Assessing & Managing IT Risk

ISACA Pittsburgh Chapter Meeting

October 18, 2010
Agenda

• Introductions
• IT Risk Assessment – An Approach That Makes Sense to IT
• Measuring Risk – Determining Results
• Audit Planning – Getting the Biggest Bang for Your Buck
• Global Technology Audit Guide (GTAG) – Developing the IT Audit Plan
“Auditing IT processes and activities within the organization is among the highest priorities for today’s Internal Audit Departments, particularly given IT’s purpose as a critical enabler of virtually all business functions.”

- Protiviti’s 2010 IA Capabilities & Needs Survey
The Protiviti Governance Model

- The Protiviti Governance Model to the left depicts our perspective on the elements of IT Governance, Service Delivery and Risk Management.

- It is important to remember that IT Governance and Risk Management are only one component of the IT Governance process.

- Managing Risks while also improving IT Processes has a direct benefit on IT’s ability to effectively deliver service to its end users.

- Groups responsible for IT Risk Management and IT Service Delivery should work in concert to identify improvement initiatives that addresses risk, improves process efficiency, and provides benefit to end users.

- Work to closely align these two areas to help ensure:
  - Risk Management activities are inline with the organization’s risk tolerance.
  - Risk and Control considerations are incorporated in process design and execution.
  - Remediation and continuous improvement activities consider the impacts to IT’s ability to deliver services to their users.
Risk Management Basics

• Risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

• The goals of a Risk Management framework:
  – Dimension risk exposure (quantitative and qualitative) to enable management to confirm an acceptable level of risk
  – Ensure adequate controls, maintain exposure and losses within acceptable levels
  – Determine the appropriate level of capital to absorb extreme losses associated with risks that do not lend themselves to controls.
Risk Management and COSO

Risk Management encompasses:

- **Aligning risk appetite and strategy** – Management considers the entity’s risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

- **Enhancing risk response decisions** – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

- **Reducing operational surprises and losses** – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

- **Identifying and managing multiple and cross-enterprise risks** – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

- **Seizing opportunities** – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

- **Improving deployment of capital** – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

Copyright © 2004 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
IT Governance vs. Compliance

Productivity

IT Governance
“Do it right”

Strategy

Value Defining
Policy

IT Processes
• Val IT
• ITIL
• ISO
• Best Practices

“Do it better”
Performance

Value Adding
Process

Risk Management
• CobiT
• Operation Risk Mgmt
• IT Security
• IT Risk Mgmt

“Do it to protect”
Mitigation

Value Preserving
Control Objectives (statements)

Compliance
• Sox
• Banking Regs
• National Regs
• Other Regs

“Do it or else”
Check & Balance

Transparency
Controls Practices

Reporting & Metrics
Regulation
Industry Best Practice

Corporate Governance

Projected Risk

Risk & Control
Self – Assessment/Risk Scenario Analysis

Key Performance Indicators / Loss Events

Realized Risk

Audit

Independent view of risks / verification
“Risk Knowledgebase” characteristics

This recommended approach provides a consistent model for measuring risk materiality by enhancing management’s “business risk experience.”

Characteristics: Driven by quantitative and qualitative major risk elements, “Risk Knowledgebase”, to derive a position using a flexible weighting approach.

– Data driven - Actual Performance:
  • KRI, KPI’s
  • internal and external loss events

– Management Driven – Projected Performance:
  • Self-Assessment
  • Risks Scenario Analysis and management judgment

– Audit focused – Perceived & independent view of performance:
  • Audit rating rational,
  • Control environment
  • Self Assessment scores
Typical Approach: Understanding the Measurement Trap

Most risk assessment processes attempt to summarize the risk associated with a project as a single, average result. However, our proposed approach discusses risks using a heat map, and does not produce an average risk score. Why is that important? As data rolls up to the executive level, the danger is that the average does not tell the whole story…

- The overall average risk is of little use, it is the distribution of the individual risks and their interpretation that matters
- Human input is required to make sure that true risks are NOT being averaged out of the equation
- Risk management is about the distribution of risk
- Good governance processes enables risk prevention and preparedness
- The images below show distributions with the same average can have very different risk profiles, ignoring this information could cause management to lose sight of high likelihood / impact risks

![Image of metrics layers diagram]
Risk Appetite

The notion of Risk Appetite resides at the heart of the model whereby businesses and TGRC must agree on thresholds:

– Acceptable loss thresholds, e.g. $ losses, impact on revenue, penalties/fines, cost of remediation, or a combination of these. See also note below.

