Deloitte.

Operationalising Risk Management & Compliance Framework

Tracy Michael G. Tantoco
Enterprise Risk Services

Enterprise Risk Services
May 2011

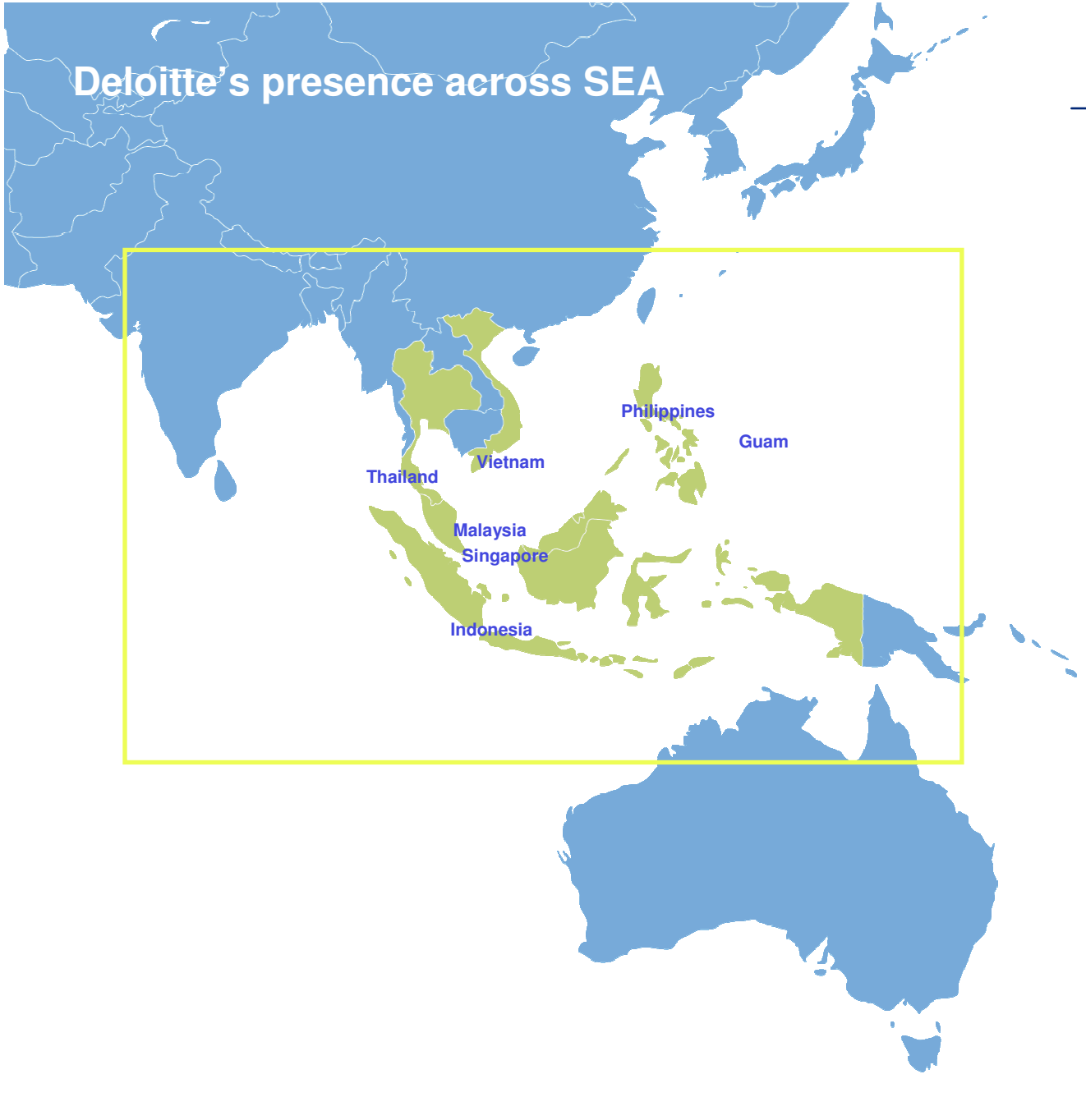
Agenda

1. Introduction
2. Deloitte's Risk Intelligence Program
3. Deloitte's Risk Platform

© 2011 Deloitte Touche Tohmatsu Limited

Extensive Industry Experience and Recognition

Deloitte's presence across SEA



Deloitte's service offering

Consulting
- Corporate Strategy
- Channel Strategy
- Strategic cost reduction
- Operational Excellence
- Outsourcing/Off-shoring Advisory
- Human Capital
- Technology Integration
- Enterprise Applications

Audit
- Conversion Services
- Environment & Sustainability
- Legal and Regulatory Consulting

Corporate Finance
- Financial Advisory
- Forensic Services
- Reorganization Services
- Valuation Services

Tax
- Corporate Tax
- International Tax
- R & D Credits
- Mergers & Acquisitions
- Transfer Pricing

Enterprise Risk Services (ERS)
- Information Technology Risk
- Business Risk

© 2011 Deloitte Touche Tohmatsu Limited

Overview – Risk Management Services and Solutions

Service Lines	Service Areas	Service Offerings
Business Risk	Contract Risk & Compliance	Business Relationship Management; Customer Relationships Risk & Compliance; Joint Venture, Alliance, & Other Relationships Risk & Compliance; Vendor Relationships Risk & Compliance
	Governance, Regulatory, & Risk Strategies	Enterprise Risk Management; Governance; Regulatory & Compliance
	Internal Audit	Internal Audit Projects; IT for Internal Audit; Outsourcing, Cosourcing, or Loaned Staff; Quality Assessment Review; Regulatory Effectiveness Testing; Risk Assessments;
	Sustainability & Climate Change Risk Services	Accounting, Reporting, & Disclosure; Controls Implementation; External Assurance; Governance & Strategy; Internal Assurance; Risk Assessments
Information & Technology Risk	Data Risk Services	Data Analytics; Data Conversion & Integration; Data Governance; Data Quality
	Information & Controls Assurance	Controls Transformation; Integrated External Audit; ISO; Third Party Reporting
	Risk Management Technologies	Capital Market Systems; Integrated Financial Risk Systems
	Security, Privacy, & Resiliency	Application Integrity; Cyber Security; Identity & Access Management; Operational Resiliency; PCI DSS; Privacy & Data Protection; Security Management & Transformation; Security Operations
	Technology Risk & Governance	GRC Systems Implementation & Integration; Independent Validation & Verification; IT Asset Management; IT Governance & Risk

© 2011 Deloitte Touche Tohmatsu Limited

Deloitte has been recognized as a leader in Risk Management Consulting

"Deloitte operates the world's largest and most robust risk consulting practice. Its offerings stretch across every segment of the market."

