

Deloitte.

Leveraging IT Risk Assessment to Add Value.

Leading Practice IT Risk Assessment

ISACA Honolulu Chapter Luncheon
June 12, 2008

Audit • Tax • Consulting • Financial Advisory.



Leading Practice IT Risk Assessment

The Fine Print

This presentation contains general information only and Deloitte & Touche LLP is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation 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 presentation.

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**

Leading Practice IT Risk Assessment

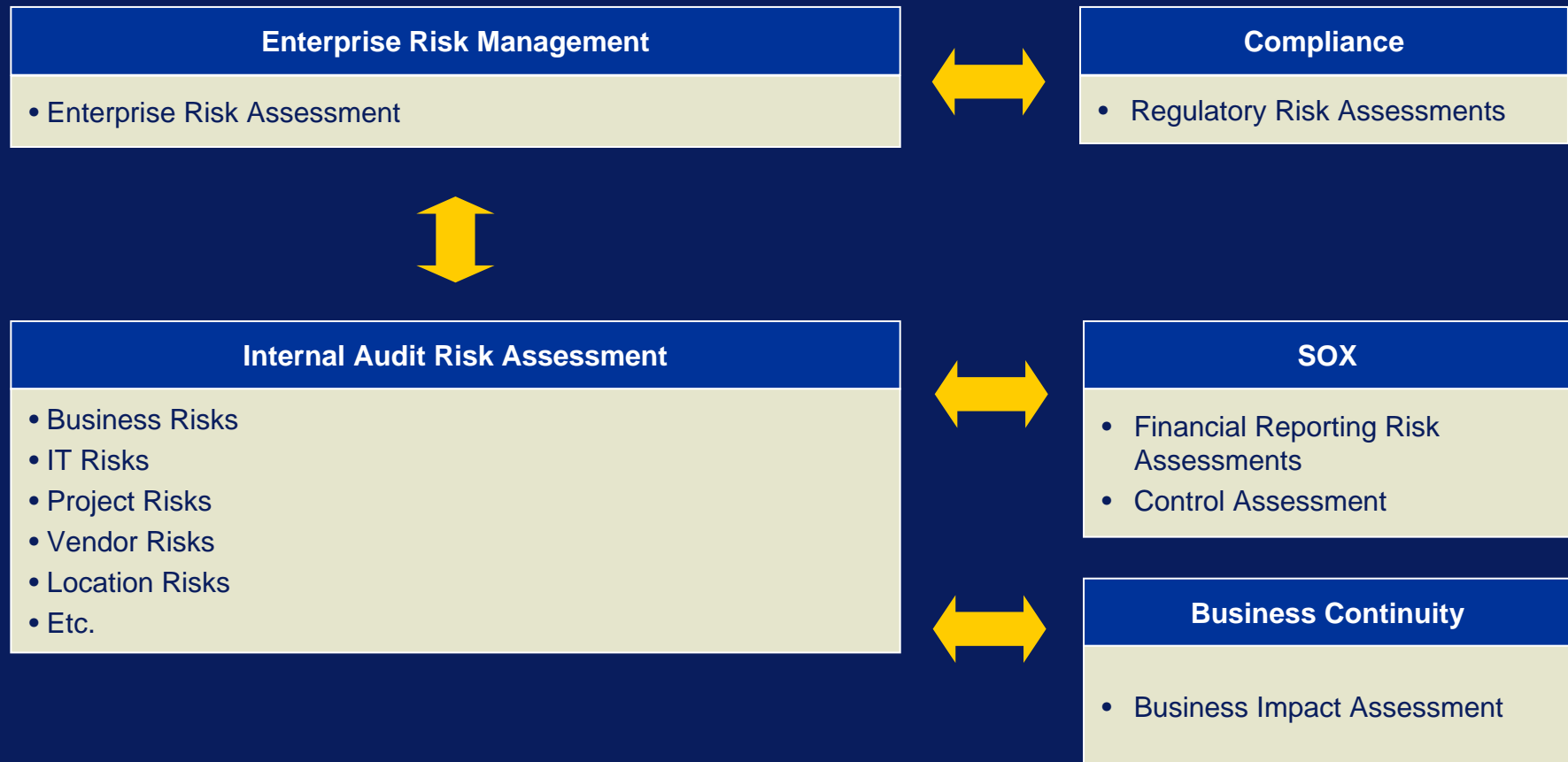
- Organizations are focusing on increasing the cost efficiency of their compliance programs while improving the effectiveness of their governance, risk management and compliance programs.
- In this high pressure business environment, how can IT internal auditors perform risk assessments to ensure that internal audit activities link to business objectives and organizational value drivers?

