Deloitte.

Leveraging IT risk assessment to add value.

Leading Practice IT Risk Assessment

ISACA San Francisco Chapter Luncheon
January 24, 2008

Audit. Tax. Consulting. Financial Advisory.

Leading Practice IT Risk Asssessment

The Fine Print

This publication contains general information only and Deloitte & Touche LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte & Touche LLP, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Today's discussion

- **Overview: Leading Practice IT Risk Assessment**
- **Performing Risk Assessments for IT**
  - Identifying and Evaluating IT Risks
  - Using IT Risk Frameworks including CobiT
  - Linking IT Risks to Organizational Objectives
- **Creating a Risk Response**
- **Common and Emerging IT Risks**

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Leading Practice IT Risk Assessment

- Organizations are focusing on increasing the cost efficiency of their compliance programs while improving the effectiveness of their governance, risk management and compliance programs.

- In this high pressure business environment, how can IT internal auditors perform risk assessments to ensure that internal audit activities link to business objectives and organizational value drivers?

Copyright © 2008 Deloitte Development LLC. All rights reserved.

The Role of Internal Audit

- "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.
- It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

Source: ***The International Standards for the Professional Practice of Internal Auditing*** **(*Standards*)**
The Institute of Internal Auditors

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Typical Company Risk Assessment Activities

Enterprise Risk Management

- Enterprise Risk Assessment

Compliance

- Regulatory Risk Assessments

Internal Audit Risk Assessment

- Business Risks
- IT Risks
- Project Risks
- Vendor Risks
- Location Risks
- Etc.

SOX

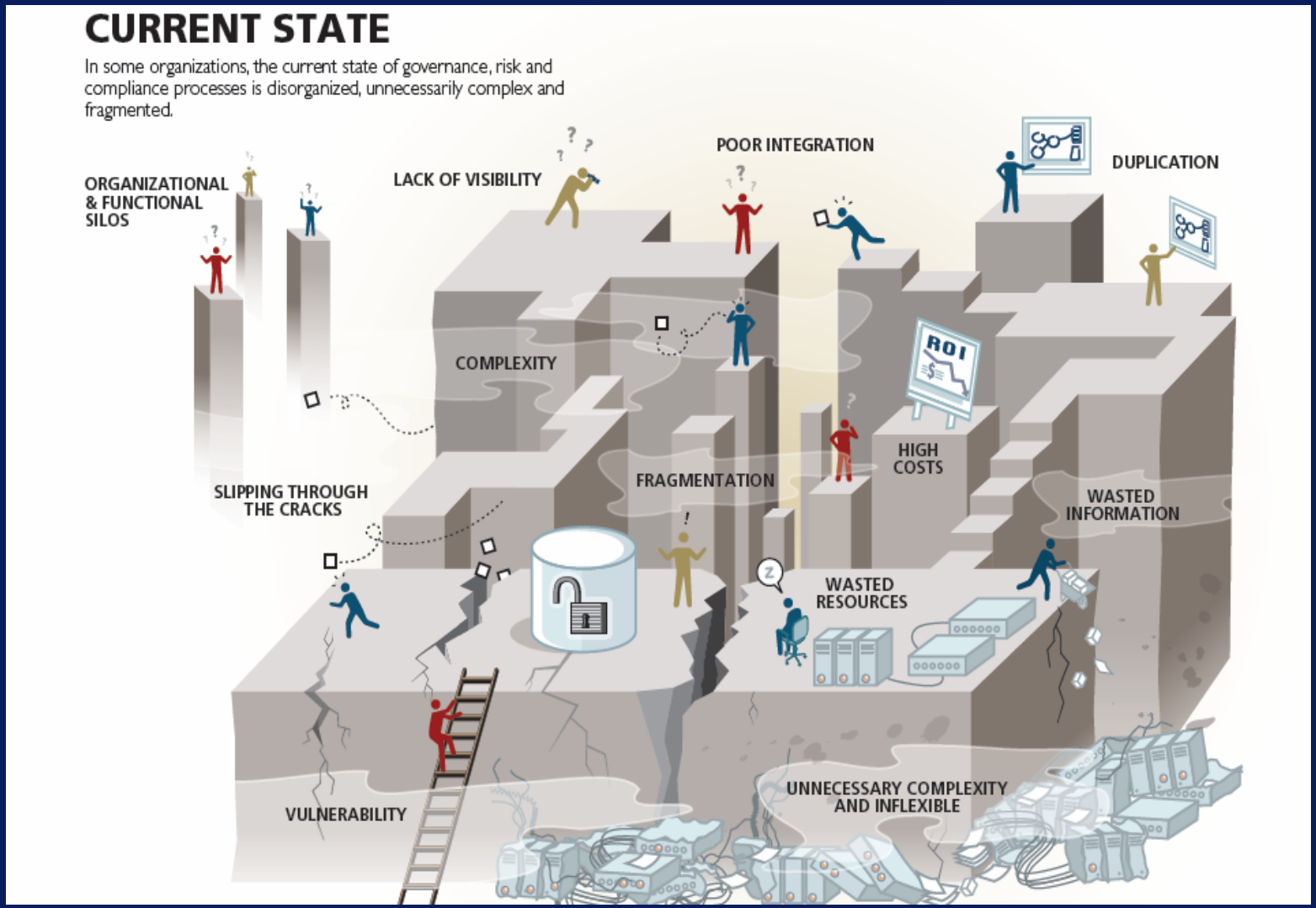
- Financial Reporting Risk Assessments
- Control Assessment

Business Continuity

- Business Impact Assessment

Copyright © 2008 Deloitte Development LLC. All rights reserved.

