



Security & Privacy Services

Risk Management and Risk Catalog

Point of View

Chris Verdon, CISSP, CEH, MCSE

Deloitte & Touche LLP

+1 713 982 4380

cverdon@deloitte.com

Agenda

Risk Management Principles

- Context
 - Assessment
 - Treatment
 - Monitoring
-

Risk Catalog Overview

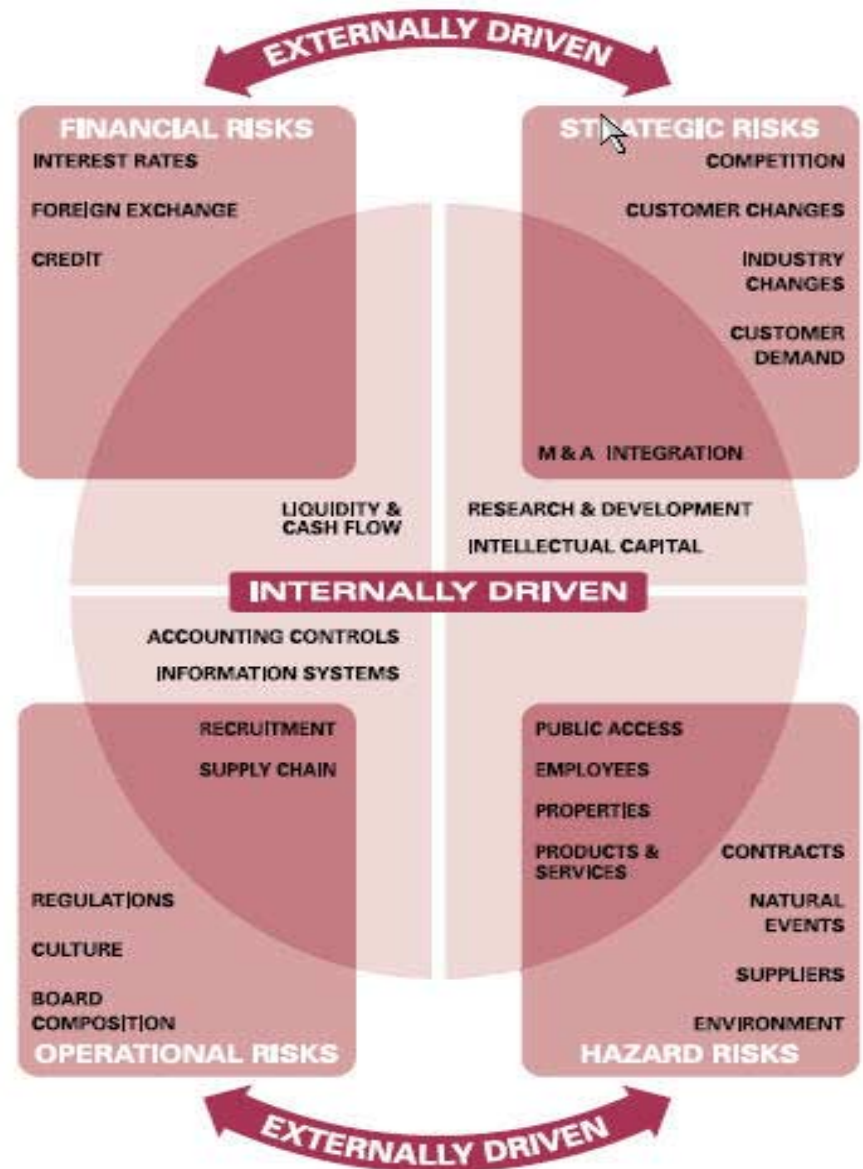
- Drivers
- Solution
- Approach

The background of the slide features a light blue field with several dark blue puzzle pieces scattered across it. The puzzle pieces are of various shapes and sizes, some with tabs and some with blanks, creating a fragmented, interconnected visual theme.

Risk Management Principles

Risk Context

- What is Risk?
 - “Risk can be defined as the combination of the probability of an event and its consequences” [ISO/IEC Guide 73]
 - Likelihood and impact of an event
- Functional Risk Areas
 - The AIRMIC/ALARM/IRM Risk Management Standard states the risks facing an organization and its operations can result from factors both external and internal to the organization.
 - The diagram to the right provides some examples of functional risk areas.



Risk Context

- Authoritative Sources
 - We must work with business groups and legal counsel to identify their authoritative sources as this is the foundation of a successful risk management program (e.g. AICPA Privacy, COBIT, ISO/IEC 17799)
- Risk Methodology
 - Identify what risk management framework to use to structure the risk management program
 - There are many risk management frameworks, including but not limited to the following:
 - ISO/IEC 27001:2005
 - COSO ERM
 - AIRMIC/ALARM/ IRM Risk Management Standard
 - AS/NZS 4360:2004
 - NIST SP800-30
 - All of the frameworks are derived from the basic principle of:
 $\text{Risk} = \text{Likelihood} \times \text{Impact}$

Risk Context

- Control Definitions
 - Individual risk and control requirements are combined to reflect 'integrated requirements'
 - Rationalized controls are designed to reflect the business' decision on how to address the risk and control considerations for a given Test Unit
 - The control design module works through a risk based analysis process that facilitates the control selection for a specific Test Unit by identifying options with associated proposed risks

Risk Assessment - Identify

- Environment Definition (Asset) – anything that has value to the organization [ISO/IEC 27001:2005]
 - Physical assets, Information/data, Software, The ability to provide a product or service, People, Intangibles
- Criticality refers to the availability requirements defined by the business
 - High criticality systems typically have high availability and redundancy requirements
- Sensitivity refers to the confidentiality requirements defined by the business
 - Low sensitivity systems typically have less control requirements

Risk Assessment - Evaluate

Risk Determination

The impact and likelihood can be measured using a combination of qualitative and quantitative factors. The specific criteria will vary for each client and should be defined in conjunction with the clients management.

		Qualitative Impact	Quantitative Impact
Impact	High	Very Bad	> \$100 Million
	Medium	Bad	Between \$1 Million and \$100 Million
	Low	Not So Bad	< \$1 Million

		Qualitative Likelihood	Quantitative Likelihood
Likelihood	High	Very Likely	> Once A Day (0.9)
	Medium	Likely	Between Once A Day And A Month (0.5)
	Low	Unlikely	< Once A Month (0.1)

Risk Assessment - Evaluate

Risk Determination (continued)

The final determination of risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact.