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

Typical Company Risk Assessment Activities



Evaluating Risk Intelligence

Illustrative



Tribal & Heroic

- Ad-hoc/chaotic
- Depends primarily on individual heroics, capabilities, and verbal wisdom

Specialist Silos

- Independent risk management activities
- Limited focus on the linkage between risks
- Limited alignment of risk to strategies
- Disparate monitoring and reporting functions

Top Down

- 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

Systemic Risk Mgmt.

- 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

Risk Intelligent

- Embedded in strategic planning, capital allocation, product development, etc.
- Early warning risk indicators
- Linkage to performance measurement/incentives
- Risk modeling/scenarios
- Industry benchmarking

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

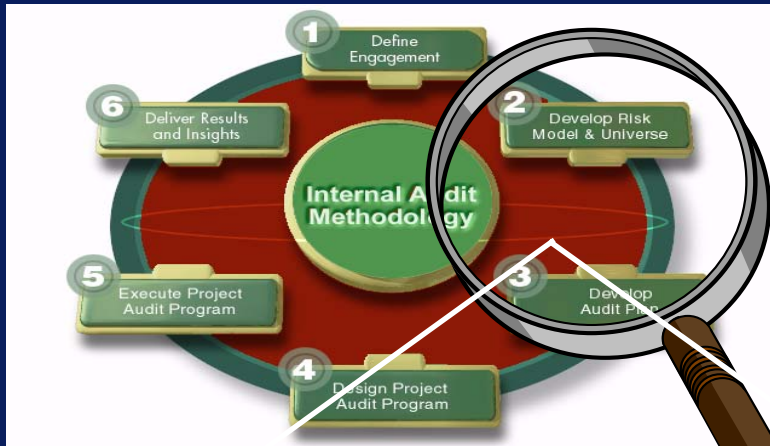
Illustrative



Typical Implications for Internal Audit

<u>Tribal & Heroic</u>	<u>Specialist Silos</u>	<u>Top Down</u>	<u>Systemic Risk Mgmt.</u>	<u>Risk Intelligent</u>
<ul style="list-style-type: none"> • 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 		<ul style="list-style-type: none"> • Leveraged risk identification / assessment • Better coordination with risk owners on risk mitigation efforts and controls 	<ul style="list-style-type: none"> • Linkage of IA risk based audit plan to ERM • Risk owners formulate mitigation • Internal Audit evaluates and monitors 	

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 One: Understand the 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

