

# **ISACA – Chicago Chapter January 13, 2011**

## **IT Risk Assessment**

**John Gatto  
Divisional Vice President  
IT Audit & Advisory Services**

**HCSC  
Chicago, Illinois**

# Learning Objectives

- **To gain an understanding of drivers that are leading companies to improve their risk assessment efforts**
- **To gain an understanding of the risk assessment process, including key takeaways from several authoritative sources**
- **To gain an understanding on how risk assessment can be used in project auditing**

# Risk Definition

**The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets**

**Then you determine the impact**

# Assessment Definition

## Definitions of assessment on the Web:

- **appraisal: the classification of someone or something with respect to its worth**
- **an amount determined as payable; "the assessment for repairs outraged the club's membership"**
- **the market value set on assets**

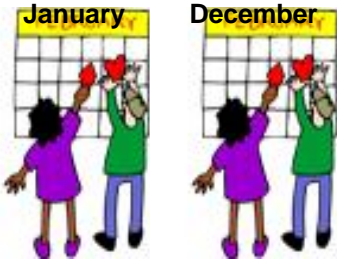
# Risk Assessment

Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard).

*Quantitative risk assessment* requires calculations of two components of risk:  $R$ , the magnitude of the potential loss  $L$ , and the probability  $p$ , that the loss will occur.

# Frequency

Annually



Monthly



Continuously



Daily



# Risk Assessment (RA)

- **IT Organization**
- **Projects**

# The Bigger Picture



**ERM: process applied across all levels of an enterprise designed to identify, prioritize and respond to risks in order to provide reasonable assurance regarding achievement of enterprise objectives.**

**IT: application of the ERM process to IT as the enterprise. It is not limited to technology risks – it looks at all risks that could affect IT's ability to achieve its objectives which are tied to the enterprise objectives.**

# The Need for RA

- **Business world is constantly changing**
- **Shareholders want to know if companies have the correct controls in place**
- **Increased regulatory requirements:**
  - **Sox**
  - **MAR**
  - **Basil**
  - **Anti-Money Laundering (AML)**
  - **Information privacy**

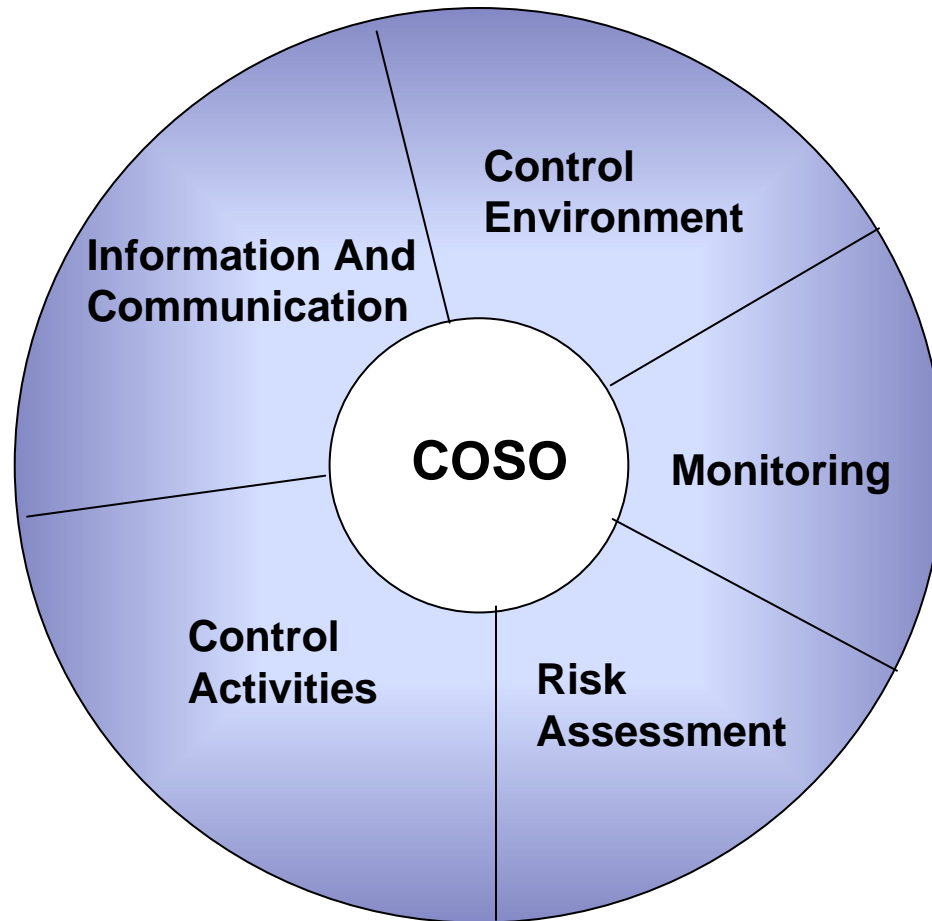
# The Need for RA

- **New systems development**
- **Greater IT exposure / risk of loss**
- **Dependence on telecommunications, Internet, mobile processing, PSD, PCI, etc.**
- **Connectivity ... VPNs and Internet with Suppliers, Customers, Providers**
- **More and smarter hackers with better tools**
- **Corporate espionage**
- **Information terrorism**

# Drivers of RA

- **COSO**
- **IIA**
- **ISACA**
- **Events / Articles / Miscellaneous**

# COSO Model



# IIA

## ▪ **Standard 2120 - Risk Management**

- **The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.**
  
- **Interpretation: Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:**
  - **Organizational objectives support and align with the organization's mission;**
  - **Significant risks are identified and assessed;**
  - **Appropriate risk responses are selected that align risks with the organization's risk appetite; and**
  - **Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.**

# IIA

- **Standard 2120.A1- The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:**
  - **Reliability and integrity of financial and operational information.**
  - **Effectiveness and efficiency of operations and programs;**
  - **Safeguarding of assets; and**
  - **Compliance with laws, regulations, policies, procedures, and contracts.**