The need to improve Governance, Risk Management and Compliance is clear



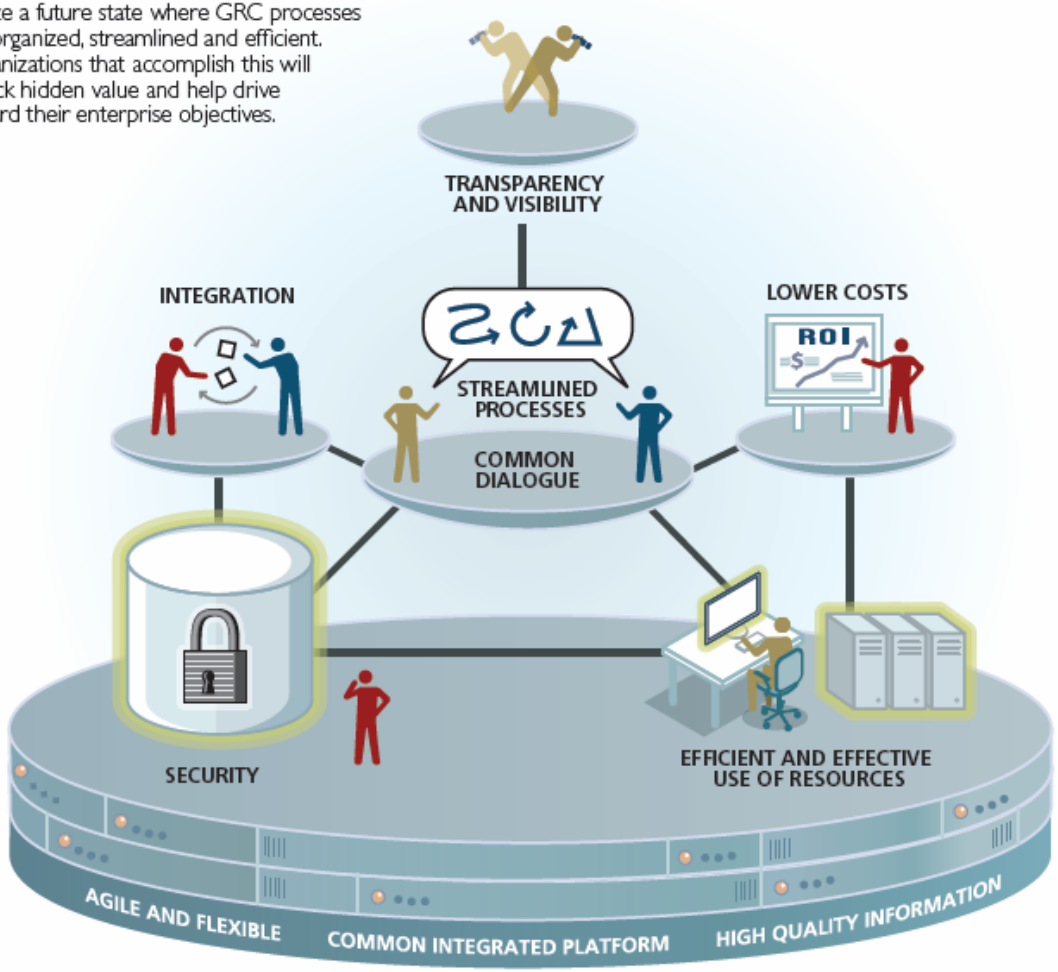
Adapted from the GRC illustration that appeared in Compliance Week, sponsored by Deloitte Consulting, SAP, and OCEG.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

The opportunity exists to simultaneously improve GRC efficiency and effectiveness

FUTURE STATE

As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive toward their enterprise objectives.



Critical Success Factors

Team
Leadership alignment and the right mix of skills to see and analyze the entire situation

Openness
Willingness to listen; face the facts; don't shoot messengers

Enterprise Perspective
Get out of siloed thinking to see the big picture

Fact-Driven Analysis
Accurate, relevant information that reflects reality; use both quantitative and qualitative evidence

Clear & Compelling Story
Numbers will not speak for themselves – the numeric case must be supported by a narrative case

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Evaluating Risk Intelligence

Illustrative

Tribal & Heroic	Specialist Silos	Top Down	Systemic Risk Mgmt.	Risk Intelligent
• Ad-hoc/ chaotic • Depends primarily on individual heroics, capabilities, and verbal wisdom	• Independent risk management activities • Limited focus on the linkage between risks • Limited alignment of risk to strategies • Disparate monitoring and reporting functions	• Common framework, program statement, policy • Routine risk assessments • Communication of top strategic risks to the Board • Executive/Steering Committee • Knowledge sharing across risk functions • Awareness activities • Formal risk consulting • Dedicated team	• Coordinated risk mgmt. activities across silos • Risk appetite is fully defined • Enterprise-wide risk monitoring, measuring, and reporting • Technology implementation • Contingency plans and escalation procedures • Risk management training	• Embedded in strategic planning, capital allocation, product development, etc. • Early warning risk indicators • Linkage to performance measurement/incentives • Risk modeling/scenarios • Industry benchmarking

Copyright © 2008 Deloitte Development LLC. All rights reserved.

The Level of Internal Audit's Effort is Dependent of the Company's Risk Intelligence Capability

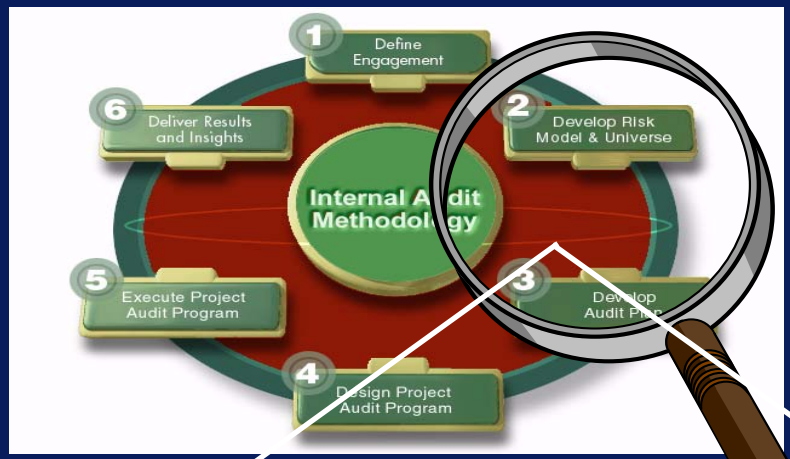
Illustrative

Typical Implications for Internal Audit

Tribal & Heroic / Specialist Silos	Top Down	Systemic Risk Mgmt. / Risk Intelligent
• Risk identification and assessment typically initiated and led by IA • Heavier involvement in risk analysis • Heavier involvement in formulation of recommendation for risk mitigation and control	• Leveraged risk identification / assessment • Better coordination with risk owners on risk mitigation efforts and controls	• Linkage of IA Risk Based audit plan to ERM • Risk Owners Formulate Mitigation • Internal Audit evaluates and monitors