"Deloitte operates a more robust offshore operation than many of the other leading risk consulting providers."

Kennedy Information; "Risk Management Consulting Marketplace 2009-2012"

Forrester Wave™: Information Security and Risk Consulting , Q3 2010

"In Forrester's 75-criteria evaluation of information security and risk consulting service providers, we found that Deloitte led the pack because of its maniacal customer focus and deep technical expertise."

Forrester Wave™: Information Security and Risk Consulting, Q3 2010

Deloitte's Risk Intelligence thought leadership campaign was recently awarded the Gold Award for the IT Services Marketing Association's (ITSMA) Marketing Excellence Awards for Thought Leadership Marketing.

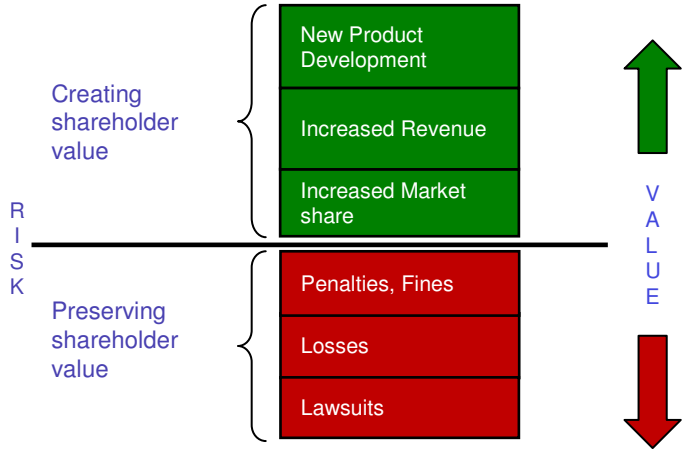
© 2011 Deloitte Touche Tohmatsu Limited

Deloitte's Risk Intelligence Program

The need for Risk Intelligence

Protecting and creating value

- Marketplace demand for board and executive accountability is intensifying
- Companies that do not effectively manage risk are being penalized by the capital markets
- Costs associated with managing risk and compliance activities are increasing



Managing in volatile times

- The recent financial crisis proves that even in a highly regulated environment, lack of effective risk management practices can have a major impact on organizations
- There is increased focus on timely and clear communications with stakeholders on how risks are being managed (board of directors, executive management, employees, bond rating agencies).
- Systemic risks and impacts on organizations have lead to significant losses in value.
- Trending for assessing future market demands and economic impacts is no longer reliable

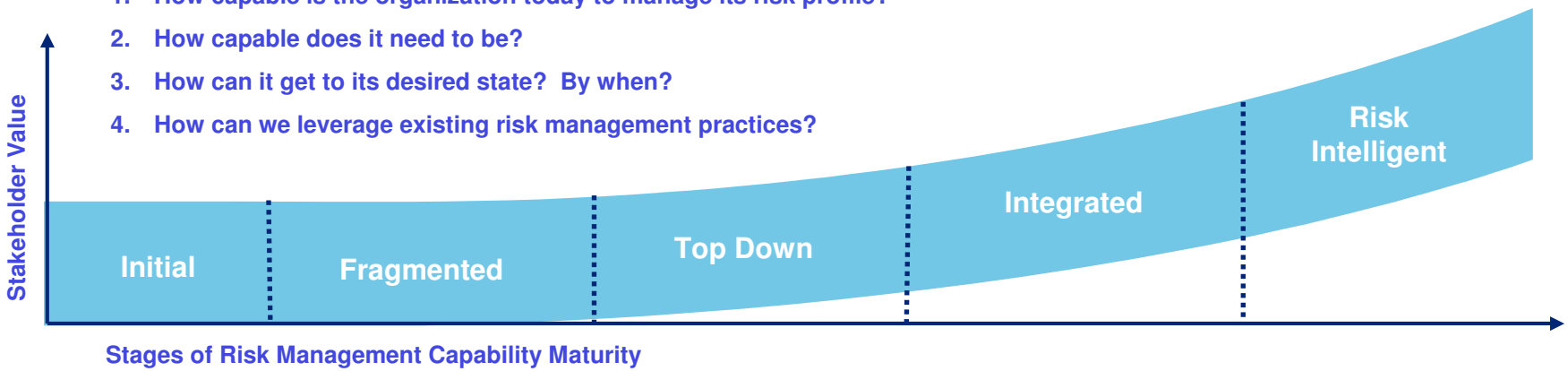
Regulatory complexity

- Regulatory bodies and rating agencies have made it clear that greater disclosure lies ahead, guided by more specific requirements
- Regulatory examinations will most likely change, with increased focus on risk management oversight
- Global regulations are increasing in volume and complexity, increasing the importance of compliance and risk management

© 2011 Deloitte Touche Tohmatsu Limited

Assessing the maturity of risk management capabilities at an enterprise

1. How capable is the organization today to manage its risk profile?
2. How capable does it need to be?
3. How can it get to its desired state? By when?
4. How can we leverage existing risk management practices?