# ISACA

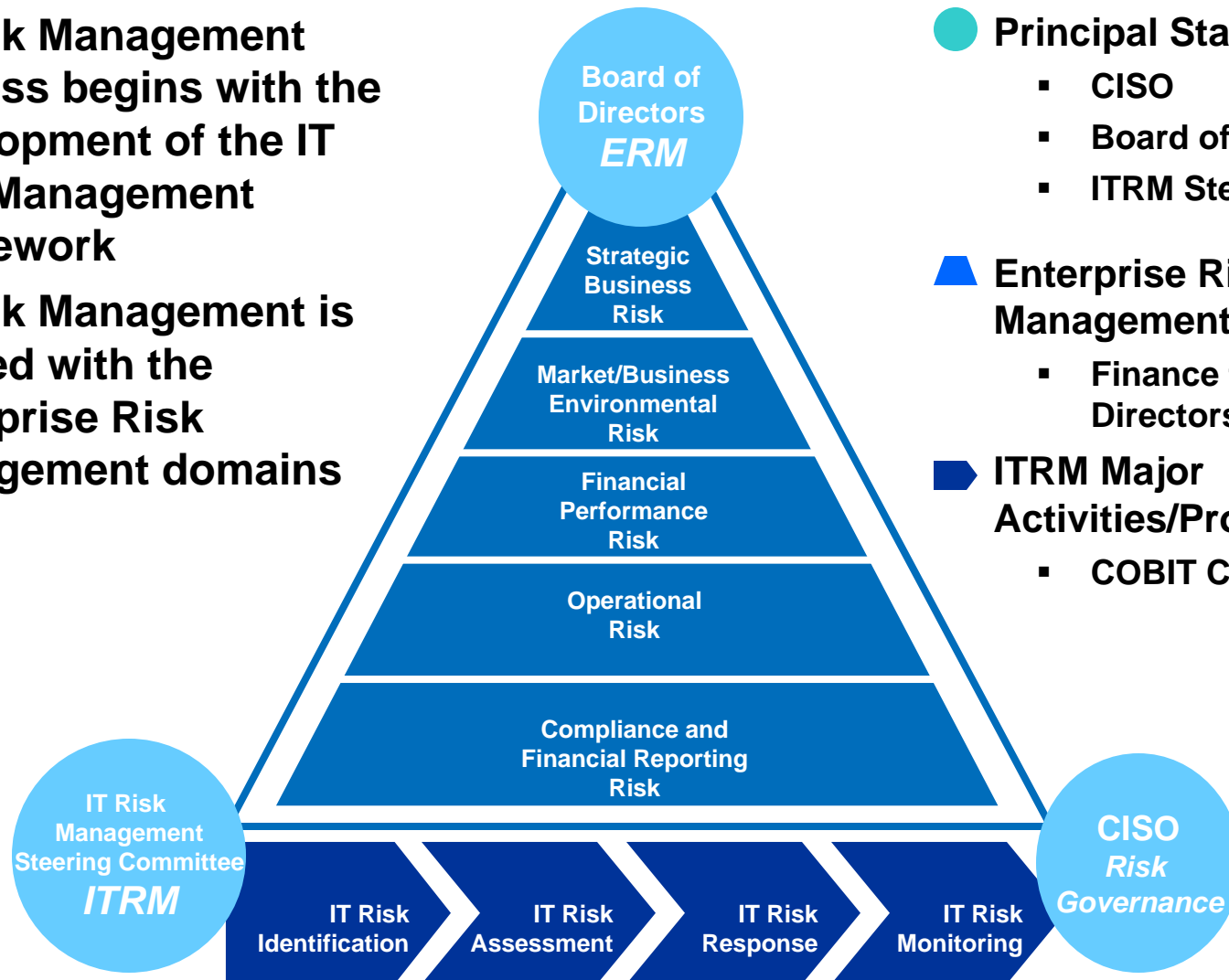
- **CobIT: PO9 Assess and Manage IT Risks**
  
- **Standard S11: Risk assessment is a technique used to examine auditable units in the IS Audit universe and select areas for review to include in the IS annual plan that have the greatest risk exposure.**

# PO9 Assess and Manage IT Risks

- **9.1 IT Risk Management Framework:**
  - **Establish an IT risk management framework that is aligned to the organization's (enterprise's) risk management framework.**
  
- **9.2 Establishment of Risk Context:**
  - **Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes.**
  - **This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.**
  
- **9.3 Event Identification:**
  - **Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects.**
  - **Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.**

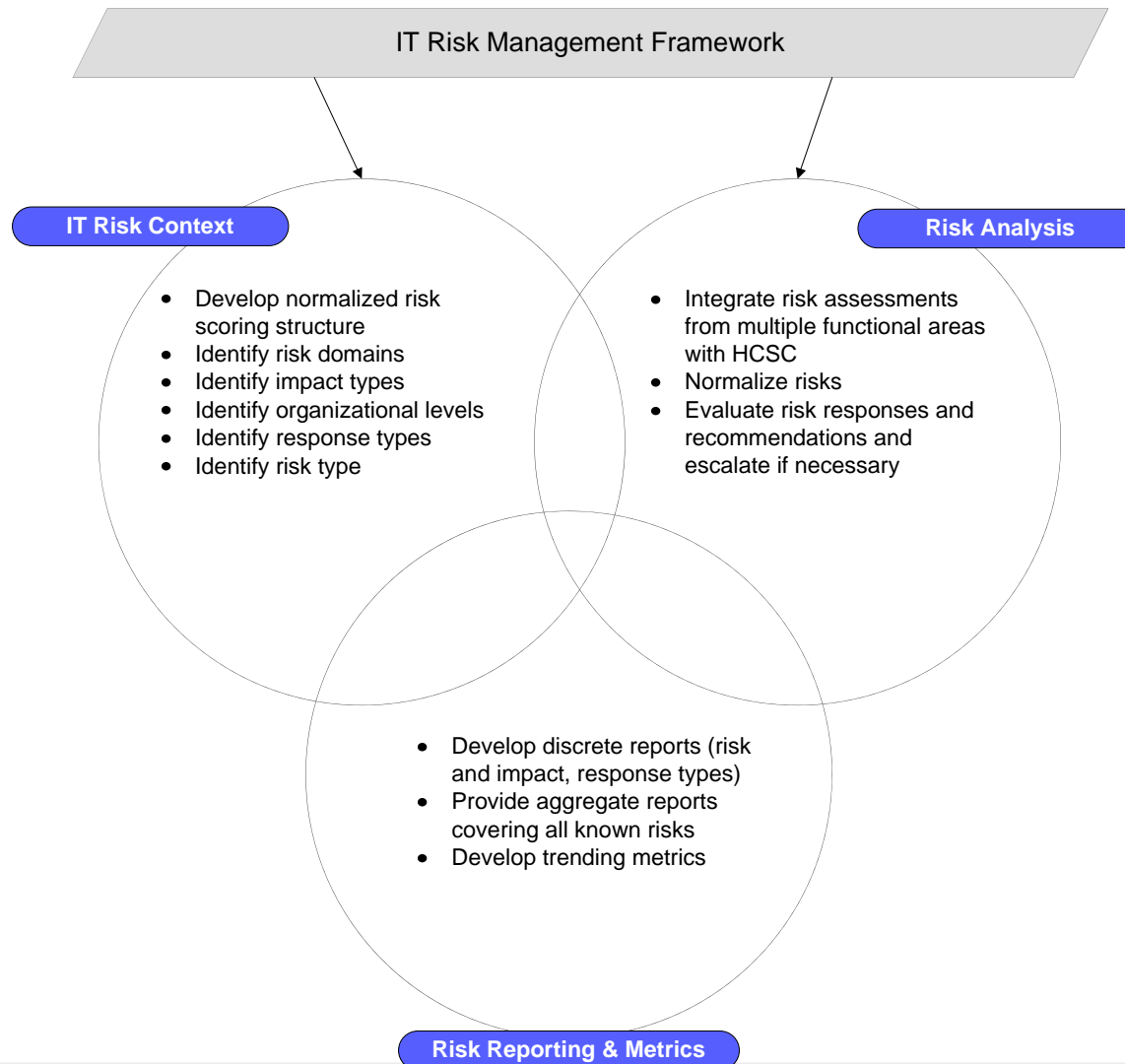
# IT Risk Management (ITRM) Framework

- IT Risk Management process begins with the development of the IT Risk Management Framework
- IT Risk Management is aligned with the Enterprise Risk Management domains



- Principal Stakeholders**
  - CISO
  - Board of Directors
  - ITRM Steering Committee
- Enterprise Risk Management Domains**
  - Finance to Board of Directors
- ITRM Major Activities/Processes**
  - COBIT Control Objectives