- In this example, the probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low.
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Example Likelihood and Impact Scales			
Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Example Risk Scale: High (50 to 100); Medium (>10 to 49); Low (1 to 10)

Risk Legend



High Risk



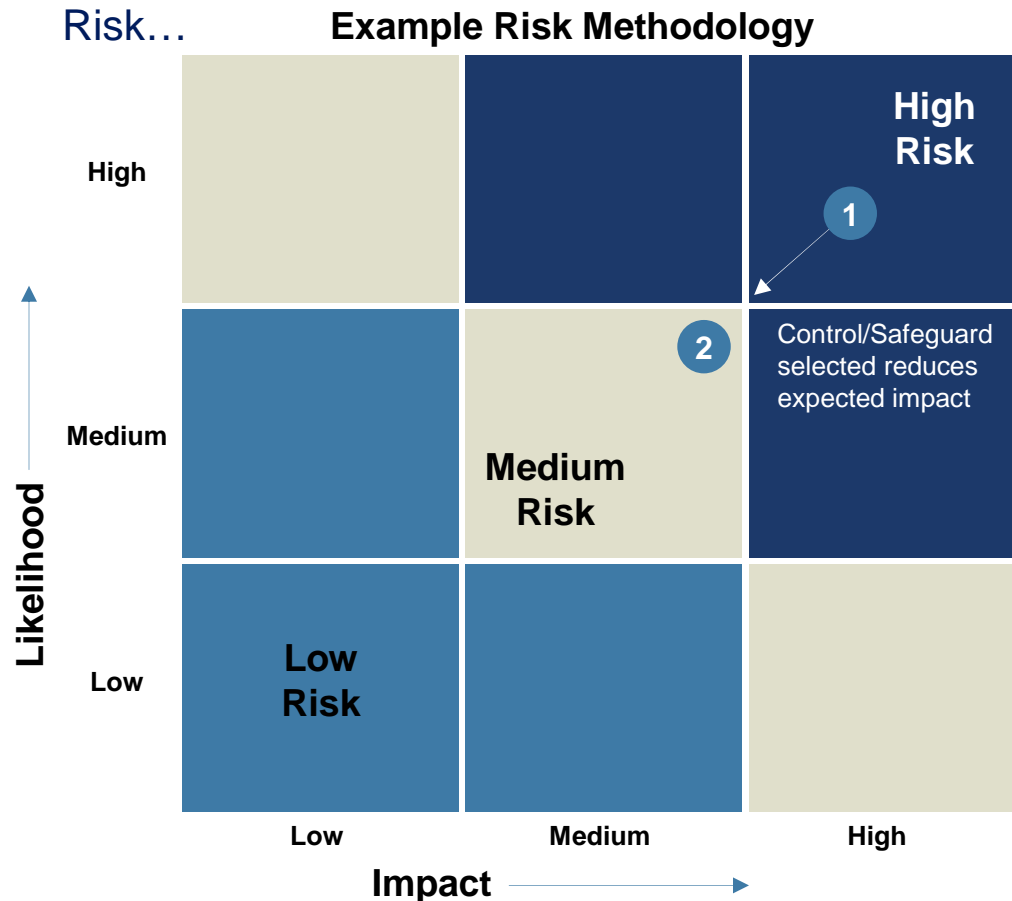
Medium Risk



Low Risk

Risk Treatment – Select Target Risk

A two-pass risk process is used to determine controls: 1) Inherent Risk and 2) Target Risk



- Inherent Risk** is the exposure to organization without control
- Proposed Residual Risk** is the exposure to organization based on the desired control following the cost-benefit tradeoff

Example Impact Scale

High – Greater than \$10M
 Medium – Between \$10M and \$1M
 Low – \$1M or Less

Example Likelihood Scale

High – Once a Month or Greater
 Medium – Between Once a Month and Ten Years
 Low – Once Every Ten Years to Never

...risk tolerance and criteria are calibrated for the business.

Risk Treatment – Select Target Risk

- *Control the Selected Risks*
- Control Baseline Cost Benefit – assess the cost benefit of each control option identified in the ‘risk assessment’ phase
- Strategy / Controls Selection – select the control option that best matches the organizations risk tolerance
- Key Controls – document whether the control option is key to satisfying the control objective; in other words, the control objective would not be met were this control not in place
- Proposed Residual Risk – the level of risk an entity would have if the selected control were implemented and effective (i.e., target risk)

Risk Treatment – Define Test

- Testing Criteria – the attributes of practices and activities that need to be present in order for a control to be deemed operating effectively
- Testing / Review Frequency – based on the inherent risk, automated or manual, and the frequency of control execution, the timing and frequency of how often the control needs to be tested is determined
- Sampling Guidance – based on the population of available examples of the control being performed, the selection requirements are established
- Tailored Test Procedures – the stepwise review, including documentation and evidence requirements, of controls to determine operating effectiveness
- Approved Statement of Applicability – document containing the risks, control objectives, selected controls, and any deviations for a given process or system (i.e., a systems control plan)

Risk Monitoring & Review – Test

- Optimized Sampling – based on sampling guidance, the sampling strategy used for testing
- Risk-based Test Plan – the documentation supporting the controls and test units to be tested which enables auditor reliance on self assessments
- Test Unit Results – the analysis of control design and operating effectiveness based on the testing performed
- Corrective Action Planning – the plan established to remediate any control deficiencies identified during testing
- Actual Residual Risk – the final risk rating based on the results of testing

Risk Monitoring

- Risk & Compliance Monitoring Strategy
 - Risk and compliance is monitored by multiple stakeholders
 - Internal Audit
 - External Audit
 - Third Party
 - Self Assessment, etc.
 - Risk and compliance can be monitored using various techniques
 - Questionnaire
 - Vulnerability Scanning
 - Testing with or without evidence
 - Key Risk Indicator or Key Performance Indicators, etc.
 - Timing of the monitoring varies but needs to be defined
 - Regulatory requirements
 - Types of risks involved (high risk system)

Summary of Methodology

Approach	Risk Context	Risk Assessment			Risk Treatment		Risk Monitoring & Review	
	Establish	Identify	Analyze	Evaluate	Select	Capture	Test	Report
Major Activities	<ul style="list-style-type: none"> • Functional Risk Areas • Authoritative Sources • Risk Methodology • Risk and Control Definitions • Risk and Compliance Monitoring Strategy 	<ul style="list-style-type: none"> • Environment Definition (Asset) • Criticality and Sensitivity • Threat • Vulnerability • Risk Register (Risk Statements) • Owners / Accountability <p>Inherent Risk</p>	<ul style="list-style-type: none"> • Existing Controls Analysis • Likelihood Determination • Impact Analysis • Business Impact Analysis (BIA) 	<ul style="list-style-type: none"> • Risk Determination • Risk Rating • Risk-based Control Baseline Options <p>Assessed Risk</p>	<ul style="list-style-type: none"> • Control Baseline Cost Benefit • Strategy/ Controls Selection • Key Controls <p>Proposed Residual Risk</p>	<ul style="list-style-type: none"> • Testing Criteria • Testing/ Review Frequency • Sampling Guidance • Tailored Test Procedures • Approved Statement of Applicability 	<ul style="list-style-type: none"> • Optimized Sampling • Risk-based Test Plan • Test Unit Results • Corrective Action Planning <p>Actual Residual Risk</p>	<ul style="list-style-type: none"> • Key Risk Indicators • Management Dashboard • Compliance Reporting • Risk Reporting • Ad-hoc Queries

Risk vs. Compliance

- Compliance
 - Measures adherence to internal policies, external regulations, laws, contracts, etc.
 - The compliance criteria needs to be established
 - Compliance is then a measurement of whether you are or are not meeting the established criteria
- Risk
 - Risk may be either good or bad
 - Based on a formal, documented decision process



Risk Catalog Overview

A common understanding

**Business needs a *common* understanding
of risk and corresponding control requirements
between the CFO, Internal Audit, Compliance,
Security, Privacy, Business Continuity, IT Risk
and Third-Parties**

Hard won client insights ...