Representative Attributes Describing Each Maturity Level				
Initial	**Fragmented**	**Top Down**	**Integrated**	**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 & 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 management 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 discussion is embedded in strategic planning, capital allocation, product development, etc. • Early warning risk indicators used • Linkage to performance measures and incentives • Risk modeling/scenarios • Industry benchmarking used regularly

© 2011 Deloitte Touche Tohmatsu Limited

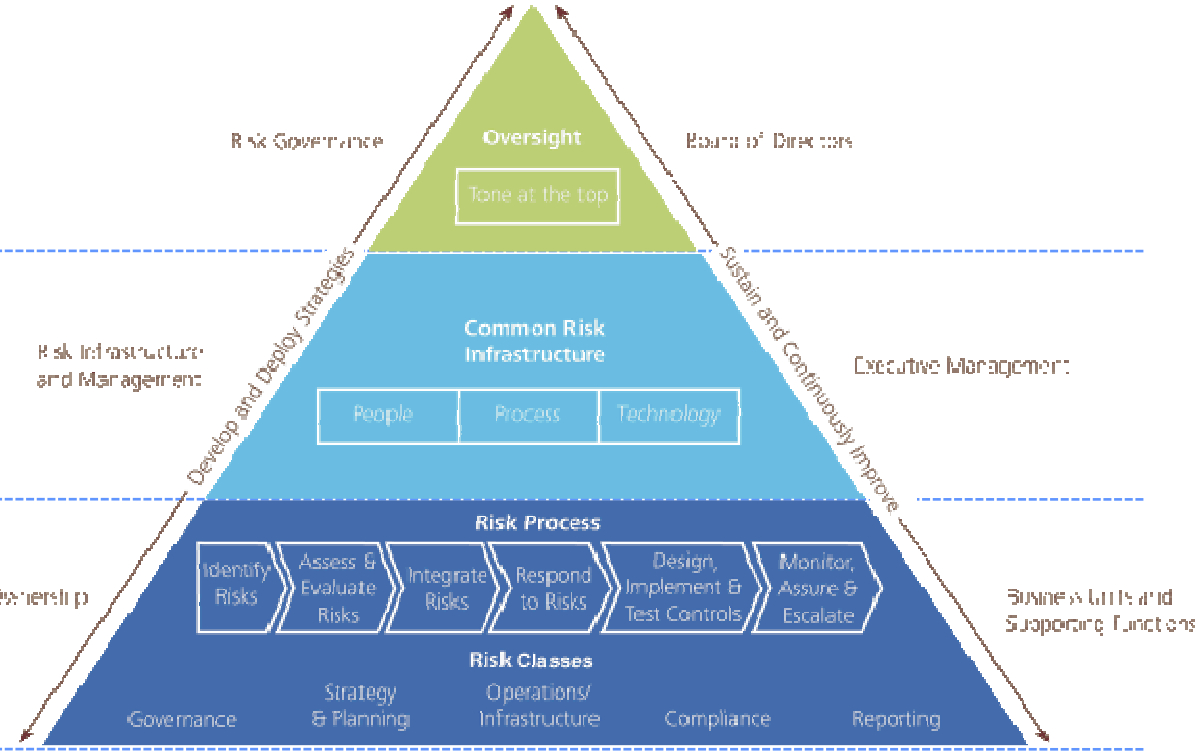
Building a Risk Intelligent Enterprise

Risk Intelligent Enterprises adopt a balanced perspective of risk management supported by fundamental principles:

Nine Principles for Building a Risk Intelligent Enterprise

- Governing Bodies Responsibility
- Roles & Responsibilities
- Common Definition of Risk
- Common Risk Framework
- Common Risk Infrastructure
- Executive Management Responsibility
- Objective Assurance and Monitoring
- Business Unit Responsibility
- Support of Pervasive Functions

The Risk Intelligent Enterprise



© 2011 Deloitte Touche Tohmatsu Limited

Risk Intelligence Program Methodology Summary

Nine Principles \ Phases		Assess	Develop	Implement	Monitor
		Assess Current State and Identify Opportunities for Enhancing the Risk Management Program	Develop Components of a Desired State for the Risk Management Program	Implement Risk Management Program Enhancements	Monitor and Sustain Risk Management Program
Risk Governance	Governing Bodies Responsibility	1.1 Business and Risk Management Strategy	2.1 Board and Executive Management Risk Committees and Charters	3.1 Integrated Approach to Strategy and Risk Management	4.1 Board and Executive Management Performance and Risk Management Oversight
	Roles & Responsibilities	1.2 Board and Executive Management Risk Oversight and Governance	2.2 Governance Structure		
	Common Definition of Risk	1.3 Risk Culture and Definition of Risk	2.3 Risk Culture, Taxonomy, Framework(s) and Metrics		4.2 Business Strategy and Risk Management Execution
		1.4 Risk Treatment, Appetite and Limits			
	Common Risk Framework	1.5 Risk, Compliance and Regulatory Framework(s)			
Risk Infrastructure and Management	Executive Management Responsibility		2.4 Enhanced Risk Management Methodology, Policies, Processes and Controls		
		1.6 Risk Management Methodology, Policies, Processes and Controls			
	Common Risk Infrastructure	1.7 Risk Management Technologies	2.5 Technology Infrastructure to Manage Enterprise Performance and Risk	3.2 Enhanced Risk Management Infrastructure to Support Business Operations	
		1.8 Data Governance			
		1.9 Resources, Skills and Training Activities	2.6 Resources, Skills and Training Program		
			2.7 Change Management and Communications Program		
	Objective Assurance and Monitoring	1.10 Risk, Compliance and Regulatory Oversight Functions and Activities	2.8 Assurance Framework for Risk Oversight and Independent Assurance	3.3 Assurance Framework, Programs and Activities	4.3 Objective Assurance over the Risk Management Program
		1.11 Internal Audit Function and Activities			
Risk Ownership	Business Unit Responsibility & Support of Pervasive Functions	1.12 Enterprise and Business Unit Risks to Value Creation / Preservation	2.9 Risk Mitigation and Response Plans	3.4 Integrated Risk Management within Key Business Functions / Activities	4.4 Risk Processes and Controls / Escalation and Response
		1.13 Risk Scenarios, Measurement, Vulnerability and Priority	2.10 Business Process and Control Enhancements		
		1.14 Existing Risk Mitigation Activities / Business Processes and Controls	2.11 Key Risk/ Performance Indicators		

© 2011 Deloitte Touche Tohmatsu Limited

Deloitte's Risk Platform

Risk Platform - Deloitte's has enabled its Risk Intelligence Program Methodology

Our Risk Platform is powered by IBM's OpenPages

Deloitte Risk Consulting practice has created the Global Integrated Risk Platform built on IBM's OpenPages that provides:

- A **global repository** of Deloitte intellectual property related to risk and regulatory compliance that can be uploaded, managed and used on engagements.