– Impact scale for deriving High, Medium, Low impact.

– Probability scale for deriving High, Medium, Low likelihood.

– Materiality scale for deriving High, Medium, Low materiality based on probability x impact and factoring in acceptable loss appetite.

**Note:** Supported business groups must provide input into the threshold definition and risk appetite. The appetite should be established based on a forward looking 12 month cycle and routinely back tested, validated and adjusted where necessary.
IT Risk Management Framework
(incorporating the triangle approach)

Deficiency Assessment Model

Assess (impact score) the control deficiency vs. each pre-established “important” risk and KPI.

Use the average impact score to derive the “impact rating”, e.g. Low, Medium, High

Assess the likelihood (of adverse event) using quantitative, e.g. status of KRI’s, and qualitative techniques.

Derive the deficiency Risk Rating using the likelihood + impact scores

Risk Assessment Profile

Define the entity

Inventory the core processes, important risks, KPI’s, etc. Perform scenario analysis

Determine weighting factor for each of the probability and impact components

Calculate $ materiality, and using business determined Materiality scale, assign Risk Rating
Key Requirements

Managing risk encompasses four fundamental areas. A successful implementation requires each to be defined and executed, in order to ultimately reduce operational exposures and improve controls.

Key Components
- Risk identification
- Tolerance setting
- Policies / Procedures

Key Components
- Data collection activities
- Loss estimation
- Likelihood estimation
- Risk Assessments, including Control Self-Assessments
- Incident reporting
- Scorecards

Key Components
- Risk monitoring
- Training
- Model and KRI (Key Risk Indicator) Validation activities
- Alert responses on tolerance triggers
- Remediation plans
- Training

Key Components
- KRI Reporting
- Audit findings tracker
- Committees and Governance structure/roles & responsibilities
- Common Org Structure & Methodology
Goals of IT Risk Assessment and Management

• Accurate view on current and near-future IT-related events
• End-to-end guidance on how to manage IT-related risks
• Understanding of how to capitalize on the investment made in an IT internal control system already in place
• Integration with the overall risk and compliance structures within the enterprise
• Common language to help manage the relationships
• Promotion of risk ownership throughout the organization
• Complete risk profile to better understand risk
IT Risk Assessment

An Approach That Makes Sense to IT
How does your organization define its IT Audit Universe?

How do you define General Computer Controls?
Who should be involved in the Risk Assessment Process?

How frequently should IT Risk be assessed or reviewed?
IT Risk Assessment Approach for Internal Audit

Identify Objectives, Resources, and Processes

Identify Business Objectives

Identify and Prioritize IT Objectives

Identify IT Risks Through Facilitated Interviews and Our Client Experiences

Identify IT Resources and Map to IT Objectives

Identify Threats and Risks

Identify Risks Related to IT Objectives

Identify Risks Related to IT Resources

Assess Risks

Assess/Prioritize Risks Related to IT Objectives

Assess/Prioritize Risks Related to IT Resources

Prioritize Processes Based on Risk/Proposed Three Year Audit Plan

Proposed Year One IT Audit Plan

IT Processes/Risk/Resource Map

Key

Interactions with Business Owners

Interactions with IT Leadership
IT Risk Assessment Approach for the IT Department

Protiviti has developed a standard approach to IT Governance and Risk Management. The approach is structured around our Risk and Control framework, depicted below. This framework provides a diagrammatic overview of the four key areas of an effective risk and control management program, namely Policy Definition & Governance, Process & Control, Training & Communication and the Toolkit.
Areas to Assess Risk

- Applied Technology
- IT Processes
- IT Projects
Collaborative Risk Assessments

Benefits of Collaborative Risk Discussions

A collaborative risk assessment process between IT and Business sponsors or other stakeholders and personnel knowledgeable about each impacted area has both intended (direct) and unintended (indirect) benefits:

**Direct**
- Aids in the comprehensive identification and prioritization of overall business environment risks
- Aligns both IT and the business to potential risks and serves to foster commitment to risk mitigation through consensus
- Builds a risk model via collective organizational knowledge of business and technology components
- Maximizes the participation of all stakeholders in the process
- Calls attention to and clarifies the different perspectives regarding technology and business risk
- Can increase effectiveness of group decision-making as risk assessments are consistently repeated

