Fluid
If you feel comfortable about the risk assessment and audit plan you probably don’t have enough information – please remember this is not an exact science!
Changing Audit Universe

• What changes have you made to your audit universe? Has your approach changed?

• Has the number of auditable areas in your universe increased, decreased or stayed the same over the last 3 years?

• How do you use your organization's Enterprise Risk Management (ERM) and Business Impact Analysis (BIA) information in relation to annual audit planning?
Risk-Based Auditing

• What percent of your audits are risk-based assurance audits?
• Consulting engagements?
• Management requests?
• Board/Audit Committee requests?
• Do you perform the same audit(s) each year no matter the results during the prior audit?
Risk Assessment

• How do you gather information? What is your process?

• Who do you receive input from during your annual risk assessment process?

• What percent of your audit universe/auditable areas are covered in your audit plan?
Audit Planning

- What process do you follow to condense the risk assessment input and map it to a specific audit areas?
- Do you establish budgeted hours for each IT audit during the development of the annual audit plan?
- Do you provide a list of potential audits/contingency audits with the proposed IT audit plan?
Audit Services

What audit services do you provide?
Audit Services

• Assurance Engagements
• Consulting/Advisory Engagements
• Special Projects
• Evaluation Teams (without decision-making responsibilities)
• Project Team/Board (ex officio)
• General Training/Awareness Activities
Audit Services - Other

- 
- 
- 
- 
- 
- 
- 
- 
- 
-
Tips/Lessons Learned

- KISS (Simple)
- Time box the gathering process
- Remember the risk assessment contributes to the audit process it is not the end result
- Develop relationships to improve input
Tips (Continued)

• Have the total team participate
• Revise the process to improve the input/quality of information received
• Be persistent
• Gather info whenever/wherever it is provided/available
• Remember this is Internal Audit’s risk assessment based on all relevant info available
Tips (Continued)

• Provide awareness/explain the process when opportunities arise
• Make the process a win-win
• Make small improvements annually unless the process has significant identified flaws
• Provide information/awareness & gather information throughout the year (e.g. include on the IA website)
Tips (Continued)

• Receive input from all levels of the organization

• Use a simple numbering process

• Include future programs, initiatives, issues

• Communicate how audit universe coverage will be accomplished without audits planned
• Benchmark/compare the process with other like entities for improvement

• Maintain the confidentiality of input, if possible
Tips Information Gathering

• Business Impact Analysis
• GLB Privacy Risk Assessment
• Trade Publications
• Facilitated Sessions
Tips – Gathering (Continued)

• PEST Analysis
  — Political
  — Economic
  — Social
  — Technological
Tips – Gathering (Continued)

• Brainstorming (Other Critical Thinking Techniques)
  – Internal Audit Team
  – Business Partners
  – Key Stakeholders
  – Peers
  – Industry groups
Tips – Gathering (Continued)

• Strategic Planning
• Competitors
• Turnover
• Legislation
• IT Research Firms (e.g. Gartner, Forrester, McKinsey & Company, Deloitte, Accenture, etc.)
Tips – Gathering (Continued)

• SWOT
  – Strengths
  – Weaknesses
  – Opportunities
  – Threats
Sample – Audit Plan Narrative

Please see Handout #8
Most Important Tip

Under promise and over deliver!
Exercise # 3
Audit Planning Process - Optional

• Please refer to slides 3 – 89 & (91 – 111 focus) for Exercise 3

• This will be a group exercise with participants working in groups of 4-6

• Upon conclusion of the exercise each group will briefly report out or share our group’s ideas/comments

• Please share your knowledge, experience & ideas
How Audit Can Help With ERM?

• Serve as an advocate for risk management
• Share information on organizational risks
• Provide input as a process is established
Help with ERM (Continued)

- Assist with benchmarking & providing reference materials
- Participate in organizational awareness/training for risk identification/reduction
- Review the risk management/ERM process
- Determine ERM is maintained as per policies/procedures
Help with ERM (Continued)

- Audit/validate risk results for reasonableness
- Review the risk response activities to determine that they have the desired impact to reduce risk
- Determine that risk results are appropriately reported (Executive Management & Board)
Something to Consider!

It is all right to forget your mistakes.

If you remember their lessons.

Anonymous
Audit Program
Risk Management

Objective/Scope

- Insurance
- Health & Safety
- Regulatory
- Business Continuity Planning
- Risk Management/Enterprise Risk Management
- Information Security
- Training/Awareness
Audit Program/Steps (Continued)

• Planning identify primary risks
• Identify, review & summarize primary organizational information
  – Corporate policies/procedures
  – Status reporting
  – Performance measures
  – Strategic planning information
  – Insurance policies/coverage
  – Human resource policies
  – Health & safety information
  – Training & awareness information
Audit Program/Steps (Continued)

• Identify, review & summarize primary organizational information
  – Information security
  – Privacy
  – Communication/reputation
  – Other

• Identify who to interview

• Identify who to survey
• Potential interview/survey questions
  – What do you see as the top (2-5) organizational risks over the next 1-3 years
  – Identify primary (2-5) risk management activities you see occurring
  – Strengths related to risk management
  – Opportunities for improvement
  – How is risk management success measured within the organization
Audit Program/Steps (Continued)

- Identify the primary organizational risk management processes
- Receive a walk-through for 3-5 of the primary risk management processes
- Flowchart the processes flowcharted
- List the primary controls
Audit Program/Steps (Continued)

• Test (2-5) of the primary controls
• Document the testwork methodology
  – List test objective/purpose
  – Identify the test population
  – Select the sample method
  – Identify the test steps
  – Extend testwork if necessary
  – Conclude on the testwork results
Audit Program/Steps (Continued)

• Testwork - Potential Test Areas
  – Insurance
  – Training & awareness
  – Reporting
  – Identification/monitoring of high risk areas
  – Ethics/governance
  – Other
Audit Program/Steps (Continued)

• Perform benchmarking/leading practices research & analysis
  – Identify resources/reference materials
  – Develop schedule of common best practices for inclusion in the report as an appendix
  – Compare benchmarking results with the information review & testwork results
Reference Materials

Please see the separate handout!
Questions & Contact Information

Phil Flora
phil@flobizllc.com
(512) 963-4954 - Mobile
Thank you!
Collaborate – Contribute – Connect

- www.isaca.org/knowledge-center

- The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!