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Introduction: Overview of the IT risk assessment methodology



- The Information Technology Internal Audit Risk Assessment Methodology adopts the broader concepts of Enterprise Risk Assessment with the overall objective of developing a risk-based internal audit plan
- Likewise, the methodology creates a meaningful linkage to value-creation, achieving both assurance and consulting objectives of an Internal Audit activity

Phases of the IT IA Risk Assessment Methodology

Phase 1: Understand the Business and IT

Phase 2: Develop the IT Risk Model

Phase 3: Prioritize IT Risks

Phase 4: Develop Risk-Based IT Internal Audit Plan

Phase 5: Schedule the Audits & Plan resources

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Phase One: Understand the Client's Business

Key Activities

- Gather information:
  - Business and IT objectives and strategies
  - Organizational structure and changes
  - Key business processes and locations
  - Key information systems
  - Company's disclosed risks (10-K)
  - Key industry risks and issues
- Organize information on the company's structure (processes, locations, and systems)

Key Deliverables

- Client Profile
  - Business and IT Objectives/Strategies
  - Organizational structure
  - Business Process, Locations and systems
- Preliminary risk information
  - 10-K disclosed risks
  - Other company risk information
  - Key industry issues

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Understand IT objectives, goals, strategy and processes

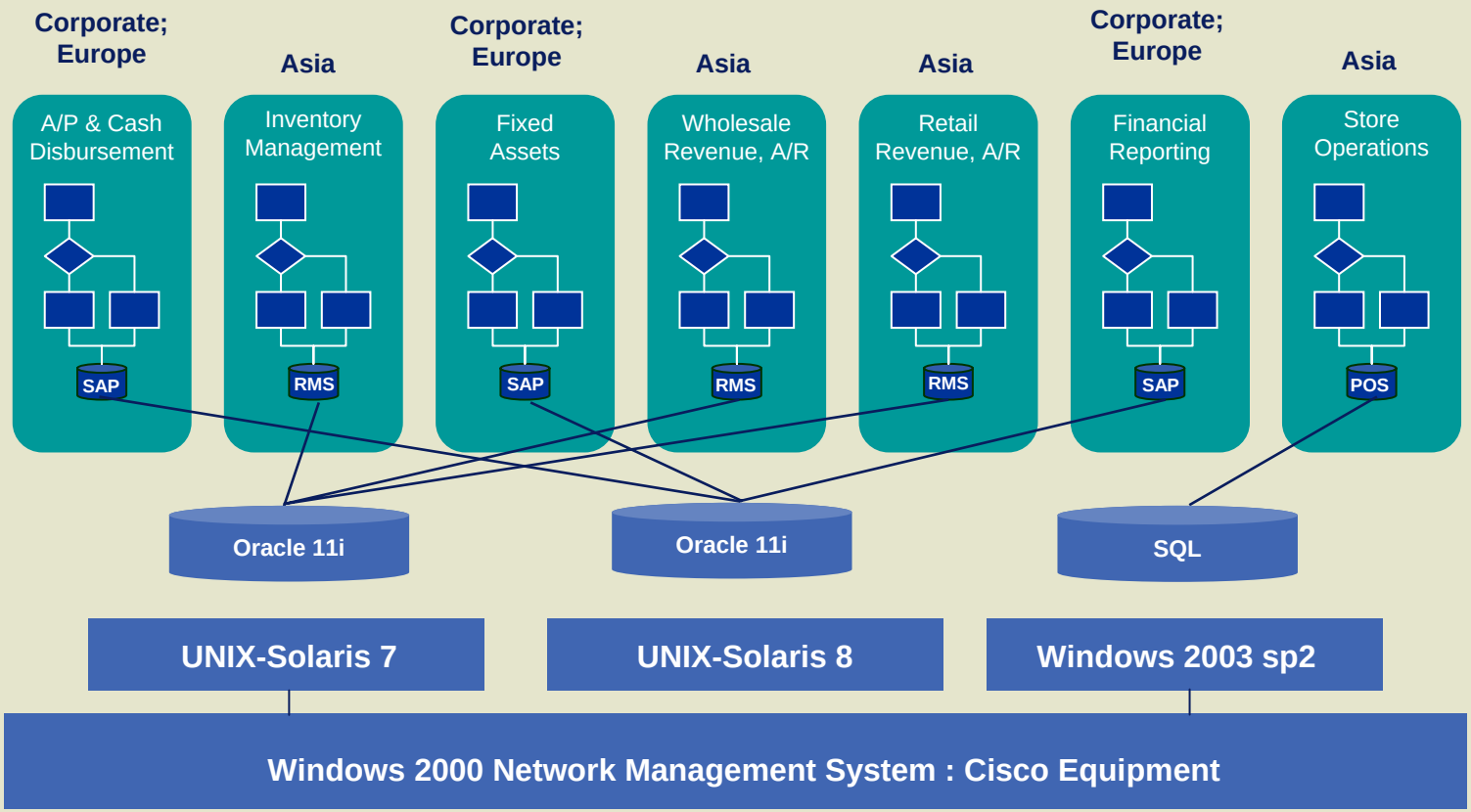
- IT & Business Strategic Plans
- Annual IT Plan & Budget
- Annual Business Plan
- Key IT Performance Metrics
  - E.g., projects, change requests, service requests, contracts, SLAs, etc.
- IT Project List
- IT Project Charters and Project Plans
- Entity Level Control Environment
- IT Policies & Procedures
- IT Risk and Control Matrices
- Attest Reports (IT)
- Management's IT SOX Results
- Previous IT Internal Audit Reports

- IT organization chart; company org chart
- Business locations
- Data Center and other IT locations
- IT processes & process owners
- Inventory of systems and key interfaces
  - Applications
  - Databases
  - Operating systems
  - Tools
  - Hardware
- Network and other diagrams

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Business Processes Linked to Information Systems and Locations

Illustrative



Copyright © 2008 Deloitte Development LLC. All rights reserved.