# IT Risk Management Process Overview

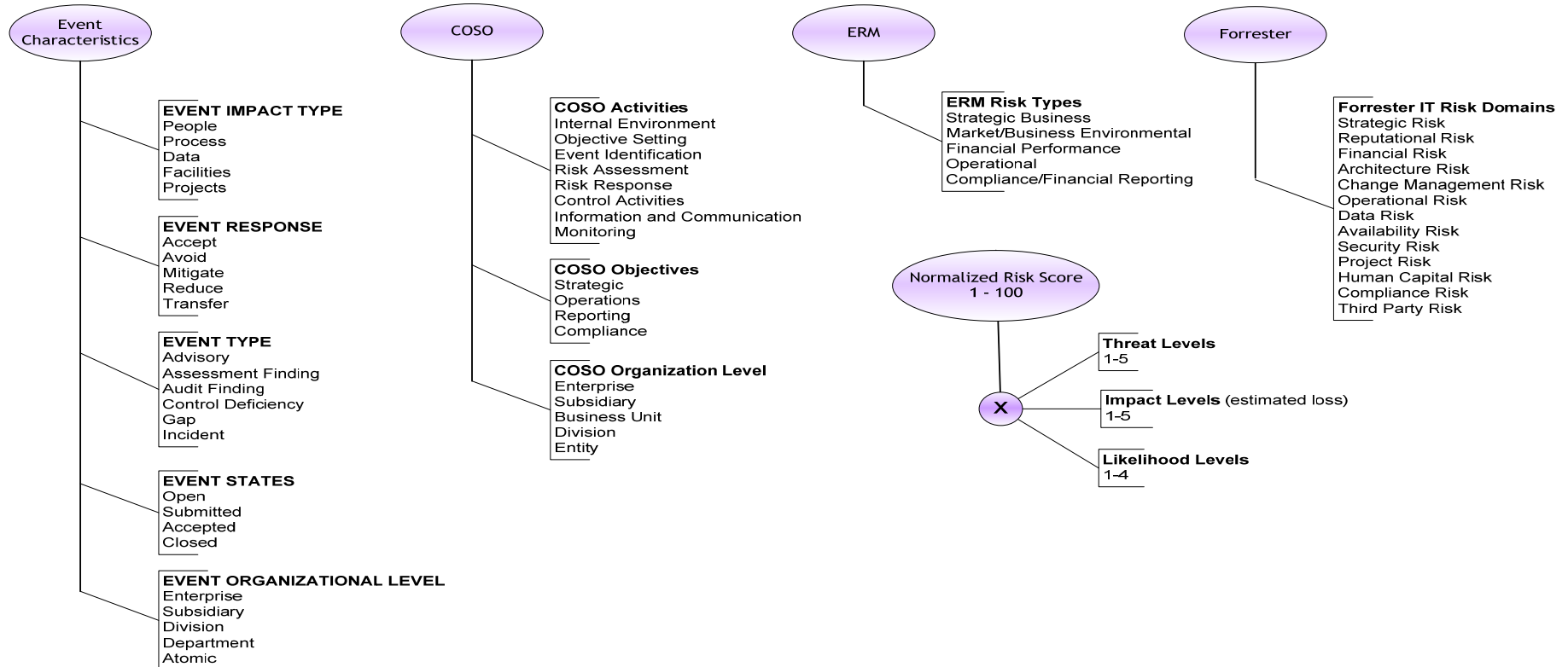


# Risk Analysis

- **ITRM performs analysis on risk assessments conducted throughout IT and business units. A partial list includes:**
  - **Regulatory Assessments**
  - **Security Risk Assessments**
  - **IT Audits**
  - **Internal Control Testing**
  - **Disaster Recovery Tests**
  - **HIPAA Risk Assessments**
  - **External Risk Assessments (i.e. Gartner)**
- **ITRM analyzes each risk using the IT Risk Context and provides a risk score using the normalized risk scoring structure**
- **The Normalized Score combines qualitative assessment of Impact and Likelihood with quantitative scoring to produce a score of 0 to 100**
- **ITRM also evaluates and determines if appropriate responses or recommendations have been provided**

# IT Risk Context

The components of the Risk Context are shown in the diagram below:

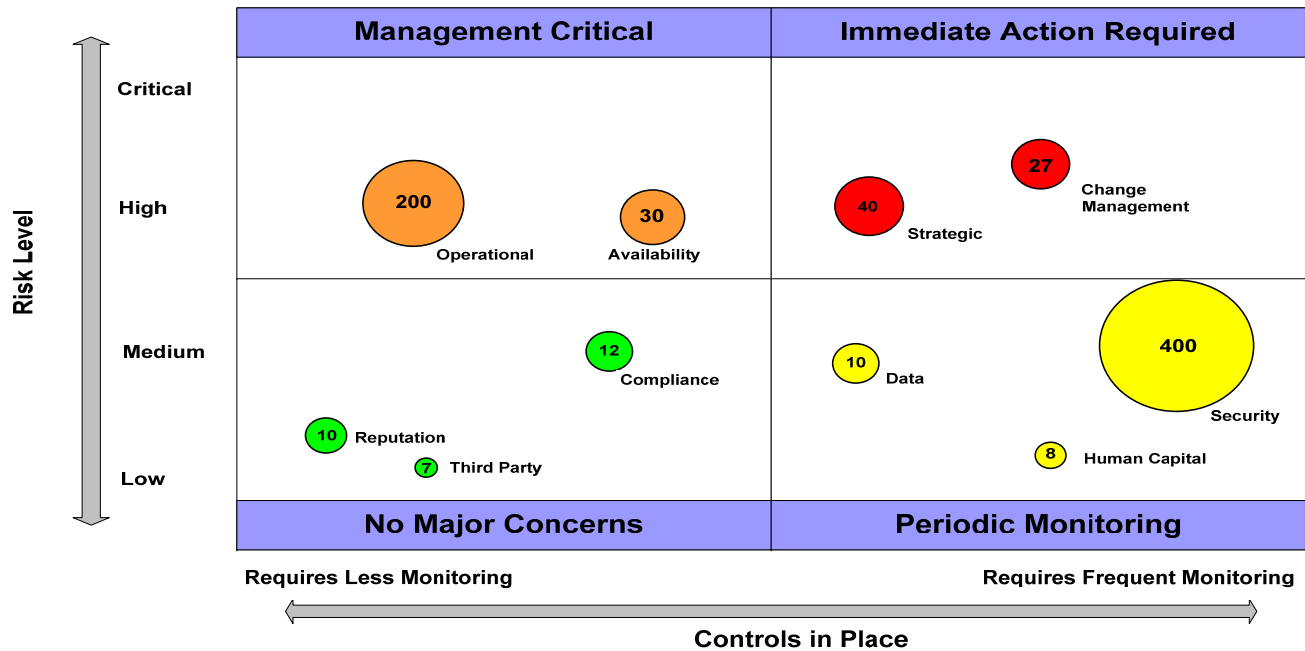


# Risk Reporting & Metrics

- **The final step is the development of reporting and metrics for senior leadership.**
- **IT Risk Management provides sufficient reporting capability in order to assist leadership in making risk aware decisions.**

# Risk Reporting & Metrics

Shown below is an hypothetical risk dashboard :  
**ITRM Risk Dashboard**  
*by Forrester® Risk Domains*



**Legend**

- Low risk domain (Green bubble)
- High risk domain (Orange bubble)
- Medium risk domain (Yellow bubble)
- Critical risk domain (Red bubble)

Velocity (bubble size) = number of risks in domain

**No Major Concerns** = domains in this quadrant contains risk scores 20 and below  
**Periodic Monitoring** = domains in this quadrant contains risk scores between 20 and 40  
**Management Critical** = domains in this quadrant contains risk scores between 40 and 60  
**Immediate Action Required** = domains in this quadrant contains risk scores between 60 and 100

# PO9 Assess and Manage IT Risks

## 9.4 Risk Assessment:

- **Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods.**
- **The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.**

## 9.5 Risk Response:

- **Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis.**
- **The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.**

# PO9 Assess and Manage IT Risks

## 9.6 Maintenance and Monitoring of a Risk Action Plan:

- **Prioritize and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution.**
- **Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s).**
- **Monitor execution of the plans, and report on any deviations to senior management.**

# Drivers of RA

- **COSO**
- **IIA**
- **ISACA**
- **Events / Articles / Miscellaneous**

# ADR 2011 Audit Plan Hot Spots

## RISK AREA

- Cloud Computing
- IT Strategic Planning

## AUDIT PLAN ITEM

- Data encryption Review
- Security Policy review
- IP Protection Assessment
- Third Party Audits
- Strategic Alignment Audit
- Organizational Agility
- Project Health Checks
- Communications Audit