**Indirect**
- Brings to the surface sensitive issues through honest and candid discussion between IT and the Business
- Potentially can identify unanticipated opportunities
- Builds productive relationships and goodwill between IT and the Business
- Helps to identify the commonality of opportunities and risks among different Business areas
- Helps instill the idea of technology solutions that support processes rather than individual applications and infrastructure
- Helps technology-focused personnel develop creative and effective tactics for business problem solving
Measuring Risk

Determining Results
How do you measure and rank risk?
Measuring Risk in an IT Risk Area

What is Included in this Risk Area?
- Applications
- Databases
- Operating Systems
- Infrastructure components

Risk Areas to Assess:
- Stability
- Integrity
- Sensitivity
- Complexity
- Financial Exposure
- Business Risk Evaluation criteria
Measuring Risk in an IT Risk Area

What is Included in this Risk Area?
- Processes that enable IT to deliver service to its end users
- Based on existing frameworks like COBIT, ITIL, ISO

Risk Areas to Assess:
- Reliability and Efficiency
- Consistency
- Technology Leverage
- Results Management
- Human Capital
- Complexity
- Business Risk Evaluation criteria
Protiviti’s Technology Risk Model SM
Measuring Risk in an IT Risk Area

What is Included in this Risk Area?
- Any in-flight or planned IT project, including new applications, changes to IT processes, other strategic initiatives

Risk Areas to Assess:
- Criticality
- Project Management Experience
- Executive Ownership
- Process and Control Reengineering
- Development Platform
- Custom Programming
- Project Budget
- Business Risk Evaluation criteria
Measuring Risk in an IT Risk Area

All three IT Risk Areas should incorporate an evaluation of Business Risk within each risk area. This risk evaluation should work in conjunction with the IT Risk evaluation criteria to determine the overall risk to the organization.

Risk Areas to Assess:
- Strategic
- Operational
- Legal/Regulatory Compliance
- Financial Reporting
Risk to Service Linkage

Service = Business activity supported by IT

Risk Framework

Level 1 Risk

Level 2 Risk

Level 2 Risk

Level 2 Risk

Application entities

Level 2 Risk

Level 2 Risk

Level 2 Risk

Level 2 Risk

Technology entities

Level 2 Risk

Level 2 Risk

Level 2 Risk

Level 2 Risk

Process entities

Level 2 Risk

Level 2 Risk

Level 2 Risk

Level 2 Risk

Third Parties

Application entities

Service 1

Service 2

Service 3

Application 1

Application 2

Application 4

Application 3

Database 1 (SQL)

Database 2 (SQL)

Database 3 (Oracle)

O/S (Windows)

O/S (Unix)

WAN

Data Center 1

Data Center 2

Incident Mgmt

Logical Access Mgmt

Change Mgmt 1

Change Mgmt 2

Capacity Mgmt

Business Cont Mgmt

Third Party 1

Risk to Service Linkage

Business Transparency Reporting/Analysis

Enterprise Risk Management/Operational Risk

CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to any third party.
By aggregating all the risk assessments that support each of the critical services provided to the business, an end to end risk profile can be created.

The end to end profile predicts the affect of all the risks which underpin the delivery of each service. For example, the service may predict 10 “severity one” outages in the coming year due to ineffective risks in change management, networks and database capacity management.

This information can then be used to develop a more transparent discussion around risk the key business stakeholders for that service.
Audit Planning

Getting the Biggest Bang for Your Buck

Powerful Insights.
Proven Delivery.
Developing the Audit Plan

- IT audit plans should be designed based on the assessment of IT risks and exposures
- Changes in management direction, objectives, emphasis, and focus should be reflected in the IT audit plan
- IT audit timing should be based on, among other factors, the levels of inherent risk and exposure
- Budgetary constraints should not impede the ability of internal audit to address risky IT areas
Evaluating Risk

Each risk area is then mapped based on the Impact and Likelihood associated with the specific risk. The risk profile associated with each quadrant of the map is noted below. Risk responses should be developed starting with those risks found in the upper right quadrant.