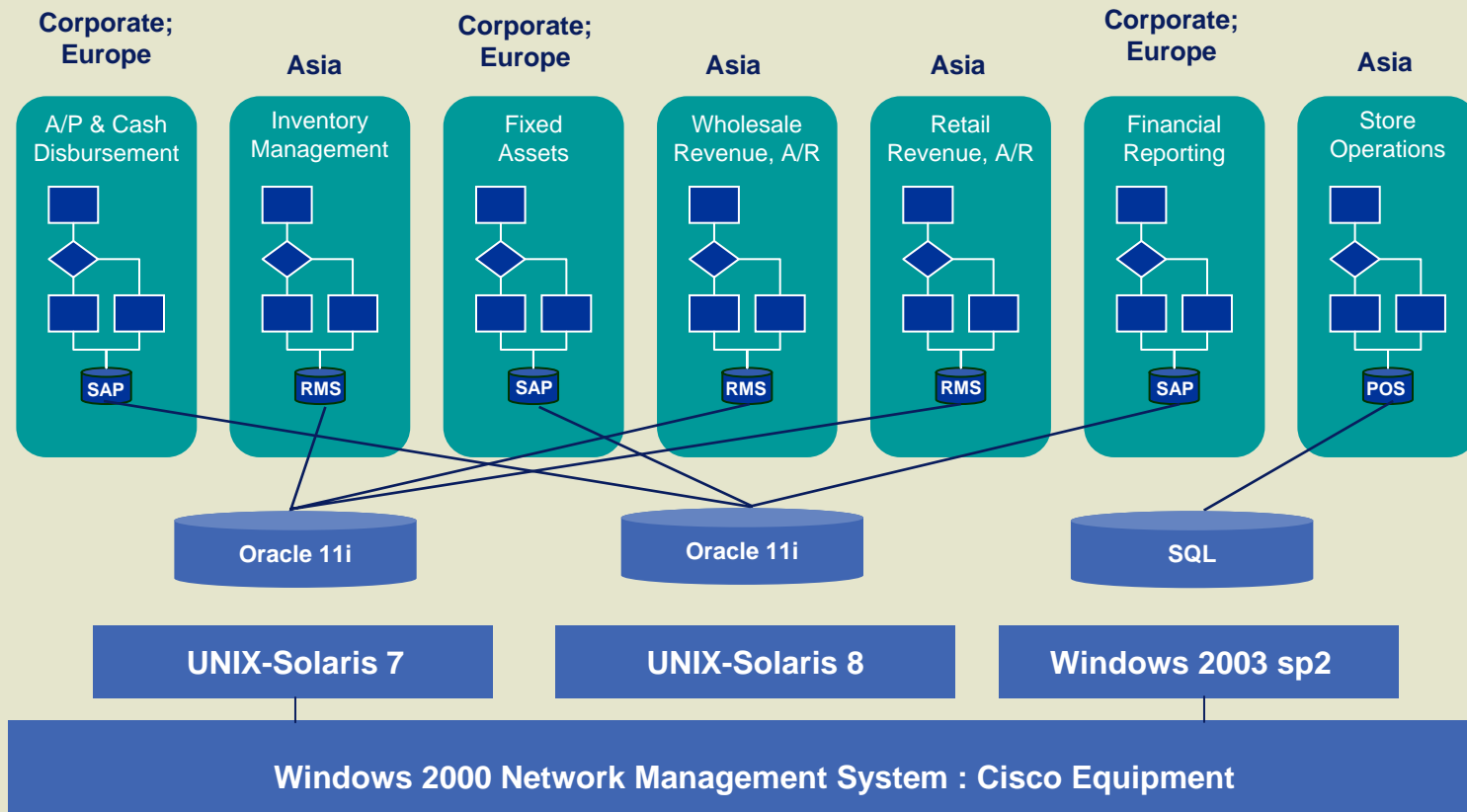
- Company profile
 - Business and IT objectives/strategies
 - Organizational structure
 - Business process, locations and systems
- Preliminary risk information
 - 10-K disclosed risks
 - Other company risk information
 - Key industry issues

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

Business Processes Linked to Information Systems and Locations

Illustrative



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	epa650trafs2	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*

Phase Two: Develop Risk Model



Key Activities

- Develop the IT risk framework:
 - Risk categories framework
 - IT Risk listing with definitions
- Validate the risk framework with key stakeholders

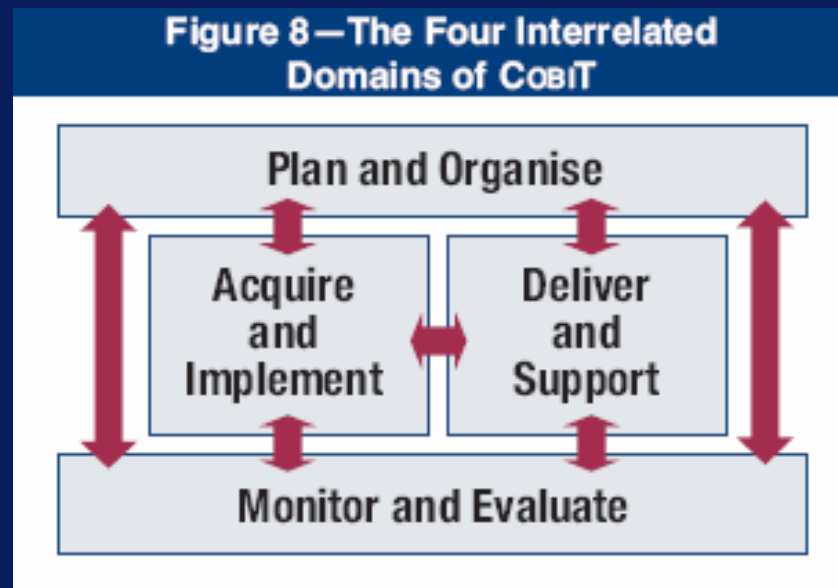
Key Deliverables

- Risk categories framework
 - Governance
 - Strategy
 - Operations
 - Infrastructure
 - External
- IT risk listing with risk definitions