# ADR 2011 Audit Plan Hot Spots

## RISK AREA

- Decentralized IT Models
- Social Media

## AUDIT PLAN ITEM

- Services and Accountability Mapping
- General Controls Review
- Strategic Outlook Review
- Social Media Policy Audit
- High-Risk User Assessment
- Awareness Training Review

# ADR 2011 Audit Plan Hot Spots

## RISK AREA

- Disaster Recovery

## AUDIT PLAN ITEM

- Application Criticality Review
- Backup & Recovery Prioritization Audit
- DR Maintenance Review
- Vendor Preparedness Review
- Disaster Simulation
- **Integration with BCP**

Off-shoring

# IT RISK CHEAT SHEET

*Audit Committees can benefit from a meaningful explanation of the IT threat landscape*

## Elements of the IT Risk Taxonomy

Threat Category	Threat	Definition	Sample Controls
Internal Non-Malicious	1. Internal Infrastructure Breakdown	Failure of IT components due to inadequate change/configuration management, heterogeneity of environment, etc.	Systems planning, change management, development, and maintenance
	2. Employee Carelessness	Unintentional actions exposing company to information risk	Application access, policy awareness campaigns, incident response
Internal Malicious	3. Privilege Abuse	Intentional misuse of access to sensitive information and IT systems to commit fraud, theft, etc.	Physical control event logging, content monitoring, privilege control
External Non-Malicious	4. Environmental Disaster	Catastrophic events—earthquakes, floods, pandemics, etc.—with implications for business continuity	Business continuity plan, business impact analysis, disaster recovery plan
	5. External Infrastructure Breakdown	Failure of public infrastructure due to inadequate maintenance, poor design, etc.	Systems maintenance, backup/restoration readiness, resiliency testing
	6. Legislation/Regulation	External compliance mandates, including privacy standards such as PCI, with implications for information security	Compliance monitoring, policy, and standards
External Malicious	7. Malware	Viruses, worms, Trojans, spyware, adware, etc.	Firewalls, anti-virus management, security patches
	8. Social Engineering	Motivated outsiders seeking to tease sensitive information out of employees	Network controls, personnel training, and awareness campaigns
	9. Physical Intrusion	Petty criminals, disgruntled former employees, etc.	Physical security, separation of duties, privilege control
	10. Industrial Espionage	Sophisticated agents seeking access to proprietary data by electronic and physical means on behalf of a competitor	Firewalls, data and file encryption, device authentication
	11. Hacking/Cracking	Sophisticated agents seeking unauthorized access to restricted networks, usually with the intention of committing fraud or theft	Firewalls, data and file encryption, device authentication
	12. Spam/Phishing/Pharming	Electronic communications designed to lure the recipient into revealing their personal data	Firewalls, anti-virus management, security patches

Source: Information Risk Executive Council research; Audit Committee Leadership Forum research.

# Business Risks

- **Inability to deliver services / products efficiently and effectively**
- **Inability to comply with regulations or contractual obligations**
- **Lack of access controls --> fraud risk, disclosure**
- **System does not meet the user needs**
- **Poor system performance / throughput impacts user productivity**
- **Data integrity problems**
- **Users frustrated with reporting capabilities ... develop their own using Excel spreadsheets**
- **Users not adequately trained and do not know how to properly use the system**

# Business Impact

- **Relate IT risks to business impact:**
  - **Financial loss**
  - **Asset loss**
  - **Bad publicity**
  - **Productivity**
  - **Customer service**
  - **Legal / regulatory ramifications**

**Business needs to have an effective identification and assessment of business risks associated with IT, where the risks is greater than nominal.**

# Types of RAs

- **Strategic**
- **Operational**
- **Compliance**
- **Internal Audit**
- **Financial Statement**
- **Fraud**
- **Market**

- **Credit**
- **Customer**
- **Supply Chain**
- **Product**
- **Security**
- **Information Technology**
- **Project**

## To Begin.....

- **Obtain the latest IT Risk Assessment document**
- **Obtain the company's business model:**
  - **Goals & Objectives**
  - **Strategies**
  - **Policies & Procedures**
- **Understand the IT function to include management and operations**
- **Identify all General Control categories**
- **Obtain the Disaster Recovery Plan and recent test results / issues**

# IT General Controls

- **Important for compliance with SOx and MAR**
- **Categorized as “Key” or “Non-Key”**
- **Key rated as H, M, or L**
- **Aspects:**
  - **Impacts on Financial Reporting**
  - **Threats and Risks**
  - **Compensating Controls**

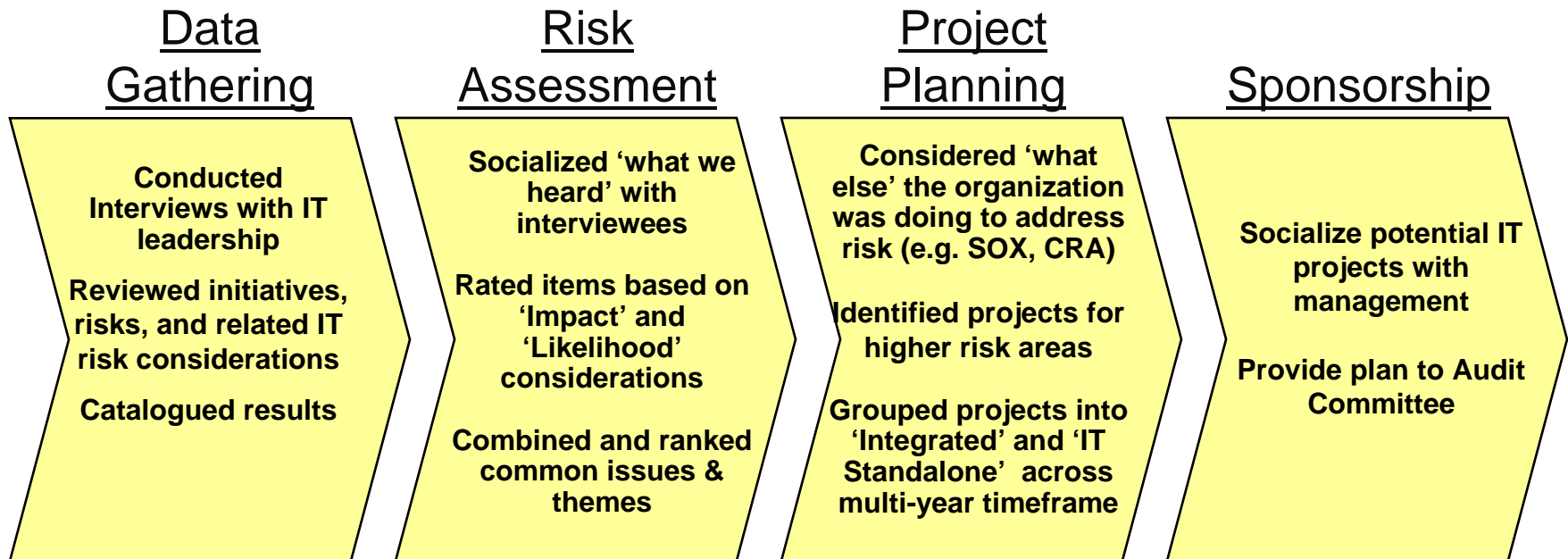
# IT General Controls

- Incident Management
- Change Management
- Release Management
- Solutions Delivery Methodology (SDLC)
- Strategic Planning
- Identity and Access Management
- Operations Management
  - Mainframe
  - Distributed
- Physical Security
- Risk Management