### High Likelihood

- **Key Risks**
  - Critical risks that potentially threaten the achievement of business objectives or success

- **Secondary Risks**
  - Lower likelihood, but could have significant adverse impact on business objectives

### Low Likelihood

- **Secondary Risks**
  - Lower likelihood, but could have significant adverse impact on business objectives

### High Significance

- **Key Risks**
  - Critical risks that potentially threaten the achievement of business objectives or success

- **Low Priority Risks**
  - Significant monitoring not necessary unless change in classification
  - Periodically reassess

- **Secondary Risks**
  - Lesser significance, but more likely to occur
  - Consider cost/benefit trade-off
  - Reassess often to ensure changing conditions (move to high significance)
Example Inherent Risk Heat Map

## Design Internal Audit Plan

<table>
<thead>
<tr>
<th>Audit</th>
<th>Risks</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>Beyond 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Service Project Controls SME</td>
<td>(5) Complexity / Integrity – SAP, (21) Shared Service Project Risk, (26) Sales Order to Invoice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Privacy Review</td>
<td>(3) Sensitivity / Integrity – Data Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Assessment</td>
<td>(27) Manage Business Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Account Management Review</td>
<td>(13) Manage Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated SAP Audit</td>
<td>(5) Complexity / Integrity – SAP, (26) Sales Order to Invoice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to any third party.
Responding to Identified Risks
Risk Response Definition

- The purpose of defining a risk response is to bring risk in line with the defined risk tolerance for the enterprise after due risk analysis.

- In other words, a response needs to be defined such that future residual risk (current risk with the risk response defined and implemented) is as much as possible (usually depending on budgets available) within risk tolerance limits.
Addressing Identified Risks

Risk Mitigation Strategies

When developing mitigation activities, there are five strategies that can be pursued individually or in tandem.

The right strategies for a given risk will be dependent on the overall risk appetite of that company and its management.

<table>
<thead>
<tr>
<th></th>
<th>AVOID</th>
<th>RETAIN</th>
<th>REDUCE</th>
<th>TRANSFER</th>
<th>EXPLOIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not performing a risky activity</td>
<td>Accepting loss from risk when it occurs</td>
<td>Reduce the severity or likelihood of a loss from risk when it occurs</td>
<td>Moving or spreading loss from risk to other parties when it occurs</td>
<td>Using the (possible) occurrence of a risk to spur beneficial outcomes</td>
</tr>
<tr>
<td></td>
<td>• Clarify requirements</td>
<td>• Develop contingency plan</td>
<td>• Use less complex processes</td>
<td>• Purchase insurance</td>
<td>• Redefine scope</td>
</tr>
<tr>
<td></td>
<td>• Improve communications</td>
<td>• Establish contingency allowance</td>
<td>• Use less innovative technology</td>
<td>• Require performance bonds</td>
<td>• Renegotiate contracts</td>
</tr>
<tr>
<td></td>
<td>• Reduce scope</td>
<td>• Develop prototypes</td>
<td>• Design redundancy into system</td>
<td>• Negotiate fixed price contracts with vendors</td>
<td>• Reorganize project responsibilities</td>
</tr>
</tbody>
</table>
# Addressing Identified Risks

**What to Document**

## Mitigation Activity

The activity that will be undertaken to address the project risk

### Activity Type

**Preventive – Detective – Reactive**

<table>
<thead>
<tr>
<th>Policies &amp; Procedures</th>
<th>Defined Processes</th>
<th>People &amp; Organization</th>
<th>Management Reports</th>
<th>Methodologies</th>
<th>Systems and Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there formal policies and procedures that guide this activity to ensure consistent execution?</td>
<td>Are there well defined processes to guide consistent execution of this activity?</td>
<td>Identify the people responsible for consistent execution of this activity. Do they know that they are responsible? Are they qualified? Do they receive necessary ongoing training?</td>
<td>Are there management reports that are consistently generated that provide the necessary information for management to make decisions regarding the risk/risk activity? Is there a proper forum to discuss these reports?</td>
<td>Are there sufficient methodologies in place to analyze available information accurately?</td>
<td>Are there sufficient systems to capture relevant data to manage this risk/risk activity? Do the systems consistently generate accurate information?</td>
</tr>
</tbody>
</table>

## Previous Lessons Learned

Has the risk been encountered before? Was it successfully mitigated? What worked, what did not?
Risk Management in Practice

Typical Challenges
Risk Management in Practice

Typical Challenges

• IT organizations typically experience issues with risk assessment processes and activities that can be attributed to three core issues:
  – Risk Management Processes and Tools
  – Periodic Review of Project Risk Profiles
  – Risk Assessment during Vendor Selection

• We have identified some key challenges that most organizations seem to struggle with.

• By evaluating these challenges and impacts, we have identified opportunities for project managers to improve both the overall risk assessment process and also some of the tools that help facilitate the process.
Risk Management in Practice

Typical Challenges

• **Processes Do Not Accurately Capture an organization’s Risk Profile**
  
  – **Issues:**
    
    • Risks identified tend to be more technology focused, rather than considering the overall business environment.
    