Root Causes

Conclusions

Organizational functions view the operating environment, risks and controls differently

Higher costs and extra work required for compliance – What is minimum necessary and why?

“Compliance” is confused with “Risk”

Business is often not provided with risk-based options

No single view of the organization’s IT control, security and privacy requirements

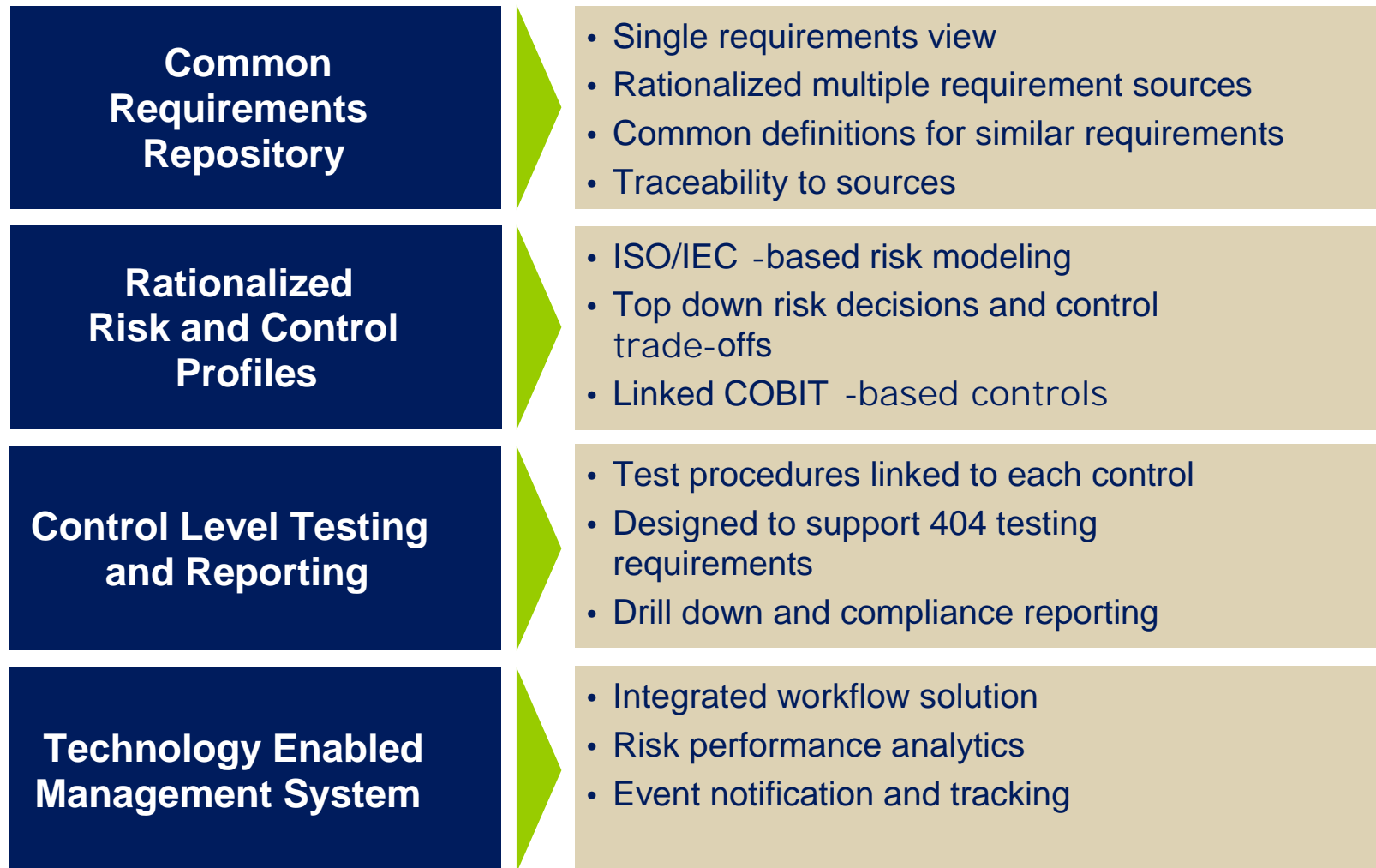
Duplication of effort due to a lack of a single source of business risk and control requirements

Audit, Compliance, Security, Privacy, Business Continuity, IT Risk and Third-Parties use different processes and tools that produce different results

More cost and time are required to de-conflict the standalone processes, tools and data

Hard won client insights...

What is Practical Pain Relief?