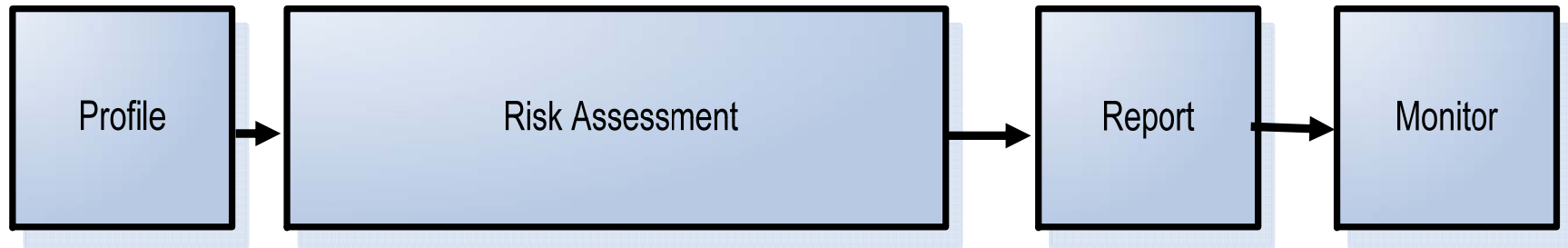
# Risk Analysis

- **Qualitative: identify the major threats to which an enterprise is exposed. Qualify which risks are worth protecting against**
  - What could happen?
  - How likely?
  - The impact?
- **Quantitative: establish monetary value for the assets and processes, probability of the occurrence, ROI for safeguarding the assets**
- **All audits start with a RA of the area being reviewed**

# IT Audit Planning Process Overview



# Risk Management Activities



# Risk Management Process

- **Identify information resources**
- **Assess threats and vulnerabilities**
- **Impact analysis**
- **Identify risks, evaluate controls**

# Identify Information Resources

- **Typical types of assets**
  - Information and data
  - Hardware
  - Software
  - Services
  - Documents
  - Personnel
- **Critical systems - based on business objectives and information assets**
- **System support infrastructures**
  - Operating Systems
  - Database Management Systems
  - Networks
  - Data Centers

# Assess Threats and Vulnerabilities

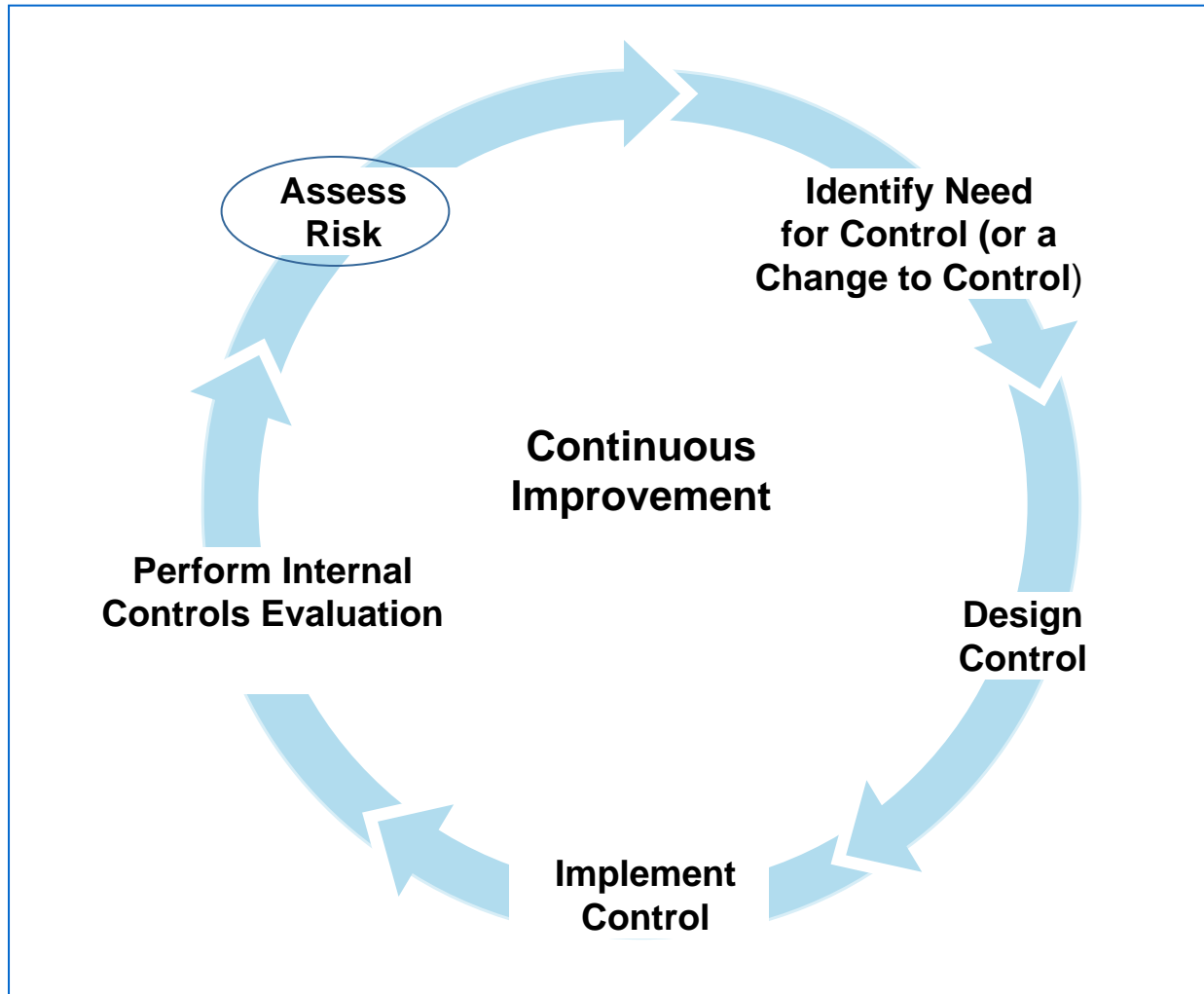
<b>Assets</b>	<b>Threats</b>	<b>Vulnerabilities</b>	<b>Impact</b>
<b>Information/ Data</b>	<b>Errors</b>	<b>Lack of user knowledge</b>	<b>Incorrect financial statements</b>
<b>Hardware</b>	<b>Malicious Attacks</b>	<b>Lack of security functionality</b>	<b>Loss of confidential data</b>
<b>Software</b>	<b>Fraud</b>	<b>Poor passwords</b>	<b>Theft, excessive payments</b>
<b>Documents</b>	<b>Theft</b>	<b>Transmissions not secured</b>	<b>Eavesdropping</b>
<b>Services</b>	<b>Internal / External</b>	<b>Poor service levels / contracts</b>	
<b>Personnel</b>	<b>Equipment failure</b>	<b>Lost productivity</b>	

# What do you do with Risk?

- **Accept:** the risk and the potential \$\$\$ fall-out
- **Avoid:** disengage in the activity or find a different approach to the activity that is creating the risk
- **Transfer:** to another department, company or take out insurance
- **Mitigate:** add controls or change the process