Example - Key Processes, Systems, and Locations

Illustrative

Key Locations

- Corporate - Japan
- Service Centre- Atlanta
- USA
- Asia
- Europe

Key Processes/ Divisions

- Revenues (A)
- Corporate Legal & Compliance (B)
- Payroll & Personnel (C)
- Fixed Assets (D)
- Corporate Finance (E)
- Expenditures (F)

Process Owners/ Head

- Corporate - Japan
- Service Centre- Atlanta
- USA
- Asia
- Europe

Key Application Systems	Key Databases	Key Operating Systems
Oracle Financials	**Oracle Database**	**Unix**
Siebel CRM	**Oracle Database**	**Unix**
Corp Legal & Compliance Apps	**Microsoft Access**	**Windows**
PeopleSoft HR	**Oracle Database**	**Unix**
ADP Payroll	**ADP (Outsourced Service Provider)**	**ADP (Outsourced Service Provider)**
Hyperion	**Oracle Database**	**Windows**

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Example – Map of Business Processes to Systems

Illustrative

Company Name: ABC

Key Applications / Module		Business Critical Process	Application vendor	Key Interfaces	Operating System	Database	Business	IT Support				
							App Owner	Application Support	Database Support	Operating System Support	Server Name	Database Name
A	Oracle	Financial system	Oracle	Avantis, ADP, Toptech	IBM AIX	Oracle	Owner	App Mgr	DB Mgr	OS Mgr	epa650trafxs2	File based database
B	Avantis	Project/ Maintenance Mgmt	Vendor - Ivensys	Excel	MS Win 2003	MS SQL	Owner	App Mgr	DB Mgr	OS Mgr	epa650avantis2	WRProduction
C	ADP	Payroll	Outsourced - ADP (SAS70)	None	N/A	N/A	Owner	App Mgr	DB Mgr	OS Mgr	N/A	N/A
D	Toptech	Marketing terminal, all daily liftings	Outsourced - Toptech	FAS	Proprietary QNX	Proprietary	Owner	App Mgr	DB Mgr	OS Mgr	epa650tms primary	N/A
E	FAS (Fixed Asset)	Fixed Assets	Sage Software (formerly Best Software)	Excel	MS Win 2000	Sybase	Owner	App Mgr	DB Mgr	OS Mgr	epa650app1	DB files in \\epa650app1\apps\bestserv*

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Phase Two: Develop Risk Model

Key Activities

- Develop the IT risk framework:
  - Risk categories framework
  - IT Risk listing with definitions
  - Risk rating criteria factors (Impact and Vulnerability)
- Validate the risk framework with key stakeholders

Key Deliverables

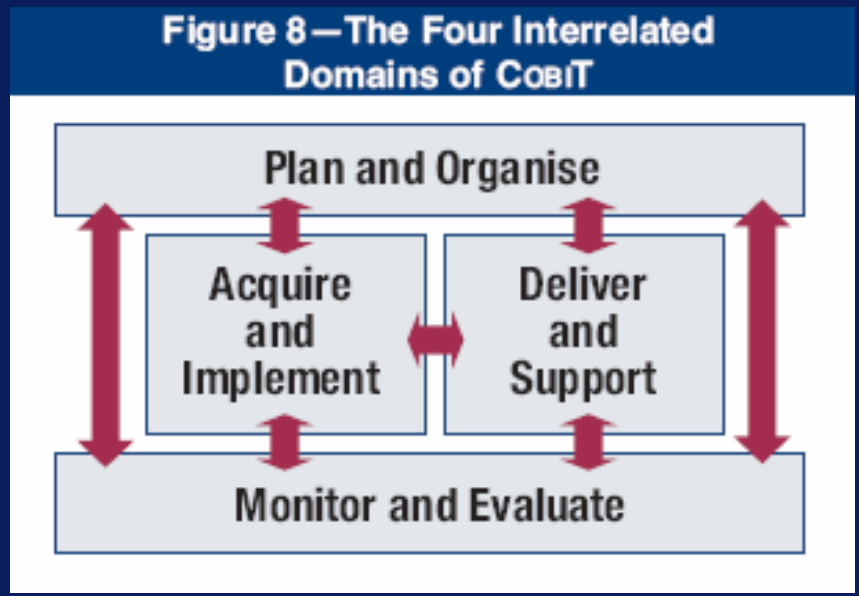
- Risk Categories Framework
  - Governance
  - Strategy
  - Operations
  - Infrastructure
  - External
- Business Risk Listing with risk definitions
- Risk rating criteria:
  - Impact
  - Vulnerability

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Develop the IT risk model

Control Objectives for Information and related Technology (COBIT®)

- An IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- Provides good practices across a domain and process framework