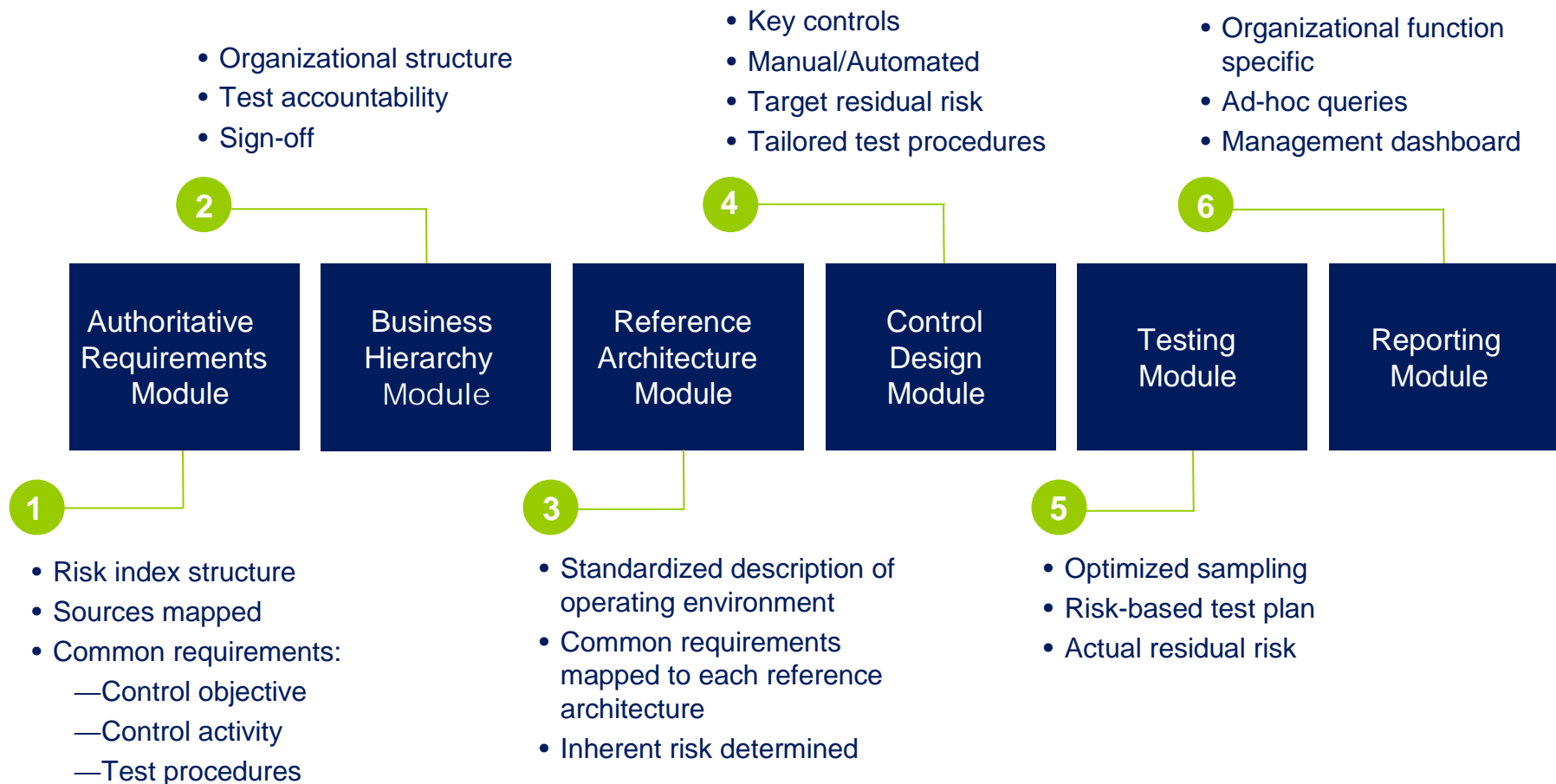
Our Response – Risk Catalog

Risk Catalog – an Integrated Risk Management Solution – provides a risk-driven, workflow solution that allows organizations to define and maintain risk and control profiles for their business systems and processes

Authoritative Requirements	Risk Assessment	Risk Response	Risk Reporting
 Common Repository for all security, IT control, and privacy requirements	 Common Risk Assessment process applied to business	 Linked Risk and Control Profiles for each business operating environment	 Linked Testing and Reporting through key risk and performance criteria

Modular Approach

‘Starter Kits’ jump start the solution implementation



Authoritative Requirements Repository

The screenshot displays the Deloitte Risk Catalog Demo Environment in a Microsoft Internet Explorer browser. The interface includes a navigation bar with tabs for 'My Workspace', 'RCSA Global Planning', 'RCSA Regional Planning', 'RCSA Local Assessment', 'RCSA Monitoring', and 'RCSA Reporting'. A workflow diagram shows five steps: 1. Maintain Authoritative Requirements (highlighted), 2. Rationalize Requirements, 3. Maintain Reference Architectures, 4. Maintain Management Units, and 5. Maintain Business Hierarchy. Below the workflow, a section titled 'Authoritative Requirement Sources: Search Results' displays a table of sources.

Source Name *	Source Type	Source Jurisdiction
12 CFR Part 7 - Bank Activities & Operations, Subpart E - Electronic Activities	Regulation	Global
AICPA/ACA Privacy Framework	Control Practice	Global
American Express	Standard	Global
Bank Holding Companies and Changes in Bank Control 12 CFR 205	Regulation	Global
Bank Holding Company Act	Regulation	Global
Bank Protection Act 12 USC 1862	Regulation	Global
Bank Service Company Act 12 USC 1867	Regulation	Global
Basel Committee on Banking Supervision - International Convergence of Capital Standards (Updated November 2003)	Regulation	Global
BSG 20: Electronic Banking and Electronic Money Activities	Regulation	Global
BSG 78: Electronic Banking Group White Paper: October 2009	Regulation	Global
BSG 78: Electronic Banking Group White Paper: September 2009	Regulation	Global
BSG 82: Risk Management Principles for Electronic Banking	Regulation	Global
BSI 86: Customer Due Diligence for Banks	Regulation	Global
BSI 91: Operational Risk	Regulation	Global
BSI 96: Management and Supervision of Cross-Border Electronic	Regulation	Global

- Business risk requirements
 - Security
 - IT Controls
 - Privacy
 - Other
- Referenced to ISO, COBIT and AICPA
- Overlap removed
- Common definitions

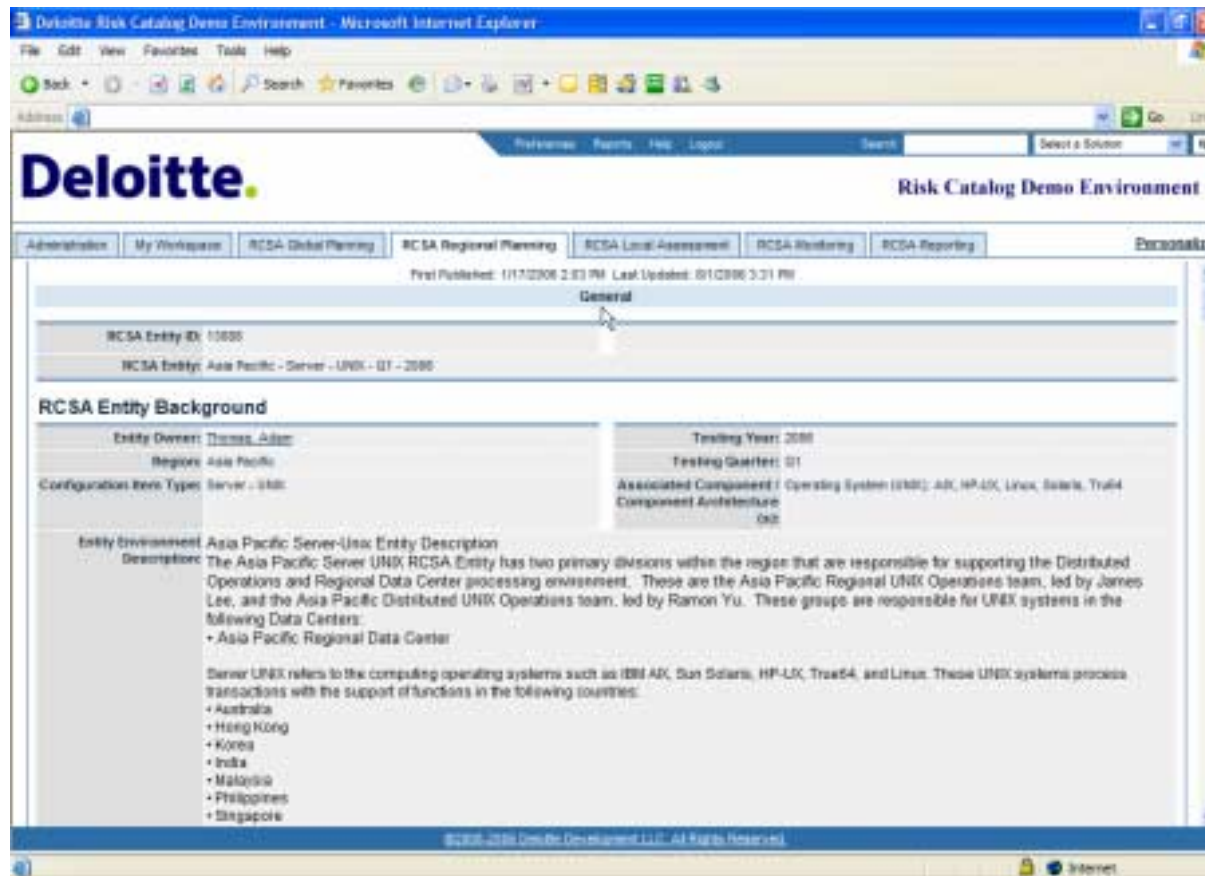
Business Hierarchy Module

The screenshot displays the Deloitte Risk Catalog Demo Environment in a Microsoft Internet Explorer browser. The page features the Deloitte logo and a navigation bar with tabs for Administration, My Workspace, RCSA Global Planning, RCSA Regional Planning (selected), RCSA Local Assessment, RCSA Monitoring, and RCSA Reporting. The main content area is titled 'Regional Entity Planning Search Results' and shows a table of regional entities. The table has columns for Tracking ID, Region, Region Code, Region Head, One Down, Site Name, and Site Code. The data lists various regions in Asia Pacific, including Australia, China, Hong Kong, Indonesia, Korea, Malaysia, Philippines, Taiwan, Thailand, and Singapore, each with a corresponding tracking ID and site code.