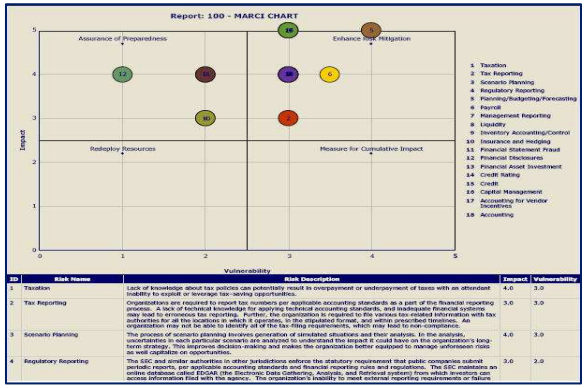
- **A flexible and powerful platform** to model and deliver the firm's risk and compliance service offerings to clients leveraging the available Deloitte intellectual property.

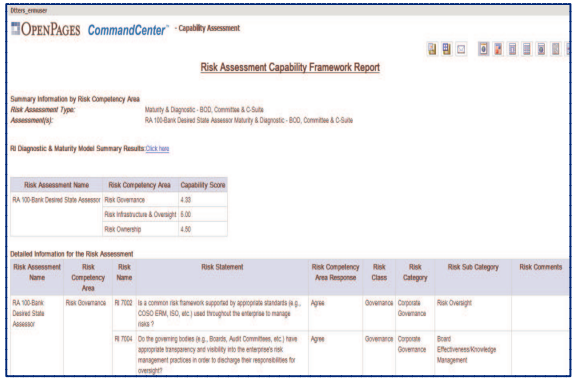
- A platform to demonstrate our **deep understanding of risk and regulatory compliance** and the underlying technology needed to build an effective program to manage it.

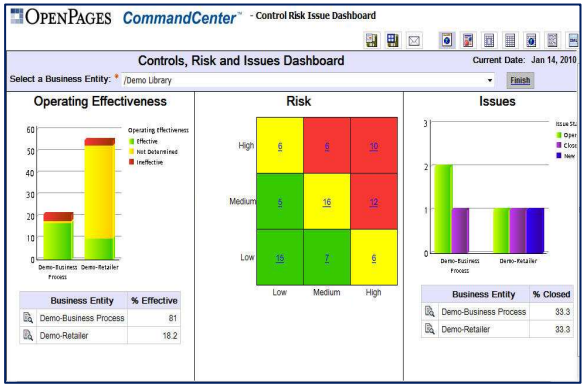
- Improving **collaboration** between various departments (CIO, CFO, CRO, etc) within the client's enterprise.

- **Avoiding duplication of effort**, content and tools across the client organization.

- Enhancing the **correlation between risk and performance information** across the client's enterprise.



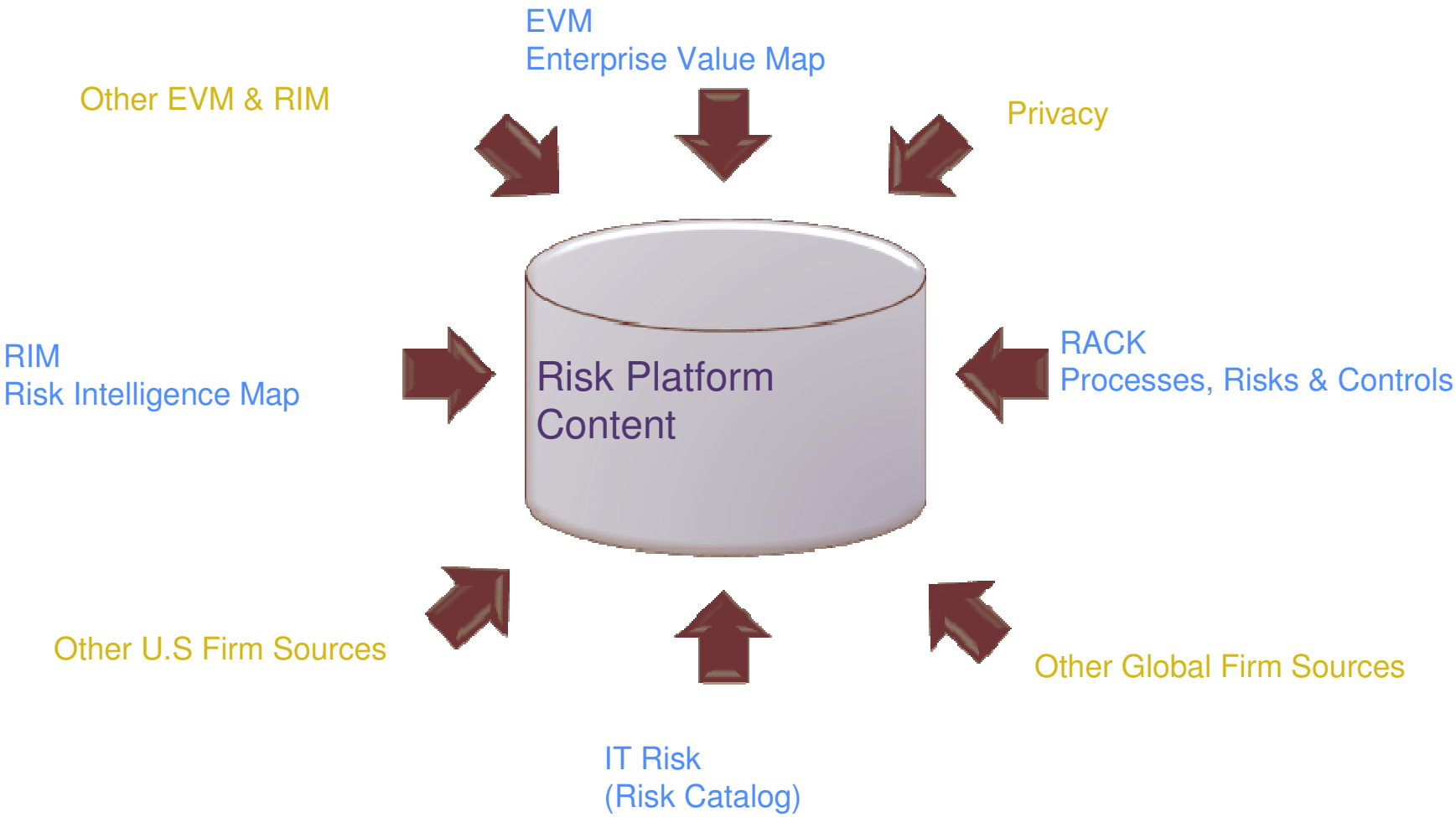




© 2011 Deloitte Touche Tohmatsu Limited

1. A global repository

A global repository of Deloitte intellectual property related to risk and regulatory compliance that can be uploaded, managed and used on engagements.