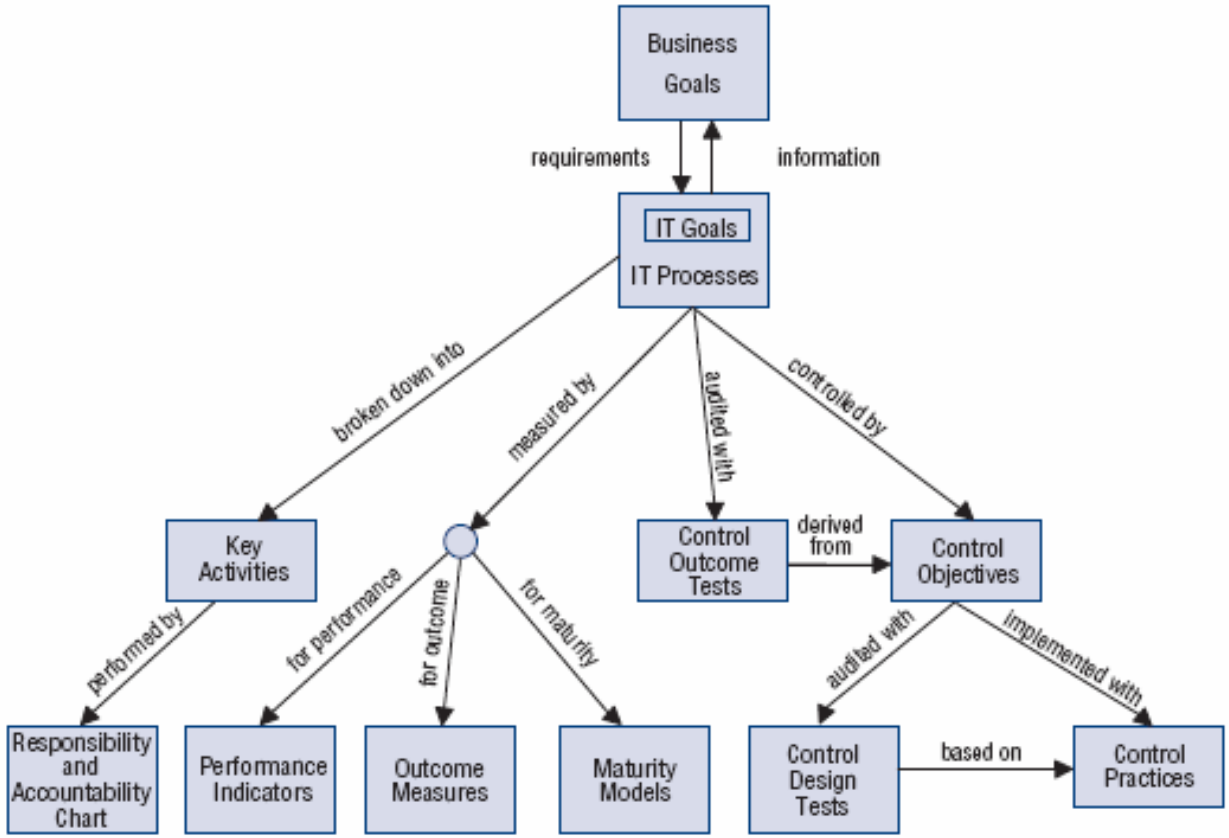


Source: CobiT 4.1 Excerpt Executive Summary, IT Governance Institute, 2007, www.isaca.org.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Control Objectives for Information and related Technology (COBIT®)

Figure 4—Interrelationships of COBIT Components



Source: CobiT 4.1 Excerpt Executive Summary, IT Governance Institute, 2007, www.isaca.org.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Deloitte & Touche LLP IT Risk Framework

Business Strategy
Corporate Governance
Regulatory & Legal
Technology Trends

IT Governance

• Mission • IT and Business Alignment • Portfolio Management • IT Risk Management • Policy

IT Strategy & Planning

• IT Planning • Strategic Sourcing • IT Organization • Human Resources • Asset Management • Budgets, Metrics & Controls

IT Processes

Architecture

- Technology Planning
- Emerging Technologies
- Standards
- Architecture Design & Management
  - Software
  - Infrastructure
  - Security
- Vendor / Product Selection
- Integration & Consolidation

Project Management

- Project Management Lifecycle (PMLC)
  - Initiating
  - Planning
  - Executing
  - Controlling
  - Closing
- Systems Development (SDLC)
  - Design
  - Acquire / Build
  - Test & QA
  - Data Conversion
  - Implement / Deploy
  - Support / Maintain
- Project Risk (Pre-Imp) Review
- Post Implementation Review

Applications & Databases

- Change Management (Applications, Databases & Infrastructure)
  - Change Prioritization
  - Documentation, Approval, and Tracking
  - Acquire / Build
  - Test & QA
  - User Acceptance
  - Approval to Transfer to Production
  - Emergency Changes
- Patch Management
- Configurable Controls
- Data Quality & Integrity
- Interface Validation & Integrity

Operations

- Data Processing
  - Batch Scheduling
  - Online Processing
- Application / Database Management
  - Capacity
  - Availability
  - Performance
- Facilities Management
- Data Retention / Backup
  - Scheduling
  - Processing
  - Offsite Storage
  - Retrieval & Restoration

Support

- Problem Management
  - Help Desk
  - Incident Response
  - Root Cause Analysis
- Service Level Management
- Vendor / Third-Party Management
- End-User Computing
- Software Licensing

Enterprise Security

- Security Configuration Management
  - Applications
  - Operating Systems
  - Databases
  - Networks
  - Hardware & Tools
- Identity and Access Management
  - User Provisioning
  - Administrative Access
  - Segregation of Duties
  - Remote Access
  - Third Party Access
- Threat & Vulnerability Management
  - Intrusion Detection / Response
  - Intrusion Prevention
  - Security Penetration & Vulnerability Testing
  - Virus Prevention / Detection
- Security Strategy & Compliance
- Security Awareness & Training
- Physical Security
- Privacy & Data Protection

Disaster Recovery

• Business Impact Assessment • Disaster Recovery Planning • Communications / Crisis Management Plans • Disaster Recovery Testing • Ongoing Maintenance / Updates

Infrastructure

• Operating Systems • Database Structures • Networks (Internal & Perimeter) • Hardware • Locations • Tools (E-mail, EDI, Messaging, etc.)

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Phase Three: Prioritize Risks

Key Activities

- Conduct interviews or workshops to gather risk ratings by designated key client participants:
  - C-Suite
  - Second tier management respondents (Vulnerability risk rating)
- Based on the executive risk assessment inputs, develop the Risk Heat Map

Key Deliverables

- Risk Heat Map
  - Risks prioritized based on Impact and Vulnerability risk ratings
  - A summary of risk assessment
  - Interview notes

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Prioritize IT risks

- Define the risk factors to be used as a basis for risk ranking:
  - Impact
  - Vulnerability
- Impact and Vulnerability can be assessed in terms of High, Medium and Low or using numerical ratings (e.g., 1 to 5 or 1 to 100)
- Risk Factors are used to assess the relative risk of each identified IT risk

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Prioritize IT risks

- Impact and Vulnerability criteria MUST be defined explicitly and agreed with the Risk Assessment sponsor in advance of the interviews, workshops, surveys and risk ranking. This will enable the following:
  - Standard criteria ensures consistency
  - Agreeing the criteria in advance helps build a foundation for consensus of risk assessment results

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Impact

- Impact is an estimate of the severity of adverse effects, the magnitude of a loss, or the potential opportunity cost should a risk be realized.
  - Impact can be thought of as gross inherent risk.
- Example Impact Criteria:
  - Strategic
  - Financial
  - Reputation
  - Legal and Regulatory
  - Operational
  - Stakeholders

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Vulnerability

- Vulnerability is the extent to which the functional area may be exposed or unprotected in relation to various risk factors after existing controls have been taken into account.
  - Vulnerability can be thought of as net residual risk.