Tracking ID	Region	Region Code	Region Head	One Down	Site Name	Site Code
11001	Asia Pacific	1	Jim Yu	Roger Lee	Australia	8
11002	Asia Pacific	1	Jim Yu	Roger Lee	China	9
11003	Asia Pacific	1	Jim Yu	Roger Lee	Hong Kong	1
11004	Asia Pacific	1	Jim Yu	Roger Lee	Indonesia	10
11005	Asia Pacific	1	Jim Yu	Roger Lee	Korea	2
11006	Asia Pacific	1	Jim Yu	Roger Lee	Malaysia	11
11007	Asia Pacific	1	Jim Yu	Roger Lee	Philippines	12
11008	Asia Pacific	1	Jim Yu	Roger Lee	Taiwan	13
11009	Asia Pacific	1	Jim Yu	Roger Lee	Thailand	14
11010	Asia Pacific	1	Jim Yu	Roger Lee	Singapore	4
11011	Asia Pacific	1	Jim Yu	Roger Lee	Singapore	4
11012	Asia Pacific	1	Jim Yu	Roger Lee	Singapore	4

- Models organizational structure
- Tailored to operating environment
- Supports sign-off, accountability and ownership

Reference Architecture Module



Entity Definition

- Establishes standard definition for the operating environment
- Associated with Authoritative Requirements
- Assists with the creation of Sarbanes Oxley (SOX) narratives

Reference Architecture Module

The screenshot displays the Deloitte Risk Catalog Demo Environment in a Microsoft Internet Explorer browser. The interface includes a navigation bar with tabs for 'My Workspace', 'RCSA Global Planning', 'RCSA Regional Planning', 'RCSA Local Assessment', 'RCSA Monitoring', and 'RCSA Reporting'. A process flow diagram at the top shows seven steps: 1. Regional Entity Planning, 2. Define RCOSA Entity, 3. Define RCOSA Entity Risk Requirements, 4. Define RCOSA Entity Risk Assessments (highlighted in blue), 5. Define RCOSA Entity Test Plan, 6. Define RCOSA Entity Risk Responses, and 7. Define Risk & Control Plans.

Below the flow diagram, the 'Associated RCOSA Entity' section shows a table with the following data:

RCOSA Entity	Region	Testing Year	Testing Quarter
Asia Pacific - Server - URGENT - Q1 - 2006	Asia Pacific	2006	Q1

The 'Associated Threat Vulnerability Scenario' section shows a table with the following data:

Common Requirement Name	Threat Vulnerability Scenario
Access Control - User Access Management - User password compromised	Unauthorized users gain access through user accounts based on a password that was disclosed during communication to the authorized users.

The 'Qualitative Inherent Impact Assessment' section shows a table with the following data:

Confidentiality	Integrity
<ul style="list-style-type: none">Contracts (C): Insignificant (1)Financial (C): Fairly Significant (2)Regulatory (C): Very Significant (3)	<ul style="list-style-type: none">Contracts (I): Insignificant (1)Financial (I): Fairly Significant (2)

Risk Assessment

- Standard risk definitions
- Qualitative and quantitative
- Multiple dimensions of risk; e.g.
 - Franchise
 - Contract
 - Regulatory
 - Customer
 - Financial

Control Design Module

The screenshot displays the Deloitte Risk Catalog Demo Environment in a Microsoft Internet Explorer browser. The interface features a navigation bar with tabs for 'My Workspace', 'RCSA Global Planning', 'RCSA Regional Planning', 'RCSA Local Assessment', 'RCSA Monitoring', and 'RCSA Reporting'. Below this is a process flow diagram with seven numbered steps: 1. Regional Entity Planning, 2. Define RCSA Entity, 3. Define RCSA Entity Risk Requirements, 4. Define RCSA Entity Risk Assessments, 5. Define RCSA Entity Test Plan, 6. Define RCSA Entity Risk Responses, and 7. Define Risk & Control Plans. Step 7 is currently selected and highlighted in blue. The main content area shows details for Step 7, including a 'Baseline Control Objective', 'Baseline Control Activity', 'Implemented Controls', and 'Baseline Test Procedures'. The 'Baseline Control Objective' states: 'Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.' The 'Baseline Control Activity' describes a formal management process for password allocation and validation. The 'Implemented Controls' section lists various security measures, including user account information, password management, and encryption. The 'Baseline Test Procedures' section provides a list of steps for testing the password management process, including verifying documentation, user requirements, and evidence of compliance.

- Documents implemented controls and reasoning
- Links risk and control trade-offs and decisions
- Tailors baseline test procedures to implemented controls

Testing Module

Deloitte Risk Catalog Demo Environment

Navigation: Home | Reports | Help | Logout | Search | Select a Scenario

Subnavigation: RCSA Global Planning | RCSA Regional Planning | RCSA Local Assessment | RCSA Monitoring | RCSA Reporting | Personal

RCSA Entity Test Execution: 00852

First Published: 2/21/2006 2:34 PM | Last updated: 9/6/2006 2:22 PM

Test Execution ID: 00852

Component Information

Site & OU Information

Tracking ID	Region	Region Code	Site Name	Site Code	Operational Unit Name	OU Code	Functional Element
00852	Asia Pacific	1	Asia	T	Asia	01	Element: Local Administration

Location: DUF Square
 Component Name: Avaya CRS
 Primary Contact: Rural
 Justification: Justification - Call Center Management System for Critical Call Center

Component Type: Call Center Management Systems - Agents
 Criticality: High

Associated Risk Assessment & Response

Risk Assessment ID	Threat/Vulnerability Scenario	Baseline Control Objective	Baseline Control Activity	Test Procedure
00852	Unauthorized access is gained through diagnostic and configuration network ports.	Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.	Physical and logical access to diagnostic and configuration ports are controlled (JUNIC, ITTTS (2005) Part 11, Remote activation is performed over an encrypted channel with a secure client & strong authentication (PFBC in formal Security and Disclosure).	1. Select a sample of Voice systems within the region. 2. For each of the selected Voice systems, confirm that logs are maintained that indicate when modem ports are enabled and control center user management approval.

Test Results

Test Results:

1. Selected a sample of systems within the testing location, DUF Square.
2. Obtained technical specification documentation on the configuration of the diagnostic and configuration access ports. Provided as evidence, Secure Build AV.
3. Verified that diagnostic and configuration access ports have access listed as defined in the documentation. Provided configuration files in screen shots as evidence.
4. Verified that remote administration is performed with a secure client using strong authentication mechanisms.
5. Verified that all remote and administrative access is encrypted. Sniffed the air and showed encrypted tunnel.