# Lifecycle of a Control



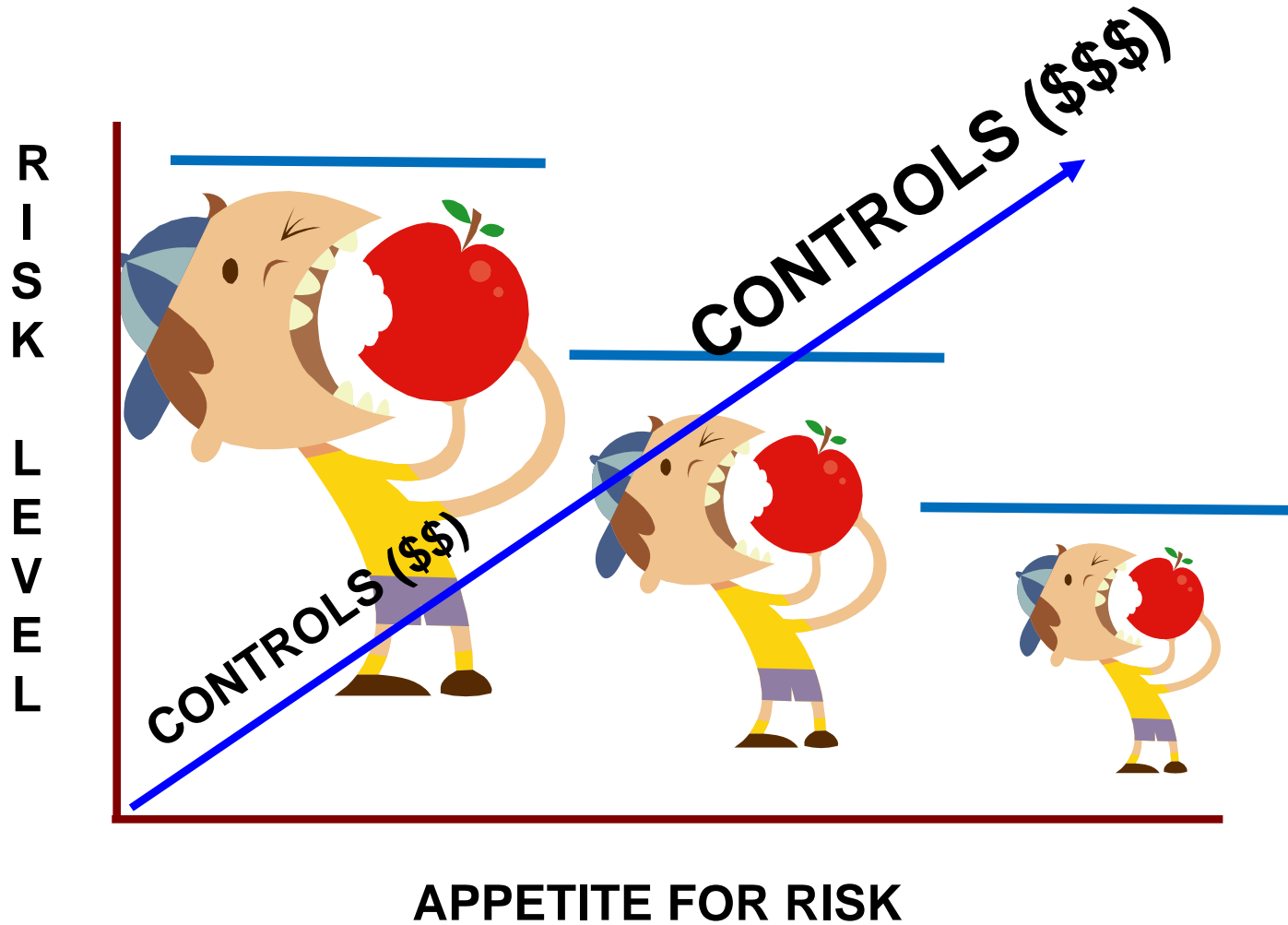
# Evaluate Controls

- **Controls are countermeasures to inherent risk**
- **Inadequate existing controls require design of new ones**
- **Inherent control: design strength and likelihood of effectiveness**
  - **Preventive vs. detective**
  - **Manual vs. automated**
  - **Ad hoc**
- **Residual risk: after applying the inherent control, the remaining risk not covered**

# Cost / Risk

- **The impact/severity of the risk is proportional to the business value of the loss / damage**
- **A fundamental problem of risk management is to achieve a cost-effective balance between risk and countermeasures**
- **An additional factor is the level of risk that management will accept (risk appetite)**

# Risk Appetite



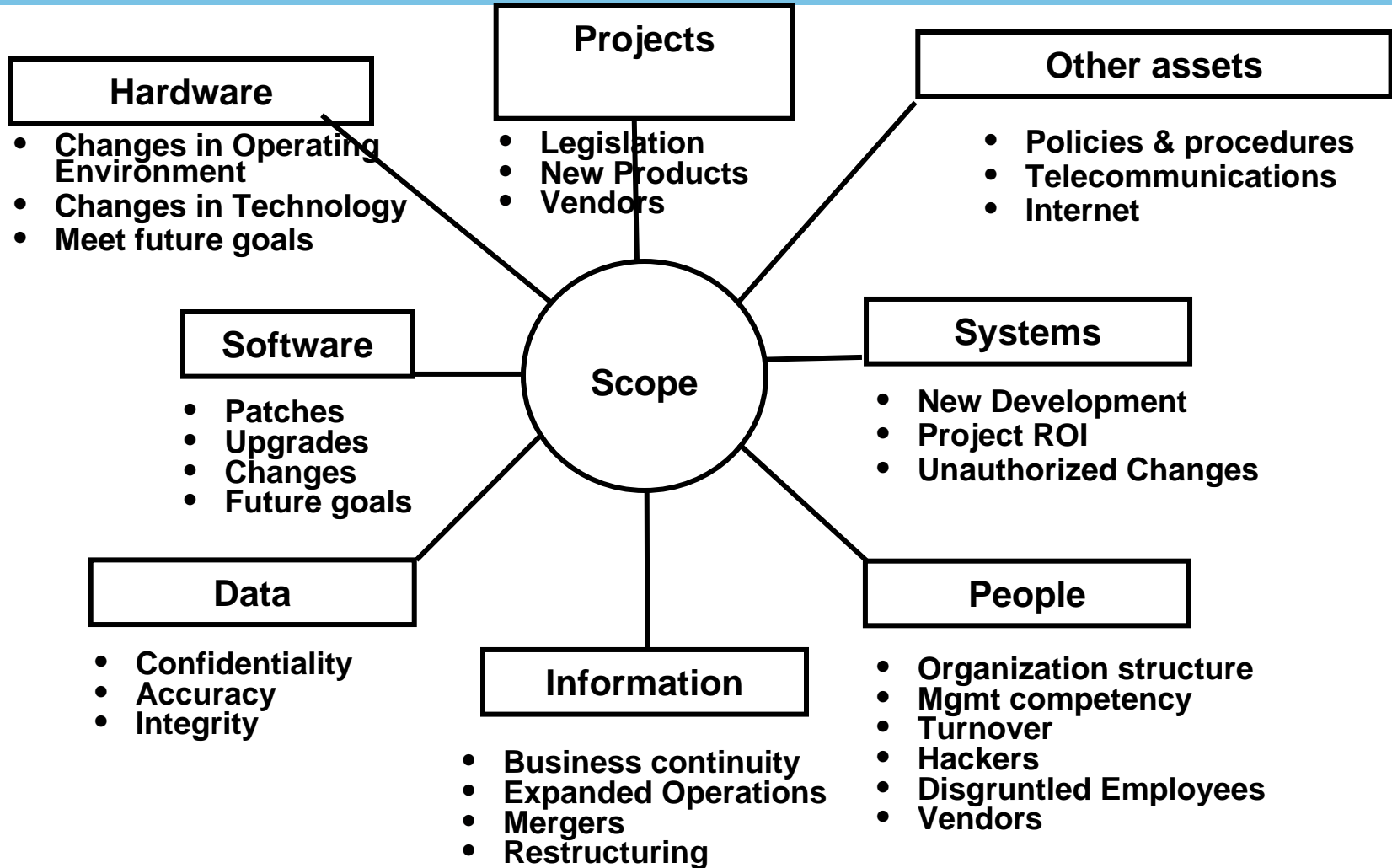
# Risk Assessment Activities

- **Determine areas to include within the scope.**
- **Leverage results of previous assessments/audits to promote efficiencies.**
- **Conduct facilitated sessions with key business and IT process owners to identify and understand IT risks.**
- **Aggregate the results to develop the risk universe.**
- **Create risk evaluation criteria to assist in the prioritization of risks.**