    NOTE: Vulnerability differs form likelihood because likelihood only considers the probability of an event occurring, whereas vulnerability considers other aspects such as control effectiveness and preparedness.

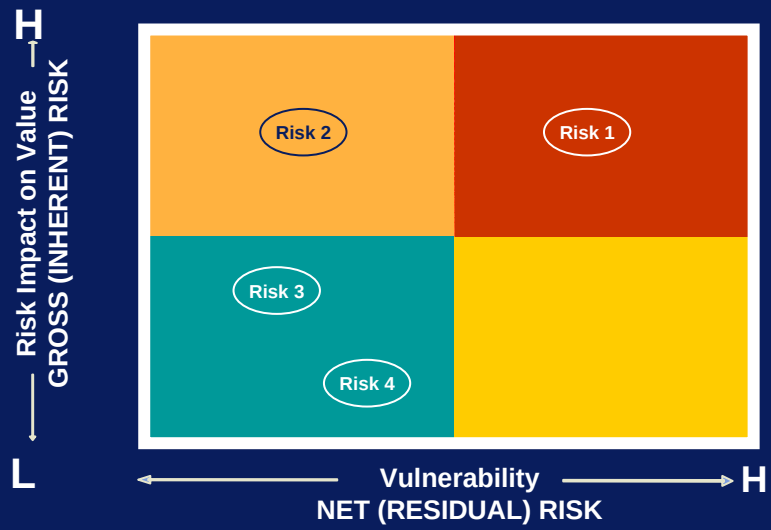
- Example Vulnerability Criteria:
  - Complexity
  - Control Effectiveness
  - Prior Risk Experience
  - Rate of Change

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Define Impact and Vulnerability Criteria

- Impact
  - Strategic
  - Financial
  - Reputation
  - Legal and Regulatory
  - Operational
  - Stakeholders
  - Competitor
- Vulnerability
  - Complexity
  - Control Effectiveness
  - Prior Risk Experience
  - Rate of Change
  - Preparedness

Define the Impact and Vulnerability criteria which will be applied to each identified IT risk to determine the relative risk rankings:



Copyright © 2008 Deloitte Development LLC. All rights reserved.

Sample Impact Criteria

RISK ASSESSMENT - IMPACT CRITERIA

NOTE: The percentages and dollar values used in this example are subject to change upon the company's actual materiality levels and risk factors, based on the judgment made together with management.

	Financial	Reputation	Legal/ Regulatory	Customer Satisfaction
	Operating Margin			
High	**$41-$80M**	**National and International coverage Wall Street Journal**	**Any Federal or State action**	**Significantly impact achievement of sales and service satisfaction goals/metrics**
Medium	**$26 -$40M**	**Escalating community activism, Regional Press Coverage**	**Any Federal or State scrutiny or Local action**	**Moderately impact achievement of sales and service satisfaction goals/metrics**
Low	**$0-25M**	**Local Press Coverage**	**Any Local scrutiny**	**Very low to No impact on the achievement of sales and service satisfaction goals/metrics**

NOTE: When evaluating the potential impact of a risk, select the highest (worst case) impact threshold exceeded and assign the corresponding impact level. (example: if a risk has a MEDIUM potential financial impact but has a HIGH reputation or regulatory

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Sample Vulnerability Criteria

RISK ASSESSMENT - VULNERABILITY CRITERIA							
	Vulnerability Factors						
	Control effectiveness & efficiency	**Previous risk experience**	**Complexity**	**Capability**			**Rate of change**
	Criteria	History of risk happening or knowledge of occurrence (through IA opinion, external auditor comments, legal cases, etc)		**People**	**Process**	**System** (timely, reliable, accessible, available, cost)	**Expansion or Contraction** (business, people, process, systems)
High	Controls are not working or do not exist	HIGH recent previous adverse experience	Risk affects a HIGH # of transactions OR a HIGH # of processes and/or systems	A limited # of staff or staff has limited or no competency to manage the risk	Risk mitigation processes are not operating as designed or design is flawed; very limited controls	Systems are not operating as designed or design is flawed; very limited controls	Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a HIGH rate of change over the last 6 months
Medium	Controls are detective but not preventative and there may or may not be effective reporting	MEDIUM recent previous adverse experience	Risk affects a MEDIUM # of transactions OR a MEDIUM # of processes and/or systems	A limited # of staff or staff has moderate competency	Risk mitigation processes are operating as designed, but design can be improved; controls are bolted on top of the process	Systems are operating as designed, but design can be improved; controls are bolted on top of the system	Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a moderate rate of change over the last 6 months
Low	Controls are appropriately preventive and detective and there is effective reporting	LOW recent previous adverse experience	Risk affects a LOW # of transactions OR a LOW # of processes and/or systems	Most staff has high competency	Risk mitigation processes are designed, implemented and operating effectively; controls are embedded in the process	Systems are designed, implemented and operating effectively; controls are embedded in the system	Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a LOW rate of change over the last 6 months

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Prioritize IT risks

Define the IT Risk Assessment Participation Approach

- One-on-one interviews
  - Determine if a a top-down or bottom-up approach is preferred
    - Tier 1 = Executive Management
    - Tier 2 = Senior Management
    - Tier 3 = Line Management
- Surveys
  - An effective way to expand the level of participation beyond interviews
  - Can be used to solicit anonymous input
- Facilitated Workshops
  - May facilitate management buy-in to the risk assessment process
  - Cross-functional workshops may enhance risk assessment comprehensiveness and quality
  - Can be used to expand the level of participation beyond interviews

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Illustrative IT Risk Assessment Summary