Result: Effective

Test Evidence

Name	Size	Type	Default Date
Secure Build AV.doc	25 KB	Word Document	9/6/2006 9:47 AM
Secure Build Evidence.doc	25 KB	Word Document	9/6/2006 9:47 AM
Secure Build Evidence.doc	25 KB	Word Document	9/6/2006 9:48 AM
Screen shot 1.jpg	2724 KB	Image	9/6/2006 9:38 AM

Evidence Tracker: Sign-off: I certify that the test was completed and the results and evidence are true and correct for the test dated above.
 Sign-off Name: Douglas, David

© 2006 2006 Deloitte Development LLC. All Rights Reserved.
 90000 2006 Security Development LLC. All Rights Reserved.

- Traceability
- Sampling
- Clearly defined test procedures
- Captured evidence

Testing Module

Deloitte Risk Catalog Demo Environment - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

https://rc.deloitte-ebc.com/frameset.asp?sessionToken=3D48AC950330A3D119B2CC41D819CBA1&workspaceId=&requestUri=

Deloitte Risk Catalog Demo Environment

Administration My Workspace RCSA Global Planning RCSA Regional Planning RCSA Local Assessment RCSA Monitoring RCSA Reporting Personalization

RCSA Entry Risk Assessment & Response: 25840

New Copy Save Apply View Delete

Export Post Email

Risk Assessment Risk Response Regional / Dept Manager Sign-off Residual Risk Determination

Quantitative Inherent Impact

Based on Financial Impact (\$ Mil):

Inherent Loss Probability

Inherent Loss Probability: Medium Edit

Impact: Yes Edit

History: Yes Edit

Inherent Risk Loss (\$ Mil):

Inherent Risk Rating

Inherent Risk Rating: Medium Edit

Impact Financial Reports: No Edit

Select Impacts Financial Reports: Yes Edit

Submit

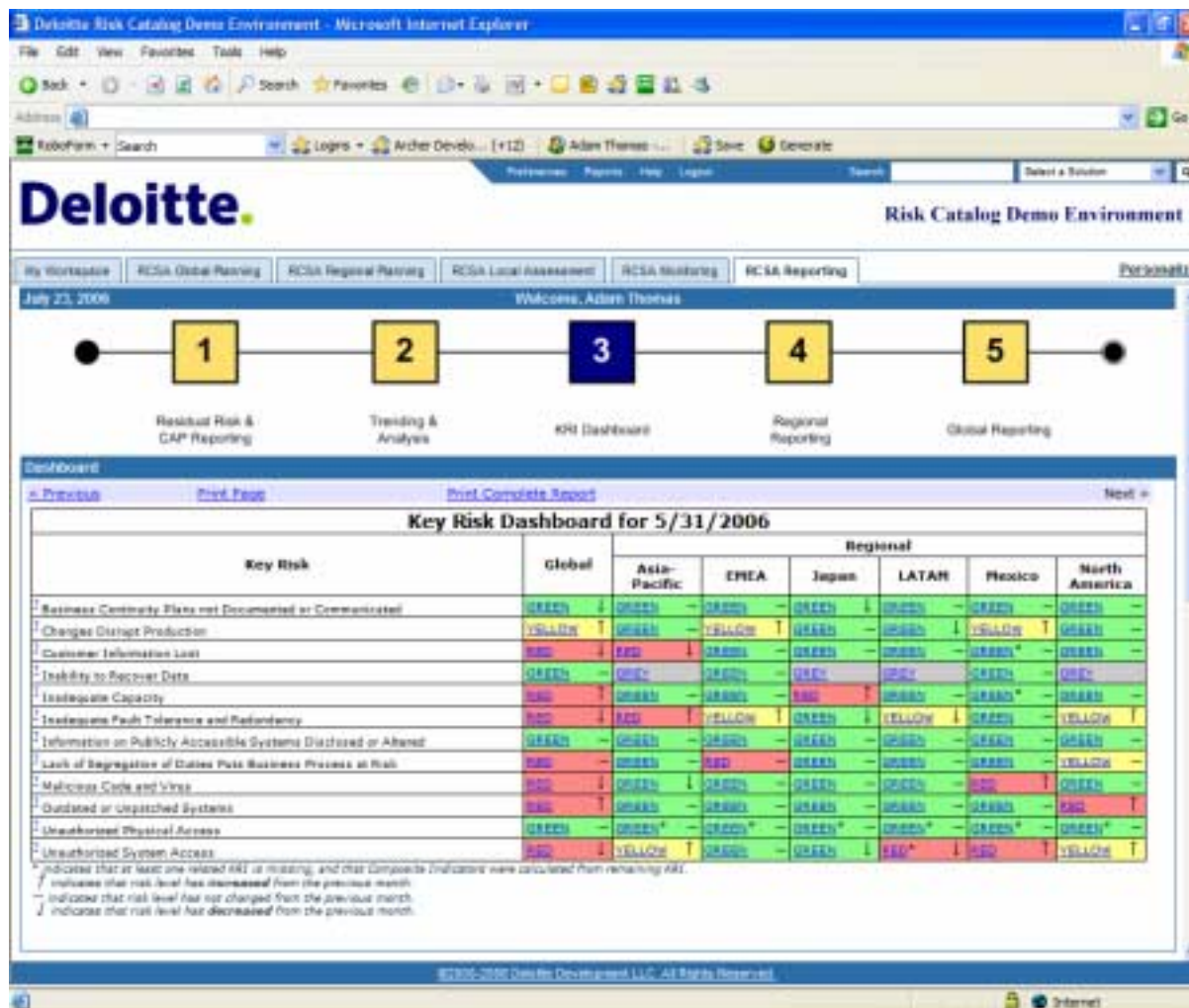
Subsequent Risk Rating: Low Edit

© 2006-2009 Archer Technologies. All Rights Reserved.
© 2003-2006 Deloitte Development LLC. All Rights Reserved.