© 2011 Deloitte Touche Tohmatsu Limited

1. A global repository (cont.)

- The Risk Platform can store many different types of risk related information.
- Relevant information can be exported into familiar formats
  - HTML, PDF, Excel, CSV & XML

Summary / Folder View

- A listing of risk information can be viewed through an easy-to-navigate folder structure
- Clicking on a risk object name opens a new screen where users can review and edit details for a specific risk

ited

Risk Platform Content

Associated Mandates			
Mandate	**Section Reference Number**	**Section Title**	**Section SubTitle**
FFIEC - Information Security July 2006	5.1.3.1	Network Access	Firewalls
FFIEC - Information Security July 2006	5.1.3.1.1	Firewalls	Packet Filter Firewalls
FFIEC - Information Security July 2006	5.1.3.1.6	Firewalls	Firewall Policy
FFIEC E-Banking	2.3.2.4	Information Security Controls	Network access controls over external connections
FFIEC Retail Payment Systems Handbook (Dated March 2004)	3.8.6	EFT/POS AND CREDIT CARD NETWORKS	
The Monetary Authority of Singapore - Internet Banking - Technology Risk Management Guidelines	5.2.2	SECURITY PRINCIPLES AND PRACTICES	FIREWALL INFRASTRUCTURE
The Monetary Authority of Singapore - Internet Banking - Technology Risk Management	5.2.3	SECURITY PRINCIPLES AND PRACTICES	FIREWALL INFRASTRUCTURE

© 2011 Deloitte Touche Tohmatsu Limited

Localization

Translated Risk Intelligence Map into Japanese

ID:	RI 1000-J
Risk Statement:	忠実義務の理解不足や違反がある / Failure to understand and exercise fiduciary duties.
Risk Map Type:	Risk Intelligence Map - Japan
Risk Intelligence Map (RIM) Class:	ガバナンス / Governance
RIM Category:	コーポレートガバナンス / Corporate Governance
RIM Sub Category:	取締役会の有効性と情報共有 / Board Effectiveness/Knowledge Management
Risk Statement Description:	The Board of Directors has the responsibility to act on behalf of the organization's shareholders and aim for increased shareholder value. The Board also needs to comply with various regulations in place to ensure proper functioning and accountability of its members.
RIM Class Desc:	Governance is a set of relationships and structure through which the objectives of the organization are set, and the means of attaining those objectives and monitoring performance are determined. It is about corporate fairness, transparency, accountability and risks related to the structure, policies, procedures and authorities in which the key directions and decisions of the organization are overseen. This includes corporate governance and ethics as two risk categories under it.
RIM Category Desc:	コーポレートガバナンスは、プロセス、風習、方針、法律や組織が影響される制度、業務の運営管理、もしくは統制のことをいう。良いコーポレートガバナンスに求められる主な要素は、正直さ、信頼性、誠実性、開放性、経営の方向づけ、責任と説明責任、相互理解、組織への献身である。特にコーポレートガバナンスは、組織の経営管理者が自ら正直で倫理的に、実際の問題または見かけの利害対立に関して対応すべきであり、財務報告における情報開示についても管理すべきであると強調する。組織が効果的なコーポレートガバナンスの慣習を整備しないことは、取締役、経営管理者や従業員を違法な/非道徳的な行為、不正な報告や情報開示に導く可能性がある。 Corporate governance is the set of processes, customs, policies, laws and institutions affecting the way an organization is directed, administered, or controlled. Key elements of good corporate governance principles include honesty, trust and integrity, openness, performance orientation, responsibility and accountability, mutual respect, and commitment to the organization. In particular, corporate governance emphasizes that, senior executives of the organization should conduct themselves honestly and ethically, especially concerning actual or apparent conflicts of interest, and disclosures in financial reports. Failure of the organization to put in place effective corporate governance practices may lead to Board members, senior management, or employees committing illegal/unethical acts, resulting in fraudulent reporting and disclosures.
RIM Sub Category Desc:	取締役には、適切かつ継続的なスキルと知識のアップデートが必要とされる。そのため、現在利用できる情報や教材を活用し、教育や研修を受けることが必要である。それにより、取締役や上級経営陣は、最新の規制・ビジネス上の問題・ガバナンスのトピック・テクニカルな問題について豊富な知識を身が付き、リスク・インテリジェンス面で効果的な決断を下せるようになるからである。また、継続的に取締役会・委員会に出席することにより、業務に対し全般的な効果を高める意思決定（ディシジョンメイキング）ができる ようになる。（例えば、取締役会に出席することにより、新たな会計実務の有効・税法のギャップ・規制に関するトピックについて得る最新情報は得る

© 2011 Deloitte Touche Tohmatsu Limited

2. Deliver services

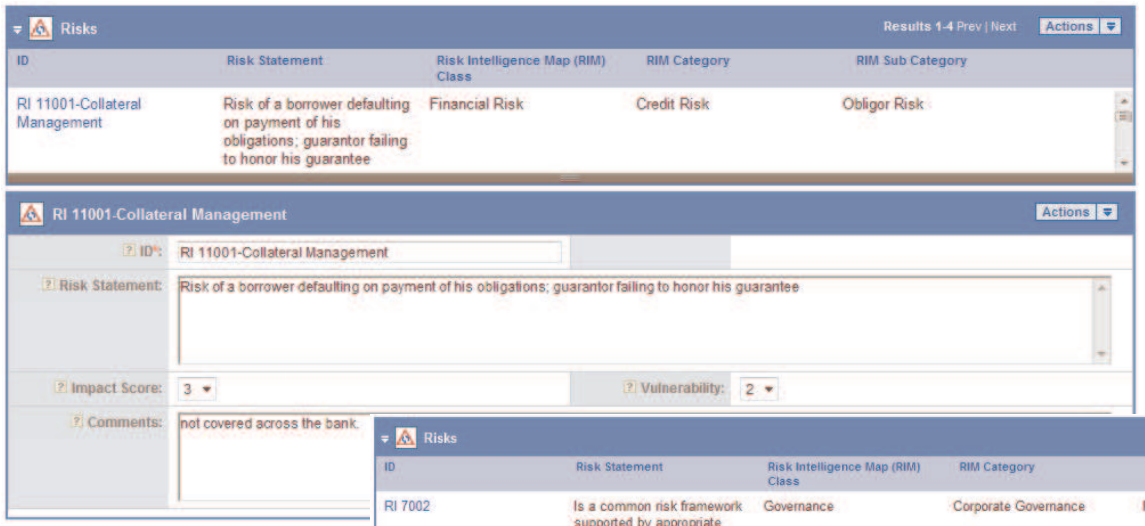
A flexible and powerful platform to model and deliver the firm's current and future risk and compliance offerings to clients leveraging the available Deloitte intellectual property.