Develop the IT Risk Model

Control Objectives for Information and Related Technology (COBIT®)

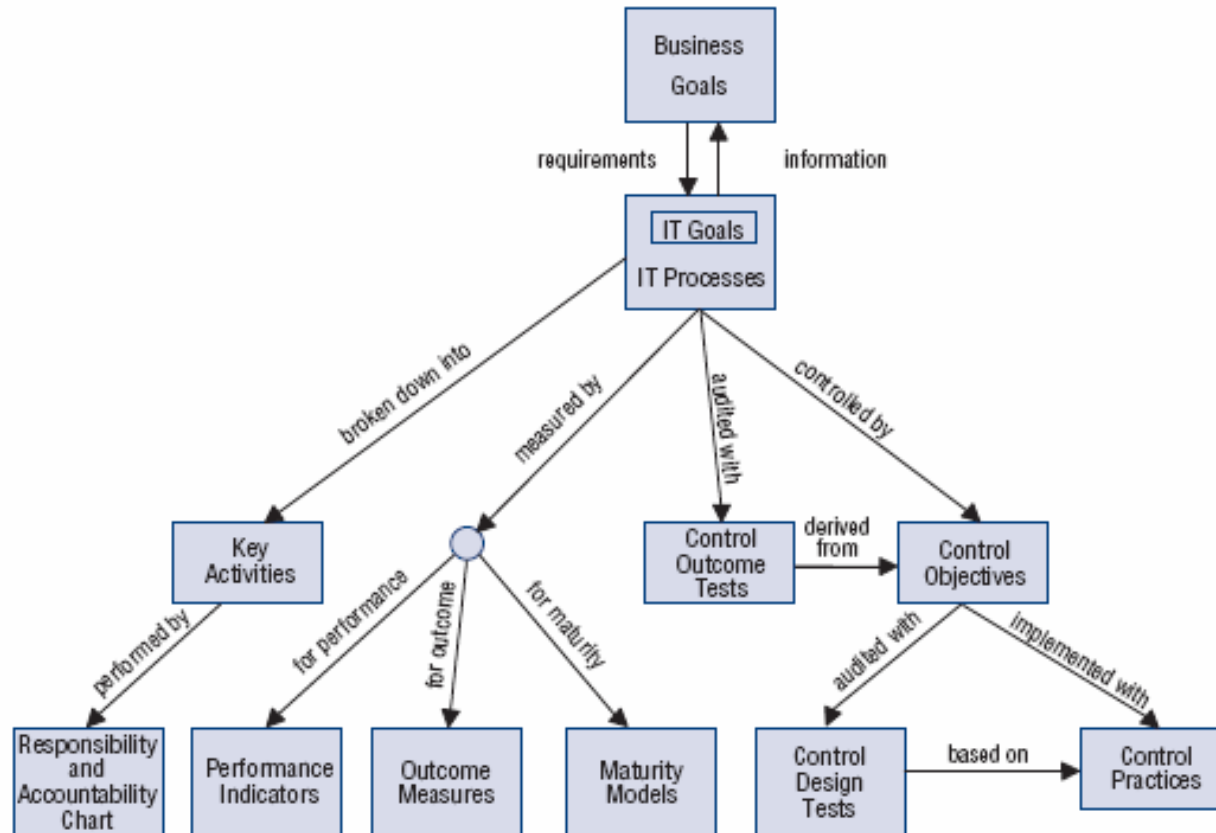
- An IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- Provides good practices across a domain and process framework



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

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.