IT RISK	Risk Definition	Impact (I)	Overall Impact Commentary	Vulnerability (V)	Overall Vulnerability Commentary
IT Management and Governance	Ensure transparency and understanding of costs, benefits, strategy, policies and service levels. Ensure proper use, controls, and performance of the applications and technology solutions. Ensure IT compliance with laws and regulations.	75	IT Control Environment considerations; high IT spend	50	Management focus on improving capability and maturity
Information Security / Asset Protection	Ensure critical and confidential information is withheld from those who should not have access to it. Ensure automated business transactions and information exchanges can be trusted. Maintain the integrity of information and processing infrastructure. Account for and protect all IT assets. Ensure IT services can properly resist and recovery from failures due to error, deliberate attack or disaster.	90	Data protection and data confidentiality are fundamental to business model and organizational success	75	Prior risk experience indicates a relatively high level of vulnerability
System Development	Define how business functional and control requirements are translated into effective and efficient automated solutions. Acquire and/or develop integrated and standardized application systems.	20	Minimal systems development activities performed	20	Proven track record of success
Change / Problem Management	Maintain integrated and standardized application systems. Ensure minimal impact to business operations.	40	Change control activities affect multiple processes and systems	20	Proven track record of success
Relationships with outsourced vendors	Ensure mutual satisfaction of 3rd party relationships. Ensure satisfaction of end-users with service offerings and service levels.	30	Limited to non-core functions	20	Positive control structure

High (100)

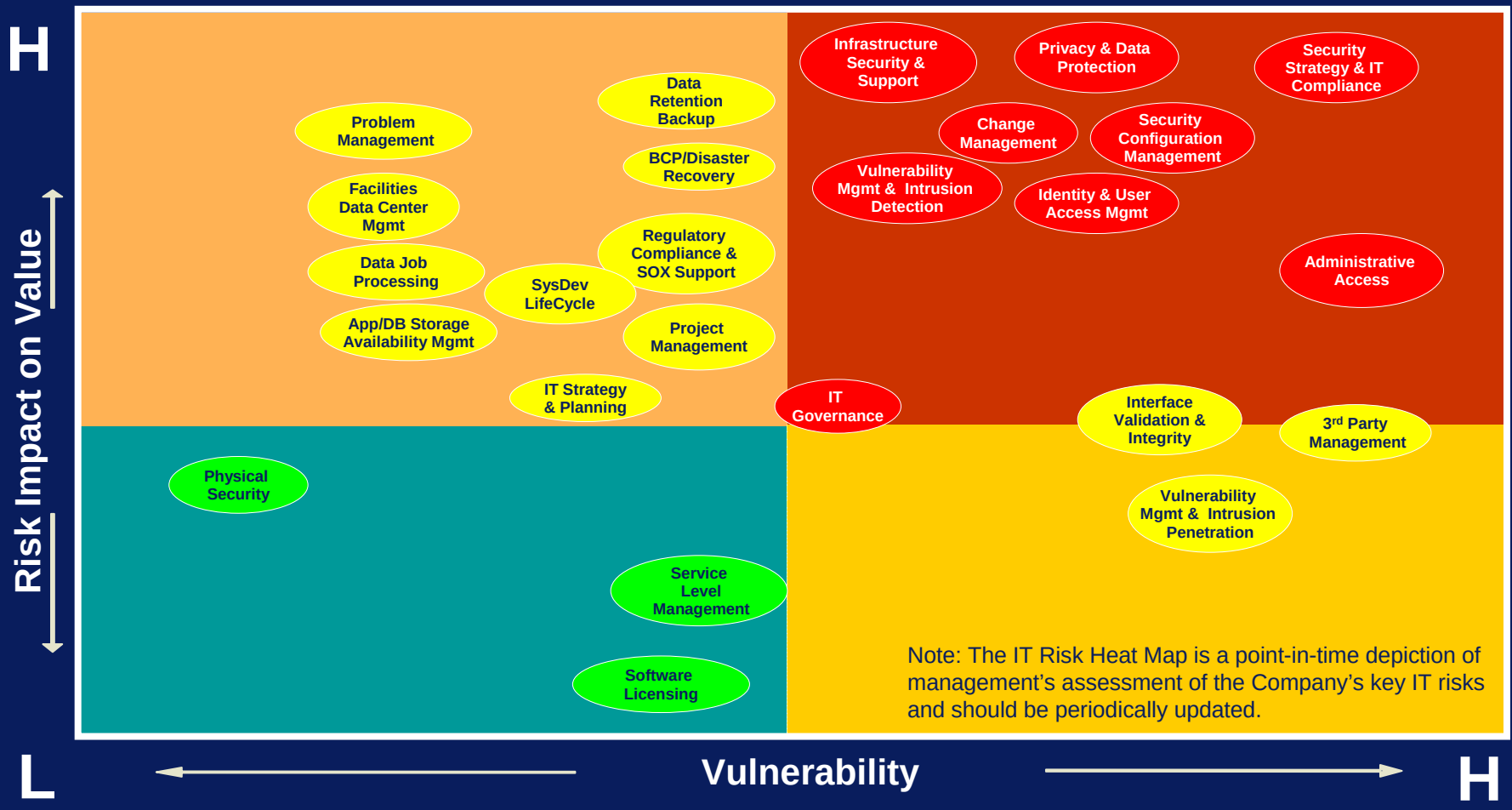
Medium (50)

Low (10)

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Sample IT Risk Heat Map for IT Processes

Based on management's assessment of the key IT risks, the Company's IT risk profile was developed as follows:



Copyright © 2008 Deloitte Development LLC. All rights reserved.

Phase Four: Develop the Risk-Based Internal Audit Plan

Key Activities

- Validate risk assessment results with management
- Map the key risks to business processes and locations (Phase 1)
- Identify risks for Internal Audit focus (to be included in the IA Plan)
- Determine the high level audit approach for risks in the IA Plan

Key Deliverables

- Risks mapped to business processes, locations and key systems
- Risks for Internal Audit focus and IA Plan development
- Risk-based Internal Audit Plan

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Develop risk-based IT internal audit plan

- Identify IT risks for internal audit focus
- Map the key risks to IT processes (IT audit universe)
- Map IT processes to locations and systems to be audited
- Determine the audit approach
- Develop the risk based audit plan

IT risks that do not get selected for IT IA focus and will not be part of the IT IA plan should be addressed by management through a variety of other control activities

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Key IT Risks Mapped to the IT Processes