- Enable rapid development of supporting technology for new service offerings (e.g. response to any new regulation)
- Perform Enterprise Risk Management assessments.
- Evaluate/assess risk maturity and/or regulatory compliance using any available risk framework.
- Document control design and effectiveness tests,
- Manage issues, signoffs and certifications (can be workflow enabled)
- Perform root cause analysis
- Flexible reporting on all of the above

© 2011 Deloitte Touche Tohmatsu Limited

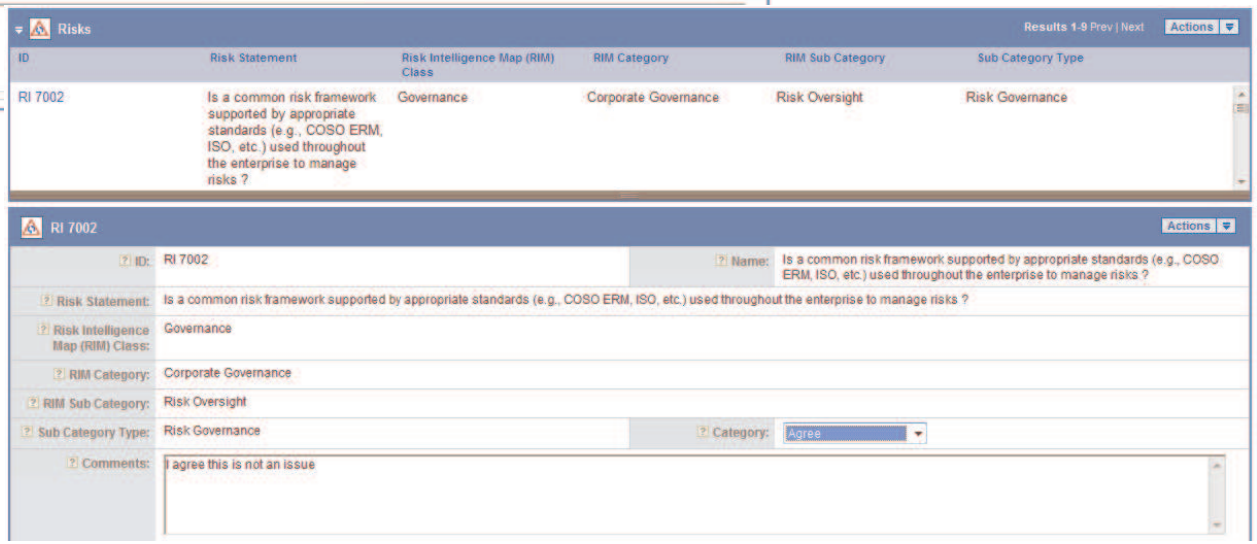
2. Deliver services – Perform assessments

- The Risk Platform offers functionality to facilitate assessments, tests or evaluations of the data stored within the platform
- **All of the content stored within the risk platform can be assessed/evaluated using**