Deloitte & Touche LLP

IT Risk Framework



Phase Three: Prioritize Risks



Key Activities

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

Key Deliverables

- Risk rating criteria:
 - Impact
 - Vulnerability
- Risk heat map
 - Risks prioritized based on Impact and Vulnerability risk ratings
 - A summary of risk assessment
 - Interview notes

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

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

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

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 from 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

Define Impact and Vulnerability Criteria

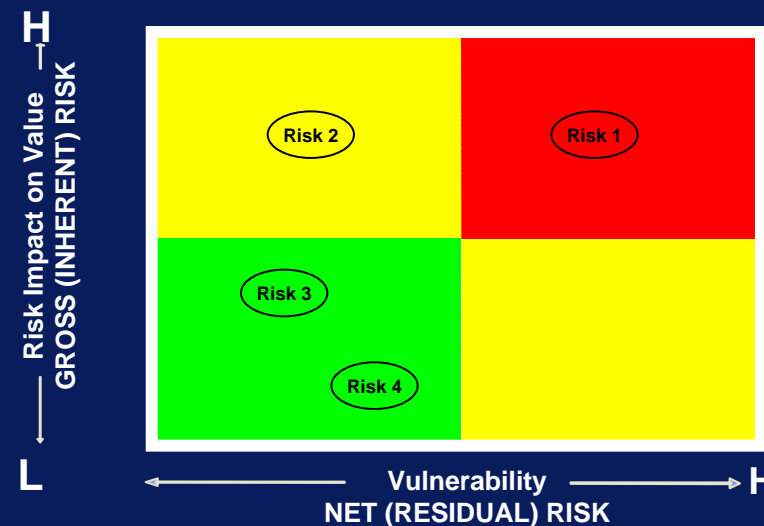
- Impact

- 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:



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

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

Prioritize IT Risks

Define the IT Risk Assessment Participation Approach

- One-on-one interviews
 - Determine if 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