    • Identified risks are not articulated in business terms
    
    • Risk mitigation strategies are not adequately considered or planned for
  
  – **Impact:**
    
    • Stakeholders lack necessary information to evaluate risk and determine whether to move forward with major initiatives
    
    • Projects are approved without complete understanding and acceptance of risks
    
    • Without mitigation strategies, risks may go unchecked and un-owned, increasing the likelihood that they will occur or worsen

• **Risk Profiles Are Not Periodically Reviewed and Updated**

  – **Issues:**
    
    • Risk identification may be a point-in-time activity and may not be reviewed at periodically
    
    • Processes may not be in place to evaluate and address potential new risks that might occur
Risk Management in Practice

Typical Challenges

• **Project Risk Profiles Are Not Periodically Reviewed and Updated (Continued)**
  - Impact:
    • Stakeholders may not know whether risk profiles have changed, whether mitigation strategies remain valid, and whether new risks surface.
    • Stakeholders may lack a view into how risk profile of one individual project impacts other projects in the portfolio.

• **The Vendor Selection process does not Consistently Anticipate or Manage Risk**
  - Issues:
    • Vendor Selection and management may not be part of the project risk management process.
    • These processes and assessment criteria may not be standardized, consistently followed, and repeatable.
    • Appropriate parties such as Finance, Legal, Procurement personnel may not be engaged during the selection process.
  - Impact:
    • Use of third-parties introduces additional risk at both the project and enterprise level that is not under the direct control of the organization.
What value can be derived from an effective IT Risk Assessment?
Other Risk Assessment & Management Frameworks
Frameworks for IT Risk Assessment & Management

- ISACA’s RiskIT Framework
- IIA’s Global Technology Audit Guides
- ISO Standards 27005 and 31000
- PMI’s Project Management Body of Knowledge (PMBOK)
- Guide to the Assessment of IT General Controls Scope Based on Risk (GAIT)
The Risk IT Framework

Risk IT Includes

• The Risk IT Framework
  – Summary + Core Framework
  – Helps convey the risk landscape and processes and prioritize activities
  – Available as a free download to all

• The Risk IT Practitioner Guide
  – Provides practical guidance on improving risk management activities
  – Available as a free download for ISACA members only

• Both publications are available for purchase in print version
Risk IT

Risk IT is a comprehensive framework for evaluating risks across the IT organization, not just information security. It covers all IT-related risks, including:

– Late project delivery
– Not achieving enough value from IT
– Compliance
– Misalignment
– Obsolete or inflexible IT architecture
– IT service delivery problems
Risk IT Extends COBIT and Val IT

Risk IT complements and extends COBIT and Val IT to make a more complete IT governance guidance resource.
Where Risk IT Fits In

• Standards and frameworks are available, but are either too:
  – Generic enterprise risk management oriented
  – IT security oriented

• No comprehensive IT-related risk framework available (until now)
Risk IT

Guiding Principles of Risk IT

- Always connect to enterprise objectives
- Align the management of IT-related business risk with overall enterprise risk management
- Balance the costs and benefits of managing risk
- Promote fair and open communication of IT risk
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Understand that this is a continuous process and an important part of daily activities
GTAG – Developing the IT Audit Plan

- Supports the approach that we’ve discussed
- Provides additional guidance in the areas of:
  - Understanding the Business
  - Defining the IT Audit Universe
  - Performing the Risk Assessment
  - Formalizing the IT Audit Plan
- Includes hypothetical example for reference

Available for download at
PMI’s Project Management Body of Knowledge

11.1 Risk Management Planning

1. Inputs
   - 1. Enterprise environmental factors
   - 2. Organizational process assets
   - 3. Project scope statement
   - 4. Project management plan

2. Tools and Techniques
   - Planning meetings and analysis

3. Outputs
   - 1. Risk management plan

11.2 Risk Identification

1. Inputs
   - 1. Enterprise environmental factors
   - 2. Organizational process assets
   - 3. Project scope statement
   - 4. Risk management plan
   - 5. Project management plan

2. Tools and Techniques
   - 1. Documentation reviews
   - 2. Information gathering techniques
   - 3. Checklists analysis
   - 4. Assumptions analysis
   - 5. Diagramming techniques

3. Outputs
   - 1. Risk register

11.3 Qualitative Risk Analysis

1. Inputs
   - 1. Organizational process assets
   - 2. Project scope statement
   - 3. Risk-management plan
   - 4. Risk register