Assessment of Impact & Vulnerability

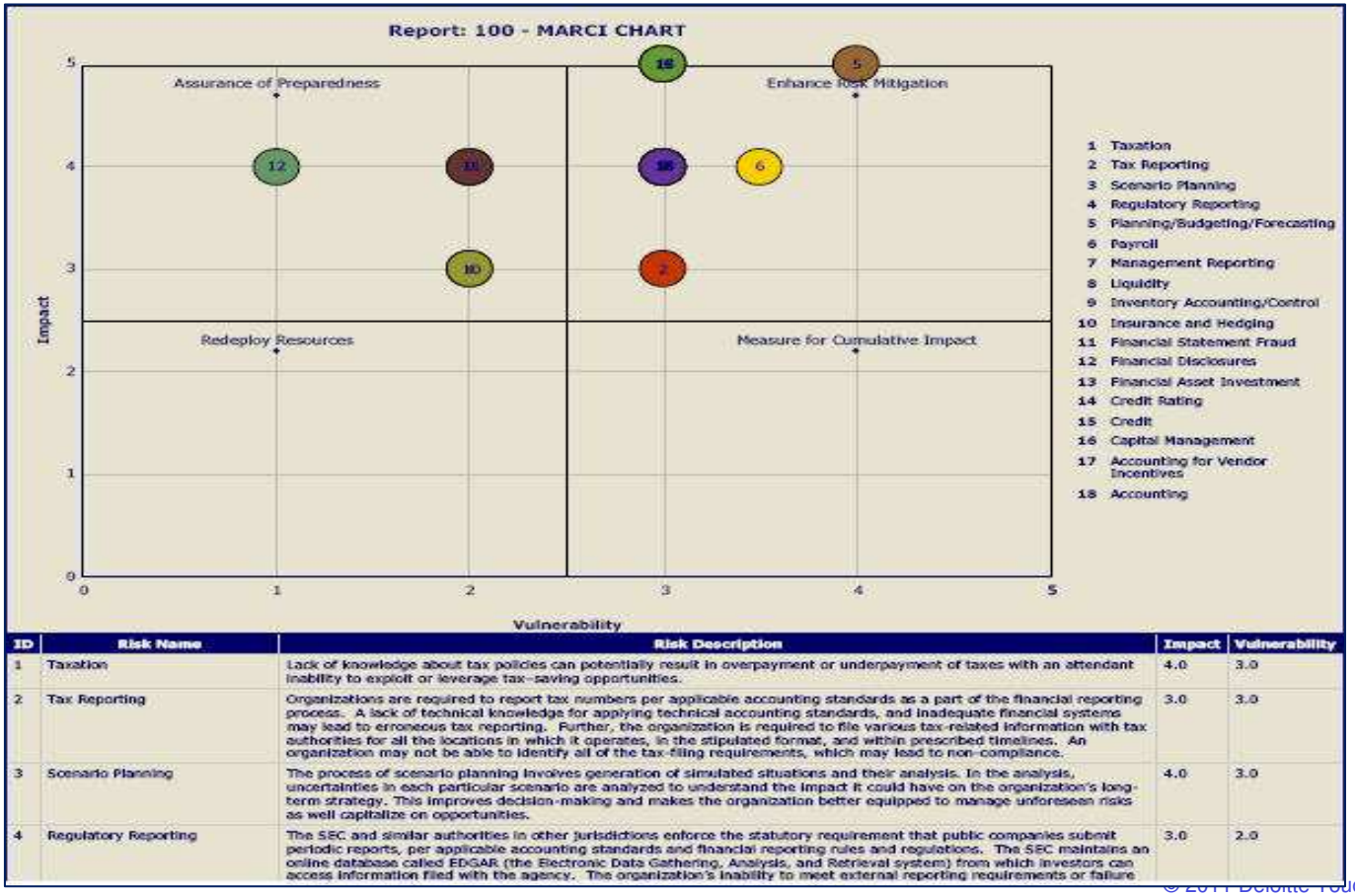
Capability Assessment



© 2011 Deloitte Touche Tohmatsu Limited

2. Deliver services – Report on Key Risks

- Several reports are available in the Risk Platform providing valuable insight into the data present within the platform and the results of an assessment or evaluation of that data.
- The platform is capable of displaying reporting data in multiple formats.
    - Grid, Pie Chart, Bar Chart, Line Graph, 4 Quadrants, etc.
- Significant knowledge of report development is present within the firm making the possibility of report enhancement or new report development easier.



ID	Risk Name	Risk Description	Impact	Vulnerability
1	Taxation	Lack of knowledge about tax policies can potentially result in overpayment or underpayment of taxes with an attendant inability to exploit or leverage tax-saving opportunities.	4.0	3.0
2	Tax Reporting	Organizations are required to report tax numbers per applicable accounting standards as a part of the financial reporting process. A lack of technical knowledge for applying technical accounting standards, and inadequate financial systems may lead to erroneous tax reporting. Further, the organization is required to file various tax-related information with tax authorities for all the locations in which it operates, in the stipulated format, and within prescribed timelines. An organization may not be able to identify all of the tax-filing requirements, which may lead to non-compliance.	3.0	3.0
3	Scenario Planning	The process of scenario planning involves generation of simulated situations and their analysis. In the analysis, uncertainties in each particular scenario are analyzed to understand the impact it could have on the organization's long-term strategy. This improves decision-making and makes the organization better equipped to manage unforeseen risks as well capitalize on opportunities.	4.0	3.0
4	Regulatory Reporting	The SEC and similar authorities in other jurisdictions enforce the statutory requirement that public companies submit periodic reports, per applicable accounting standards and financial reporting rules and regulations. The SEC maintains an online database called EDGAR (the Electronic Data Gathering, Analysis, and Retrieval system) from which investors can access information filed with the agency. The organization's inability to meet external reporting requirements or failure	3.0	2.0

© 2011 Deloitte Touche Tohmatsu Limited

2. Deliver services – Report on Findings

Dtters_ermuser

OpenPages CommandCenter™ - Capability Assessment

Risk Assessment Capability Framework Report

Summary Information by Risk Competency Area

Risk Assessment Type: Maturity & Diagnostic - BOD, Committee & C-Suite

Assessment(s): RA 100-Bank Desired State Assessor Maturity & Diagnostic - BOD, Committee & C-Suite

RI Diagnostic & Maturity Model Summary Results: Click here

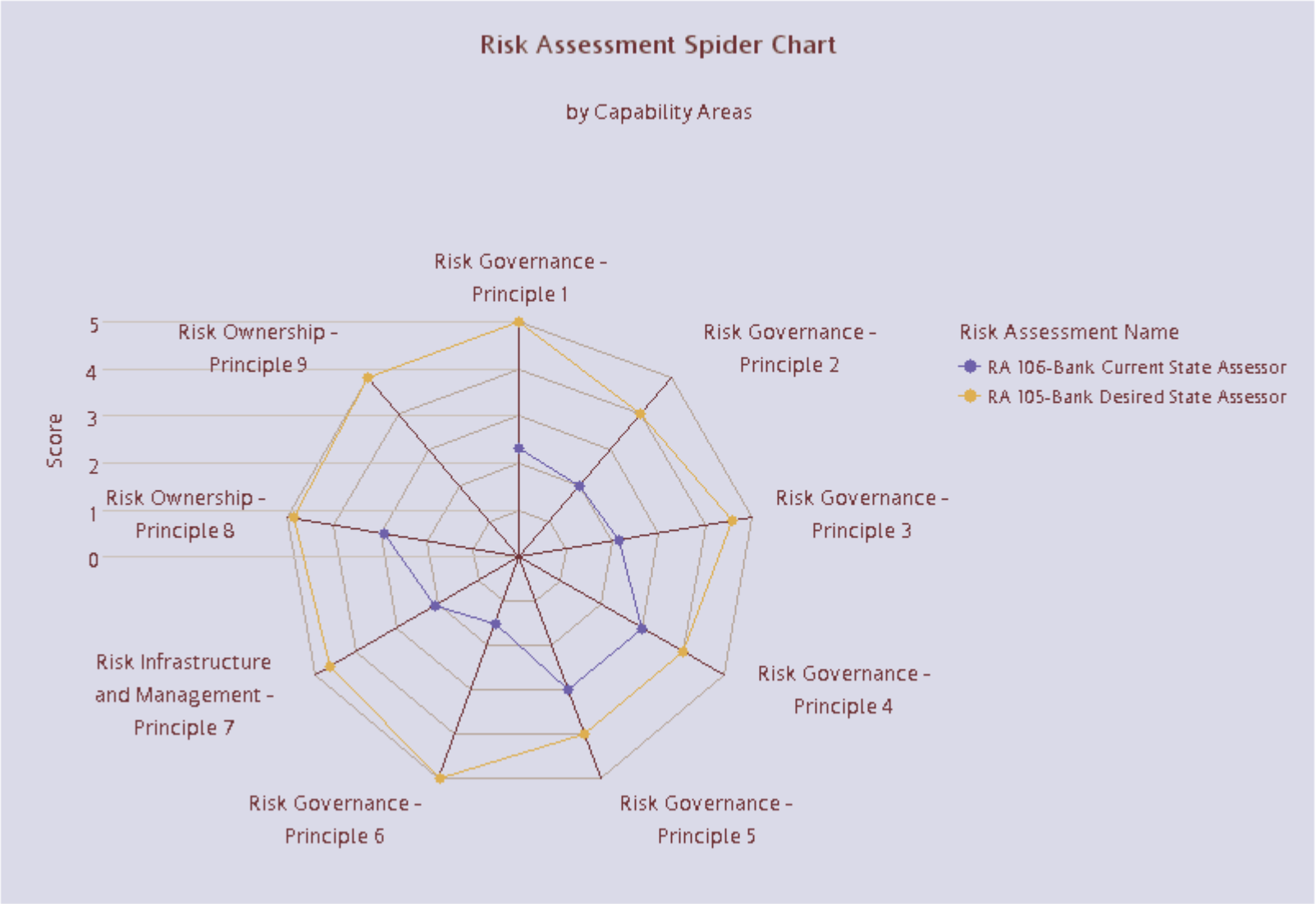
Risk Assessment Name	Risk Competency Area	Capability Score
RA 100-Bank Desired State Assessor	Risk Governance	4.33
	Risk Infrastructure & Oversight	5.00
	Risk Ownership	4.50