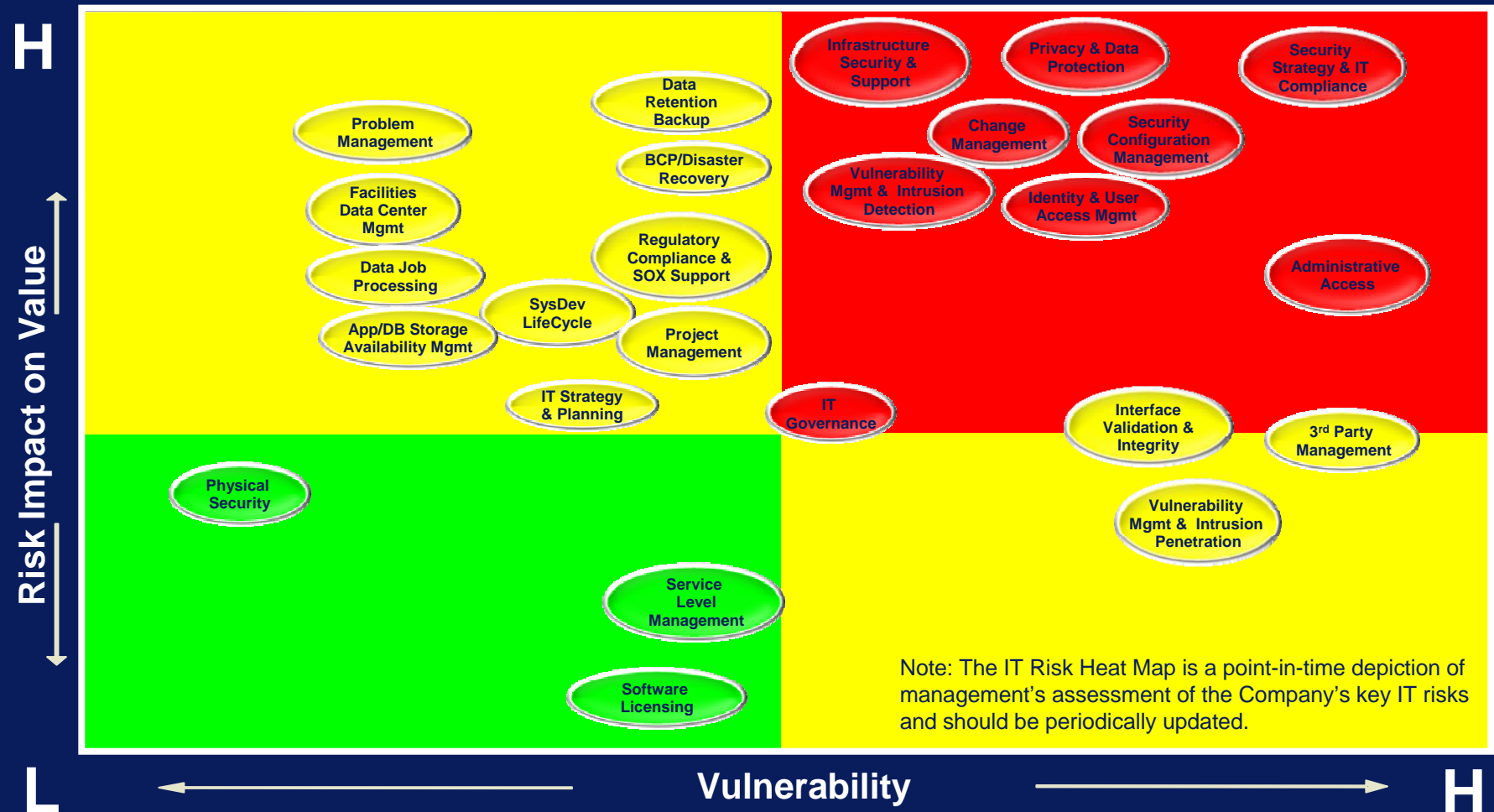
Illustrative IT Risk Assessment Summary

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)

Sample IT Risk Heat Map for IT Processes

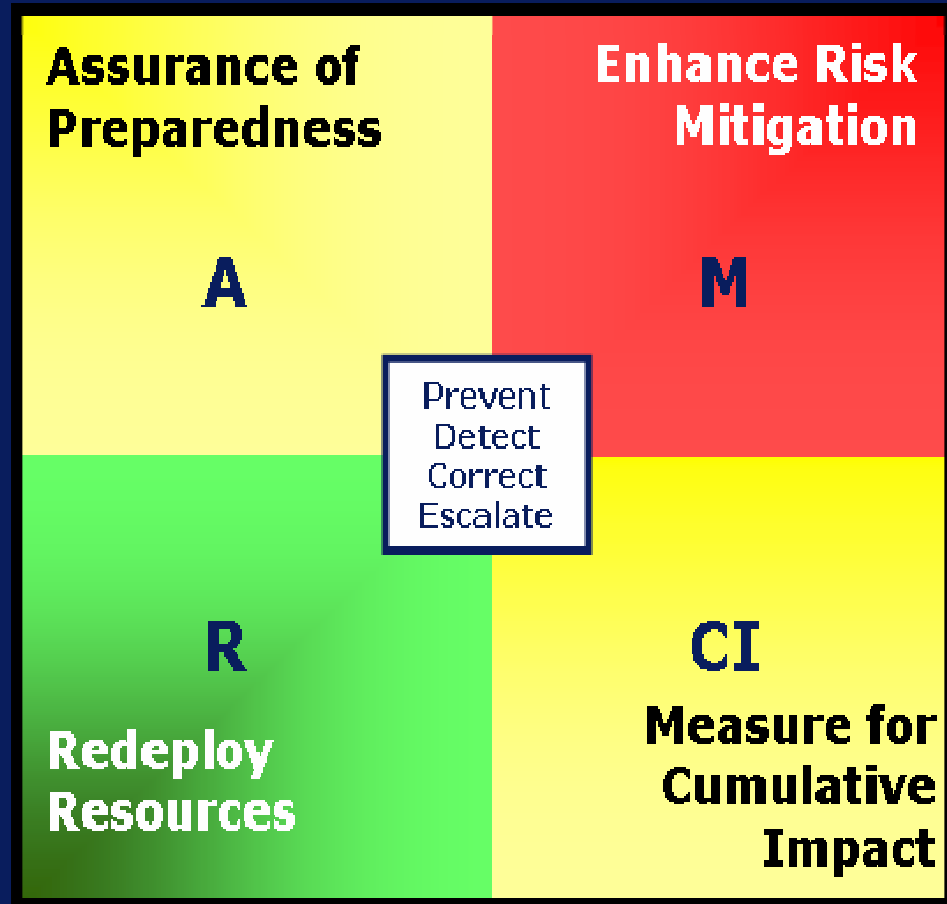
Based on management's assessment of the key IT risks, the Company's IT risk profile was developed as follows:



Prioritize IT Risks Using MARCI Chart

MARCI (Mitigate, Assure, Redeploy and Measure for Cumulative Impact)

The MARCI chart is a graphic tool which helps in plotting the risks' impact and vulnerability scores to assess the appropriate audit approach for auditing the relevant business segment (segment which relates to the risks plotted on MARCI Chart).