# Components of Risk Assessment

- **Risks and risk impact:**
  - **Identify risk**
  - **Classify the risk**
  - **Prioritize the risk**
  - **Evaluate the risk and impact**
- **Provide management with recommendations**
- **Management review:**
  - **Risk identification**
  - **Risk analysis**
  - **Predetermined organization objectives**

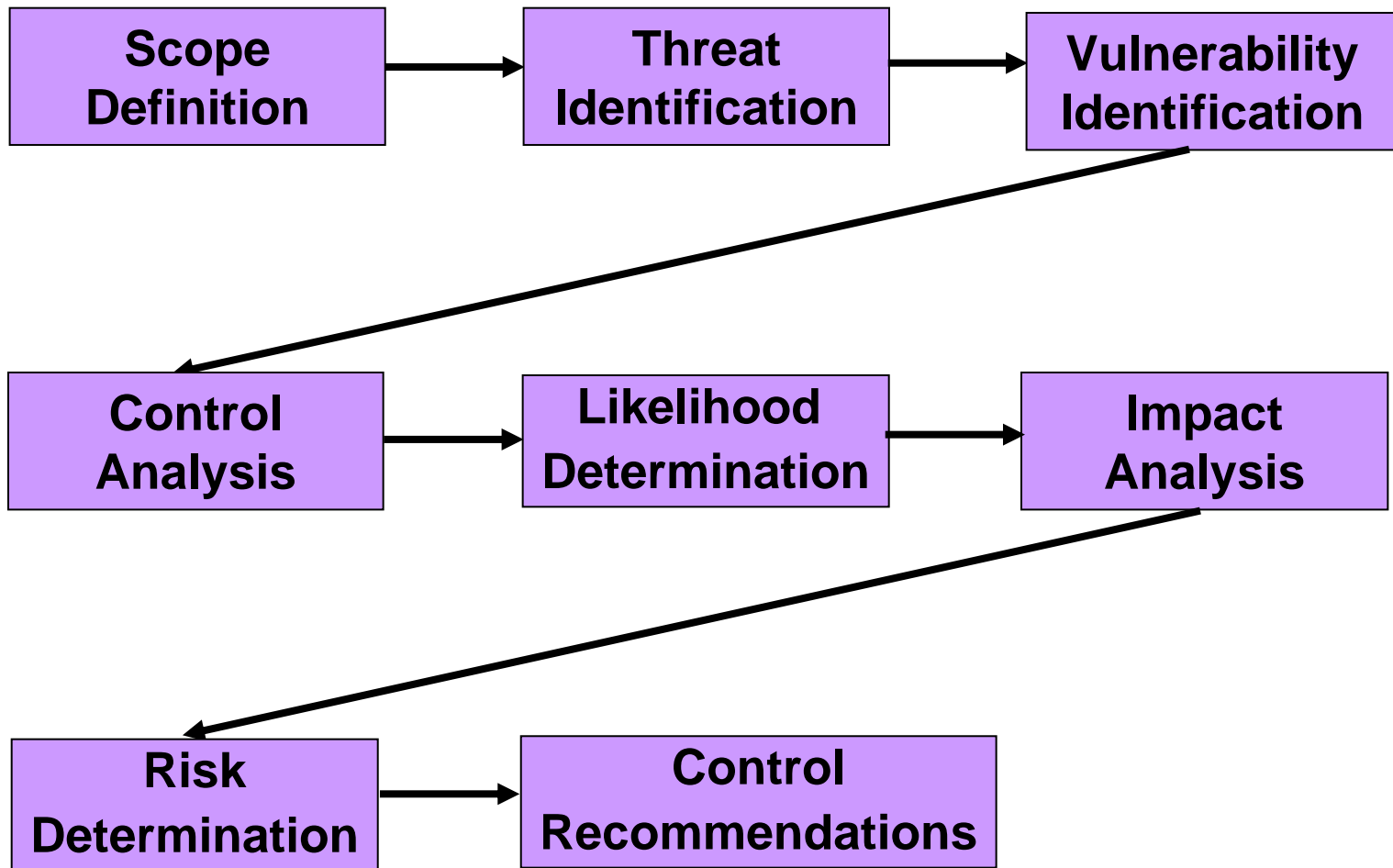
# Scope of an Assessment



# Data Integrity Risks

- **Data / systems**
  - **Critical to operations**
  - **Contain confidential information**
- **Data integrity- risk of unauthorized access:**
  - **If the data is changed**
    - ... will it alter the value of corporate assets?
    - ... will it cause a change in the outcome of a basic business function?
  - **Disclosure of information represents a risk of damage to the company or an individual**
- **Systems support the critical data?**

# Risk Assessment Flow



# IT Risk Assessment Steps

## 1. Scope Definition

### ❖ What

- IT Infrastructure
- Resources
- IT Risk Assessment document
- Documentation: business model, P&P, goals & objectives

### ❖ How

- Questionnaires
- Interviews
- IT Strategic Plans
- Documentation Reviews

## 2. Threat Identification

### ❖ What

- Object
- Person
- Outside entity
- New technology
- Business environment

### ❖ How

- History of attacks
- Intelligence reports

# IT Risk Assessment Steps

## 3. Vulnerability Identification

### ❖ What

- Flaw or weakness in security
- Design flaws
- Control flaws
- Documentation

### ❖ How

- Previous Risk Assessments
- Audit Comments
- Security Reviews

## 4. Control Analysis

### ❖ What

- Current Controls
  - Technical
  - Non-Technical
  - P & D
  - K & S
- Planned Controls

### ❖ How

- Audit Comments
- CobiT 4.1

# IT Risk Assessment Steps

## 5. Likelihood Determination

- ❖ **What**
  - Threat source motivation
  - Threat capacity
  - Current Controls
- ❖ **How**
  - Interviews with IT
  - Interviews with Management
  - Rank as High, Medium, Low

## 6. Impact Analysis

- ❖ **What**
  - Mission
  - Asset Criticality
  - Data Sensitivity
  - Data Criticality
- ❖ **How**
  - Interview information owners
  - Analyzing data sensitivity

# Joining Two Aspects

	<b>High</b>	<b>Medium</b>	<b>Low</b>
<b>Likelihood</b>	<b>&gt; 40%</b>	<b>10 - 40%</b>	<b>&lt;10%</b>
<b>Impact</b>	<b>\$5MM</b>	<b>\$1 - 5 MM</b>	<b>&lt; \$1MM</b>

# IT Risk Assessment Steps

## 7. Risk Determination

- ❖ **What**
  - Likelihood of threat
  - Extent of Impact
  - Controls Adequacy
  
- ❖ **How**
  - Risk Matrix
  - Determine Probability
  - Determine Severity

## 8. Control Recommendations

- ❖ **What**
  - Policies & Procedures
  - Human Resources
  - Hardware / Software Controls
  
- ❖ **How**
  - Audit Comments
  - CobiT 4.1

# Control Recommendations

- **Categorize weaknesses and prioritize the remediation**
- **Control weaknesses not mitigated could have negative impact on the organization**
- **Remediation strategy, while costly, must be adopted, approved and reviewed by senior management**
- **Progress on the remediation should be monitored and reported**
- **Conduct the assessment again**