2. Tools and Techniques
   - 1. Risk probability and impact assessment
   - 2. Probability and impact matrix
   - 3. Risk data quality assessment
   - 4. Risk categorization
   - 5. Risk urgency assessment

3. Outputs
   - 1. Risk register (updates)

11.4 Quantitative Risk Analysis

1. Inputs
   - 1. Organizational process assets
   - 2. Project scope statement
   - 3. Risk management plan
   - 4. Risk register
   - 5. Project management plan
   - 6. Project schedule management plan
   - 7. Project cost/management plan

2. Tools and Techniques
   - 1. Data gathering and representation techniques
   - 2. Quantitative risk analysis and modeling techniques

3. Outputs
   - 1. Risk register updates

11.5 Risk Response Planning

1. Inputs
   - 1. Risk management plan
   - 2. Risk register

2. Tools and Techniques
   - 1. Strategies to reduce risk or threats
   - 2. Strategies to positive risk opportunities
   - 3. Strategies for both threats and opportunities
   - 4. Contingent response strategy

3. Outputs
   - 1. Risk register (updates)
   - 2. Project management plan (updates)
   - 3. Risk-related contractual agreements

11.6 Risk Monitoring and Control

1. Inputs
   - 1. Risk management plan
   - 2. Risk register
   - 3. Approved change requests
   - 4. Work performance information
   - 5. Performance reports

2. Tools and Techniques
   - 1. Risk reassessment
   - 2. Risk audits
   - 3. Variance and trend analysis
   - 4. Technical performance measurement
   - 5. Reserve analysis
   - 6. Status meetings

3. Outputs
   - 1. Risk register (updates)
   - 2. Requested changes
   - 3. Recommended corrective actions
   - 4. Recommended preventive actions
   - 5. Organizational process assets (updates)
   - 6. Project management plan (updates)

Figure 11-1. Project Risk Management Overview

CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to any third party.
The GAIT Methodology

Guide to the Assessment of IT General Controls Scope Based on Risk (GAIT)

- A series of principles and methodologies for top-down, risk-based scoping of IT general controls

GAIT for IT and Business Risk (GAIT-R)

- Methodology for identifying the key controls essential to achieving business goals and objectives
- Identifies the critical aspects of information technology essential to the management and mitigation of business risk
- Critical IT functionality and its inherent risks should be considered when planning audit work
GAIT - Top-Down, Risk Based Approach

- Identify, understand, and evaluate the effectiveness of company-level controls
- Identify significant accounts and locations and relevant assertions
- Identify significant business processes and major classes of transactions
- Identify the points at which errors or fraud could occur in the process
- Identify controls to test that prevent or detect errors or fraud on a timely basis
- Identify/validate critical IT functionality
- Identify significant applications where ITGC need to be tested
- Identify ITGC process risks and related control objectives
- Identify ITGC to test that meet control objectives
- Perform a “reasonable person” review
GAIT – IT Risk Assessment and Scoping

**STEP 1**
Validate understanding

- Significant accounts
- Business processes
- Business controls
- Applications

**STEP 2**
Perform risk assessment at each layer

**STEP 3**
Conclude: Is it *REASONABLY POSSIBLE* a failure in this IT Process area could impact application controls/IT functionality and result in a material misstatement?

Risk is not eliminated; it is reduced to a REASONABLE level.
Summary

• **IT Risk must**
  – take a complete look at technology across the enterprise
  – be grounded in business risk and business context

• **When you measure IT risk**
  – use quantitative factors in addition to the qualitative measures
  – focus on the maturity of the risk assessment over time
  – involve and educate the IT organization in the risk assessment process

• **Use IT risk to**
  – drive the audit plan
  – enable the entire audit organization to assess risk
For additional information on Protiviti’s approach to assessing and managing IT Risks or to receive a copy of this slide deck, please contact the presentation team:

Timothy Maloney

Protiviti
Risk & Business Consulting.
Internal Audit.

One PPG Place, Suite 2350
Pittsburgh, PA 15222

Direct: 412.402.1720
Mobile: 412.303.6338
Fax: 412.402.1791
Timothy.Maloney@protiviti.com

Darren Jones

Protiviti
Risk & Business Consulting.
Internal Audit.

One PPG Place, Suite 2350
Pittsburgh, PA 15222

Direct: 412.402.1747
Mobile: 412.302.2978
Fax: 412.402.1764
Darren.Jones@protiviti.com

CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to any third party.
Powerful Insights. Proven Delivery.™