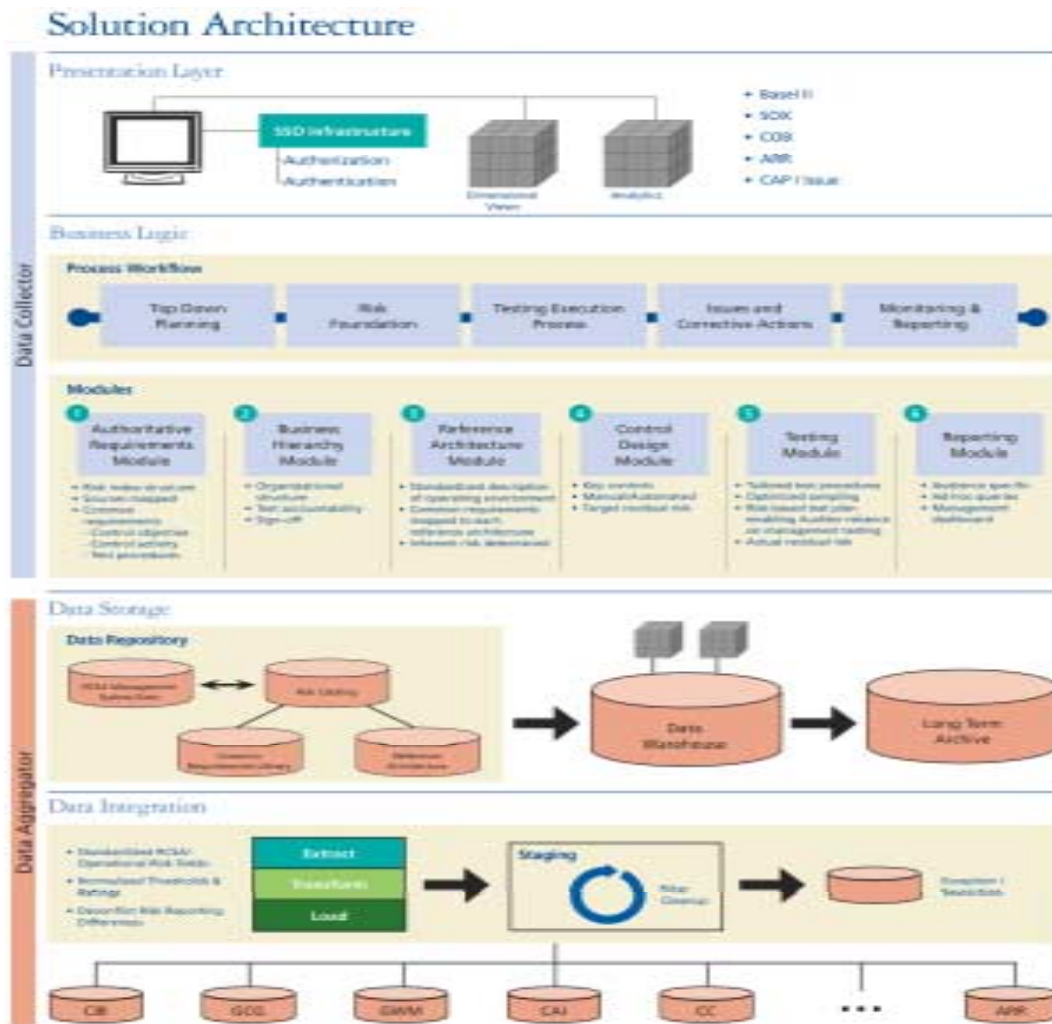
- Supports tracking SOX 404 IT controls
- Each risk and control can be tagged by the client as to whether or not they impact financial reporting

Reporting Module

- Drill down reporting
- Compliance and risk monitoring
- Top down “Key Risk” management
- Trending