# Risk Assessment

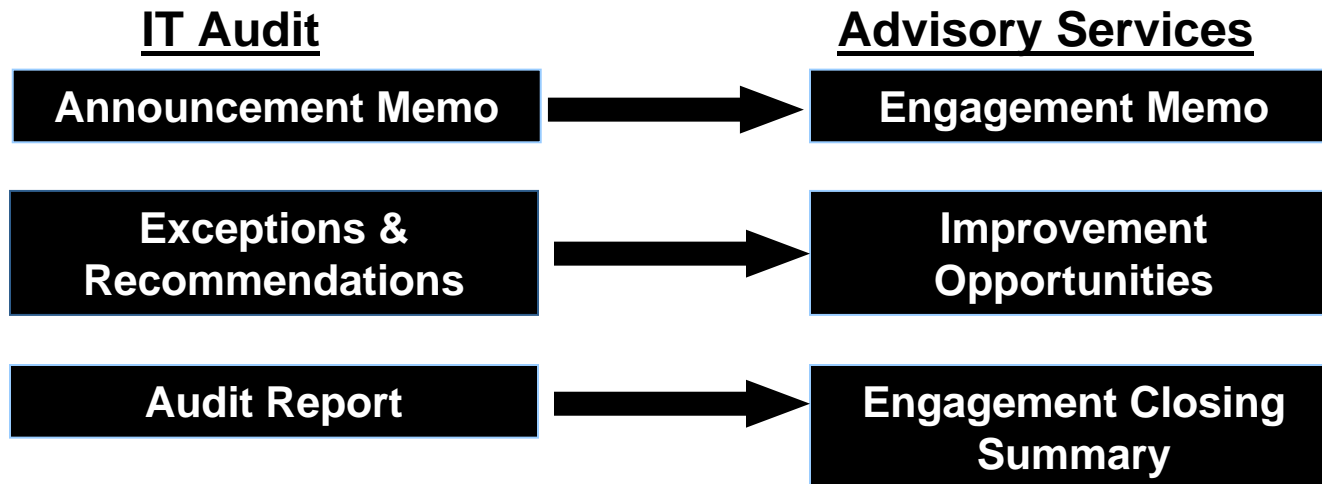
- **IT Organization**
- **Projects (Audit Advisory Services)**

# Project Factoids

- **More than 60% of large projects:**
  - fail to meet the business objectives
  - are significantly late
  - are severely over budget
  
- **Success rates of execution:**
  - 50% are over budget
  - 58% missed major milestones
  - 42% had defects after production

# Audit Advisory Services

- Services that are designed to be more advisory (i.e. front end) in nature than traditional audits
- Include consultations, special projects, internal control & accountability reviews, systems development and process re-engineering



# Audit Advisory Services

The utilization and reliance upon technology to manage and support the business has increased exponentially over the last two decades

IT Auditing has evolved into a necessary requirement to manage and govern an organization's risk and compliance posture

## RISK MANAGEMENT

Continue to invest in technology to reduce administrative costs, increase efficiencies and achieve competitive advantages

Proactive controls consulting will result in appropriate controls being implemented early in the development process

# Risk Category

<b>Risk Category</b>	<b>Risk Factors</b>
<b>Business Risk</b>	<b>Alignment with Vision Points</b>
<b>Business Risk</b>	<b>Impact of Not Doing</b>
<b>Business Risk</b>	<b>Cost</b>
<b>Business Risk</b>	<b>Impact on Processes and Functions</b>
<b>Business Risk</b>	<b>Projects That Depend on This Project</b>
<b>Business Risk</b>	<b>Results Subject to External Audit</b>
<b>Project Risk</b>	<b>Business Owner</b>
<b>Project Risk</b>	<b>Business Lead(s)</b>
<b>Project Risk</b>	<b>Project Manager</b>
<b>Project Risk</b>	<b>Project Urgency</b>
<b>Project Risk</b>	<b>Estimated Project Duration</b>
<b>Regulatory Risk</b>	<b>Mandated by Law, a Government Contract, etc.</b>
<b>Regulatory Risk</b>	<b>Data Type</b>
<b>Regulatory Risk</b>	<b>MAR Application Impact</b>
<b>Regulatory Risk</b>	<b>Mandated by HCSC, BCBSA, customer contract, etc.</b>
<b>Technical Risk</b>	<b>Impact on Systems/Applications</b>
<b>Technical Risk</b>	<b>In-house or Vendor-based Solution</b>
<b>Technical Risk</b>	<b>Data Complexity</b>
<b>Technical Risk</b>	<b>Data Transmittal/Access Method</b>
<b>Technical Risk</b>	<b>Technology Used</b>
<b>Technical Risk</b>	<b>IT Impact</b>

# Risk Analysis Template

Risk Category	Risk Factors	Response	Risk	Score
Project Risk	Business Owner	3+ or None (zero)	HIGH	75
Project Risk	Business Lead(s)	2	MEDIUM	50
Project Risk	Project Manager	Not Identified	HIGH	75
Regulatory Risk	Mandated by Law, a Government Contract, etc.	Yes	HIGH	94
Business Risk	Alignment with Vision Points	Remote/Indirect	HIGH	75
Project Risk	Project Urgency	High	HIGH	75
Business Risk	Impact of Not Doing	Lose Advantage	MEDIUM	50
Business Risk	Cost	> \$7,000,000	HIGH	75
Business Risk	Impact on Processes and Functions	3-4	MEDIUM	50
Business Risk	Projects That Depend on This Project	2+	HIGH	75
Technical Risk	Impact on Systems/Applications	2-3	MEDIUM	63
Technical Risk	In-house or Vendor-based Solution	Offshoring	HIGH	75
Technical Risk	Data Complexity	Very Complex	HIGH	75
Regulatory Risk	Data Type	Medium Sensitivity	MEDIUM	62
Technical Risk	Data Transmittal/Access Method	New Method for Remote Access	MEDIUM	63
Project Risk	Estimated Project Duration	9-13 months	MEDIUM	50
Regulatory Risk	MAR Application Impact	Critical Application	HIGH	94
Technical Risk	Technology Used	Mix of current and state-of-the-art	MEDIUM	63
Regulatory Risk	Mandated by HCSC, BCBSA, customer contract, etc.	Yes	HIGH	75
Technical Risk	IT Impact	Severe or not considered	HIGH	94
Business Risk	Results Subject to External Audit	Yes	HIGH	75
			<b>Total Risk Score</b>	<b>1483</b>
			Low Risk	337 - 680
			Medium Risk	681 - 1024
			High Medium Risk	1025 - 1368
			High Risk	1369 - 1708

# Provides Summary

#	Business Cases	Risk Score	Risk Rating
1	Nantional Provider Identifier (NPI)	1368.75	High
2	BHI	1318.75	High
3	Enterprise Content Management	1246.75	High
4	Enterprise Operational Data Store	1246.25	High
5	CCSP Pre-Adjudication	1218.75	Medium
6	Ariba	1125	Medium
7	Manager of Managers	1121.25	Medium
8	Enterprise Search Capability	1098.75	Medium
9	Distributed Environment Access Clean-Up	1093.65	Medium
13	Workers Choice Conversion	1017.5	Medium
14	PIDDS	1010	Medium
15	MME	1000	Medium
16	PeopleSoft v8.9 Upgrade	987.5	Medium
17	ABS	950	Medium
18	Re-engineer Shared Claims Processing	948.75	Medium
34	Application Optimization	867.5	Medium
35	DR Plan/Development	856.23	Medium
36	Provider Data Accuracy	847.5	Medium
37	Enterprise IVR	825	Medium
38	HIT-RHIO Initiatives - Participation & Leadership	815	Low
39	Unique BIN/PCN	812.5	Low
40	Offsite Encryption Phase I	812.5	Low
41	FCR	809.25	Low
42	ITG - In Center Datat Replication	807.5	Low
43	EMC Net Replacement	773.75	Low
44	BlueCap	734.25	Low
Average Risk Score		967.27	
Average Risk Rating		Medium	



**[john.gatto@bcbsil.com](mailto:john.gatto@bcbsil.com)**