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

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

Key IT Risks Mapped to the IT Processes

Sample

Company 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	

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			

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

Phase Five: Schedule the Audits and Plan Resources



Key Activities

- Determine 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 competencies to
 - risk focus of the project
 - audit timeline

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

Develop the Risk Response (cont'd)

- 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)

Today's Environment

TJX credit data stolen; wide impact feared

By Ross Kerber, Globe Staff | January 18, 2007

TJX Cos. yesterday said credit and debit card information from its computer system had been stolen from customers of T.J. Maxx and Marshalls stores. The Framingham retailer, which has more than 2,500 outlets, said it does not know how much data was taken.

Phishing attack plunders employment website

Updated Wed. Aug. 22 2007 6:12 PM ET

BOSTON -- A recently disclosed fraud involving hundreds of people on the Monster.com jobs Web site reveals the plaudits of leaving detailed personal information online, security analysts say. Before the scheme was uncovered last week by researchers at Symantec Corp., con artists had filched legitimate user names and passwords from recruiters who search for job candidates on the site. Then, with access into the Monster.com system, the hackers grabbed e-mail addresses and phone numbers to create e-mail accounts and make them appear to be from Monster.com.

Privacy

Breach At Tech Firm Exposed Data On 27,000 Customers

Technology Daily AM

Assessing the countless corporate security threats

September 17, 2007; 12:19 AM

Malware, carelessness, data leaks--whether internal or external threats, there's too many to count. Defining the most ominous security threat to businesses is difficult, apparently there are just too many to choose from.

At The Security Standard conference held in Chicago, executives and experts took the stage to discuss the countless threats to corporate security.



Microsoft copy protection cracked again

Updated Tue. Jul. 17 2007 8:58 AM ET

Associated Press

SEATTLE -- Microsoft Corp. is once again on the defensive against hackers after the launch of a new program that gives average PC users tools to unlock copy-protected digital music and movies.

ID theft costs banks \$1 billion a year

Report: There's no way to positively identify new customers

By Bob Sullivan

Techn
MSNE

Mar

to id

repo

Whil

atta

Security Fix

Cyber Crime Hits the Big Time in 2006

Experts Say 2007 Will Be Even More Treacherous

By Brian Krebs

washingtonpost.com Staff Writer

Friday, December 22, 2006; 9:51 AM

New HD Format, eBay Fraud, SSN Protection

Readers discuss the HD VMD high-def standard, a recent eBay fraud scandal, and the use of Social Security numbers for identification.

Kellie Parker

PC World

Friday, September 14, 2007; 12:19 AM

There's a new high-def format in town, set to battle Blu-ray Disc and HD DVD: HD VMD. Most of you seem to think that it won't really matter in the format wars. Read the article and then let us know what you think: Can HD VMD beat Blu-ray or HD DVD?

Boomtime for Malicious Hackers

August 06, 2007 -- CSO

Facing a persistent deluge in malicious code, IT security managers are looking for ways to protect their networks.

Offshore Worker Nabbed for Caterpillar Data Theft

17 September 2007

Caterpillar Inc.'s engineering design center

lost 4,000 confidential documents from one of the

employees. A spokeswoman in China confirmed that the incident

occurred in connection with the alleged data theft.

Common and Emerging IT Risks

“Top 10” IT Risks

- IFRS and XBRL (International Financial Reporting Standards and eXtensible Business Reporting Language)
- Embedded Systems
- Green IT
- External Contractors
- Spreadsheets
- Windows Vista
- Anti-Fraud Programs
- Data Management
- Wireless Devices
- FCPA / OFAC (Foreign Corrupt Practices Act and Office of Foreign Assets Control)

Source: *Top 10 IT Audit Risks*, Michael Juergens, at the North America Computer Audit, Control and Security (CACs) Conference, April 28, 2008.

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**

Contact Information

Carey Carpenter

Enterprise Risk Services

Honolulu, HI

Tel: +1 808 543 0776

Mobile: + 1 415 602 7605

ccarpenter@deloitte.com

www.deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2008 Deloitte Development LLC. All rights reserved.

Member of
Deloitte Touche Tohmatsu