Sample

Client IT Processes	Primary Risks															
	Problem Management	Security Strategy & IT Compl.	BCP/Disaster Recovery	Reg Compliance & SOX	Physical Security	Privacy and Data Protection	Security Config Management	Change Management	Infrastructure & Security Supp	Project Management	Identity & User Access Mgmt	Vulnerability Mgmt & Intrusion	Administrative Access	IT Strategy & Planning	Service Level Management	System Development Life Cycle
IT Governance																
Governance				X		X								X		
Strategy and Planning		X	X	X		X								X		
IT Processes																
Architecture						X					X	X		X		
Project Management						X				X						
– Project Management Lifecycle						X				X						X
– Project Risk (Pre and Post Imp Review)																X
Applications and Databases																
– Change Management	X						X	X	X	X						X
– Patch and Configuration Management							X	X	X	X	X	X	X			
– Data Quality and Interfaces															X	
Operations																
– Data Processing			X												X	
– Application Management			X												X	
– Database Management			X					X	X						X	
– Storage Management			X						X						X	
– Facilities Management					X	X									X	

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Example #1 – Risks for IT internal audit focus

Illustrative

Risks for IT IA Focus	IT Process(es)	Risk Ranking	General Audit Approach	Corporate Illinois	Texas	Canada	Mexico	Ireland	European Shared Service Center	Italy	France	China
Security Strategy & IT Compliance	Enterprise Security	H	Risk Mitigation				X			X	X	X
Privacy and Data Protection	Enterprise Security	H	Risk Mitigation	X			X		X			X
Infrastructure Security & Support	Enterprise Security Support	H	Risk Mitigation	X								
Security Config. Management	Enterprise Security Architecture	H	Risk Mitigation		X	X		X		X	X	
Change Mgmt	Apps & Databases	H	Risk Mitigation	X			X		X			X
Data Retention Backup	Operations	M	Assurance		X	X	X			X	X	X
BCP/Disaster Recovery	Disaster Recovery	M	Assurance		X	X		X		X	X	X
Regulatory Compliance & SOX Support	IT Governance	M	Assurance	X			X		X			X
Project Mgmt	Project Mgmt	M	Assurance	X			X		X			X
Sys Dev Lifecycle	Project Mgmt	L	Assurance	X	X	X	X	X	X	X	X	X
Physical Security	Enterprise Security	L	Assurance	X					X			

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Example #2 IT – Risks for IT internal audit focus

IT Risk Universe Area	Impact	Vulnerability	Risk Category	Rotation
IT Governance				
IT Governance	H	H	Mitigate	Consult
Regulatory Compliance & Sarbanes-Oxley Support	H	M	Assurance	Annual
IT Strategy & Planning				
IT Strategy & Planning	M	M	Assurance	Every Two Years
Architecture				
Architecture Design and Management	L	H	Cumulative Impact	Annual
Project Management				
Project Mgmt (PMLC)	H	M	Assurance	Annual
Systems Development Lifecycle (SDLC)	H	M	Assurance	Annual
Data Management & Operations				
Data/Job Processing	H	L	Assurance	Annual
App/DB Storage & Availability Management	H	L	Assurance	Annual
Facilities/Data Center Management	M	L	Review Resources	As Needed
Data Retention / Backup	L	M	Review Resources	As Needed
Applications & Databases				
Change Management	H	H	Mitigate	Consult
Data Quality & Integrity	M	H	Mitigate	Consult
Infrastructure Patch Management	M	H	Mitigate	Consult
Interface Validation & Integrity	M	H	Mitigate	Consult
Support				
Problem Management	H	L	Assurance	Annual
Service Level Management	L	M	Cumulative Impact	Every Two Years

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Phase Five: Schedule the Audits and Plan Resources

Key Activities

- Work with the client (CAE) to determine the resource needs (skill sets, tools, competencies) given the risk information for the planned audits
- Allocate resources and schedule the audits

Key Deliverables

- Detailed risk-based internal audit plan showing:
  - linkage of IA projects to the risk assesment process and risk information
  - alignment of resource compentencies to
  - risk focus of the project
  - audit timeline

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Develop the risk response

- Internal audit can respond risks
  - Incorporate areas of risk into the risk-based internal audit plan and performing internal audits to provide assurance to management and the board on the design and operation of controls
    - Validate that reliance on existing controls is warranted
    - Recommend control improvements
  - For areas with higher vulnerability, internal audit can act in a consultative role
    - Advise management on control design
    - Monitor and report on management remediation activities
- Management has the primary responsibility for risk management
  - Perform risk assessment to identify areas of greatest risk
  - Identify and / or develop risk responses – investments, initiatives, strategy, etc.
  - Besides risk response (reactive), management should also define the overall risk management approach (proactive risk identification, classification and risk management)

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Today's Environment

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Common and Emerging IT Risks

“Top 10” IT Risks

- Segregation of Duties
- Project Risk
- Application Configurable Controls
- Administrative Access
- Privacy
- Interfaces and Middleware
- High Availability
- Data Management
- User Provisioning
- Wireless

Source: *Top IT Audit Issues,* Deloitte presentation for The Institute of Internal Auditors, October 24, 2006.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Review of today's discussion

- **Overview: Leading Practice IT Risk Assessment**
- **Performing Risk Assessments for IT**
  - Identifying and Evaluating IT Risks
  - Using IT Risk Frameworks including CobiT
  - Linking IT Risks to Organizational Objective
- **Creating a Risk Response**
- **Common and Emerging IT Risks**

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Contact information

Melissa Bishop
Enterprise Risk Services
San Francisco, CA

Tel: +1 415 783 6380
Mobile: + 1 415 407 5818
msbishop@deloitte.com
www.deloitte.com

Carey Carpenter
Enterprise Risk Services
Honolulu, HI

Tel: +1 808 543 0776
Mobile: + 1 415 602 7605
ccarpenter@deloitte.com
www.deloitte.com

Copyright © 2008 Deloitte Development LLC. All rights reserved.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 135,000 people worldwide, Deloitte delivers services in four professional areas, audit, tax, consulting and financial advisory services, and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu" or other related names.

In the United States, Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 40,000 people in more than 90 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at www.deloitte.com.

©2008 Deloitte & Touche LLP

Member of
Deloitte Touche Tohmatsu