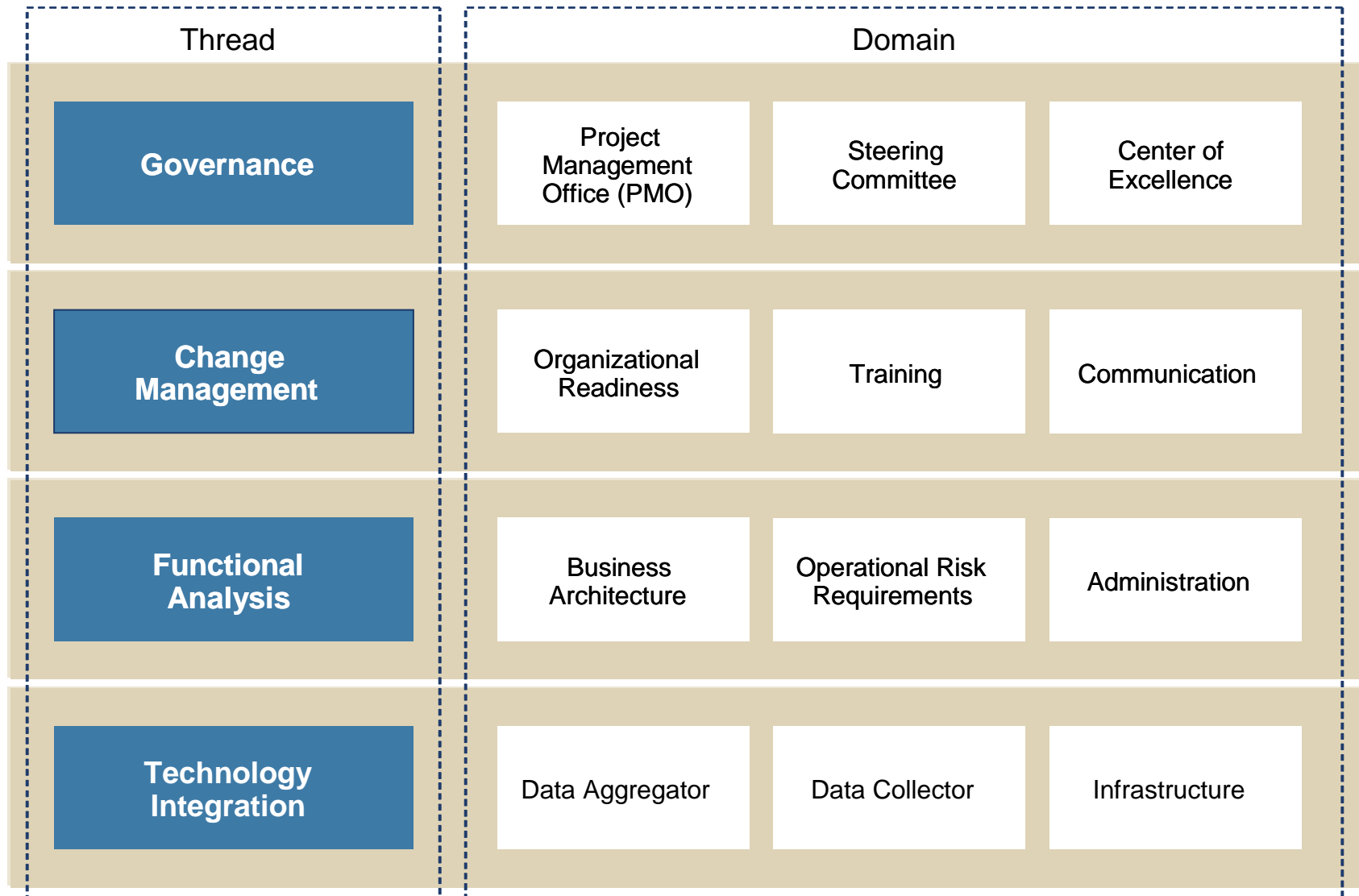


Risk Catalog Management System



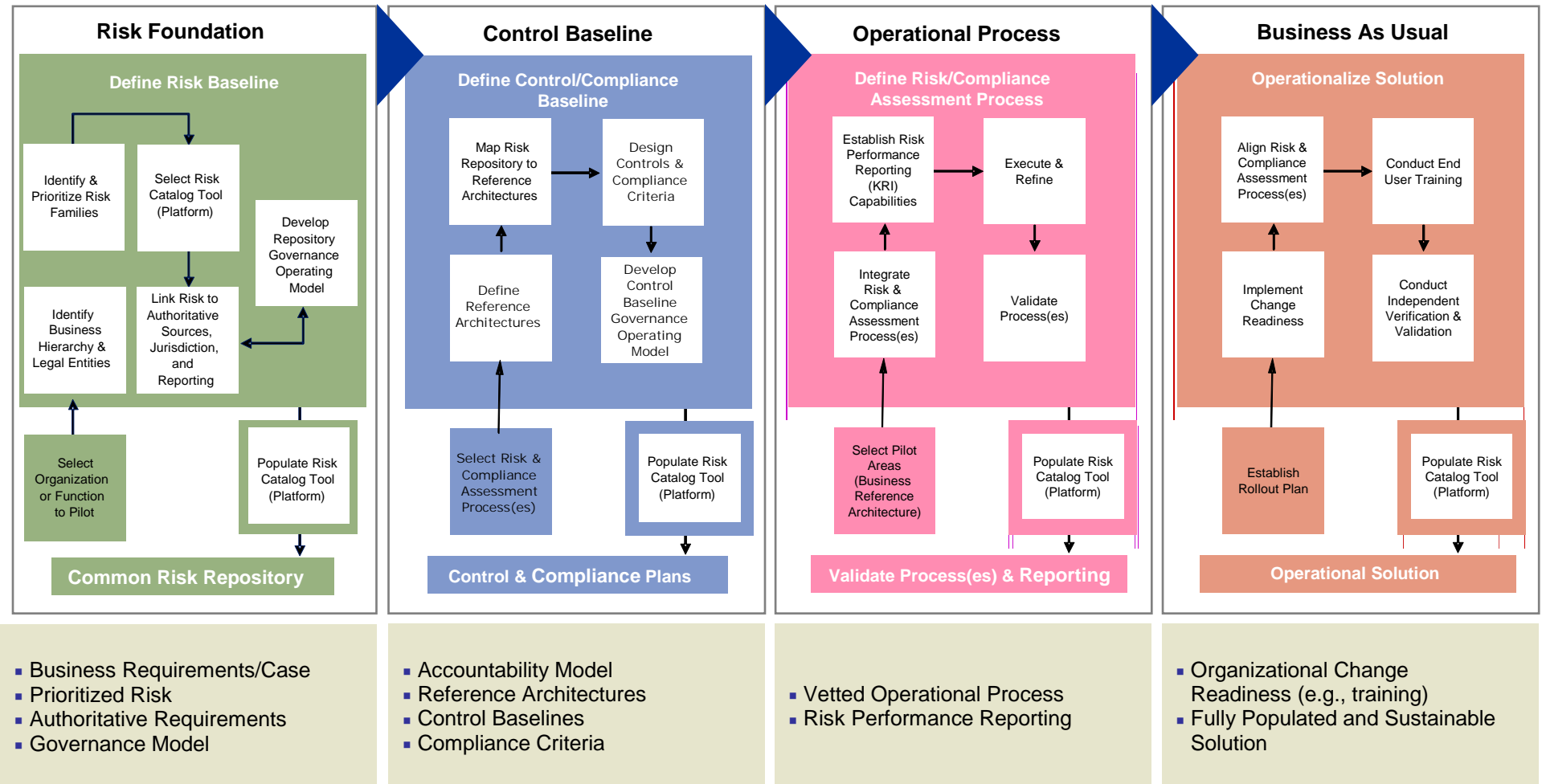
- Workflow enabled
- Event notification
- Database managed vs. spreadsheets
- Single management view
- Rapid reporting and trending

Risk Catalog Delivery Framework



Implementation Roadmap

Incremental Deployment Achieving Incremental Value



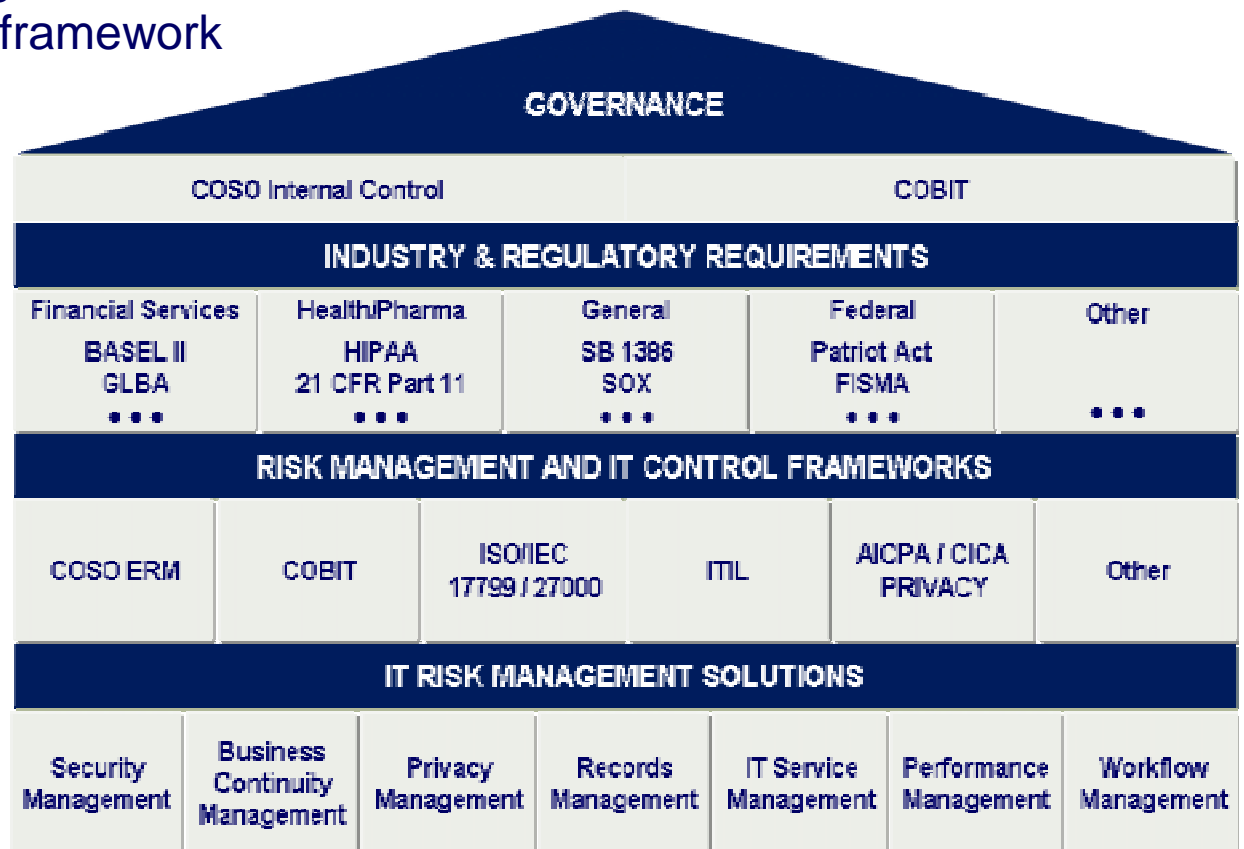
Adaptable to an Organization's Foundation

Different components of Risk Catalog are able to support an organization's overall risk management framework

Authoritative Requirements in a Common Repository

Risk Rationalized Controls for the Entire Business Operating Environment

Testing and Reporting Capability





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 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas, audit, tax, consulting and financial advisory services, and serves more than one-half 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 US, Deloitte & Touche USA LLP is the US 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 US member firm are among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through nearly 30,000 people in more than 80 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 US member firm's web site at www.deloitte.com/us.

Copyright © 2006 Deloitte Development LLC. All rights reserved.

**Member of
Deloitte Touche Tohmatsu**