Detailed Information for the Risk Assessment

Risk Assessment Name	Risk Competency Area	Risk Name	Risk Statement	Risk Competency Area Response	Risk Class	Risk Category	Risk Sub Category	Risk Comments
RA 100-Bank Desired State Assessor	Risk Governance	RI 7002	Is a common risk framework supported by appropriate standards (e.g., COSO ERM, ISO, etc.) used throughout the enterprise to manage risks ?	Agree	Governance	Corporate Governance	Risk Oversight	
		RI 7004	Do the governing bodies (e.g., Boards, Audit Committees, etc.) have appropriate transparency and visibility into the enterprise's risk management practices in order to discharge their responsibilities for oversight?	Agree	Governance	Corporate Governance	Board Effectiveness/Knowledge Management	

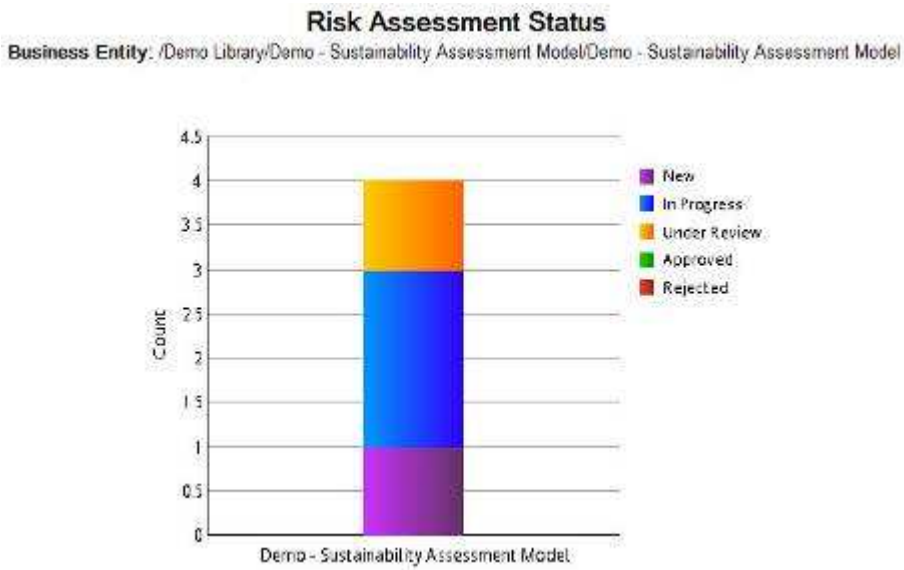
© 2011 Deloitte Touche Tohmatsu Limited

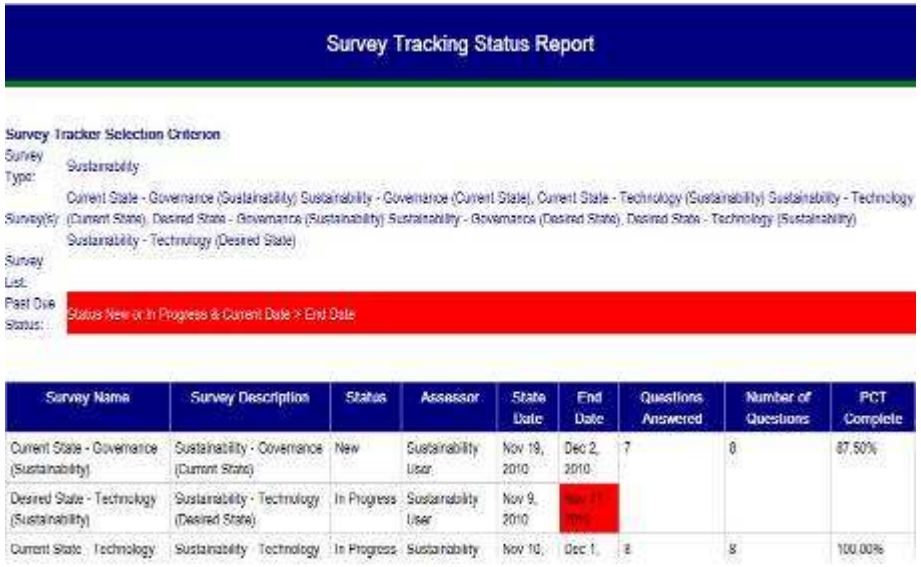
2. Deliver services – Report on Maturity



© 2011 Deloitte Touche Tohmatsu Limited

2. Deliver services – Report on Status





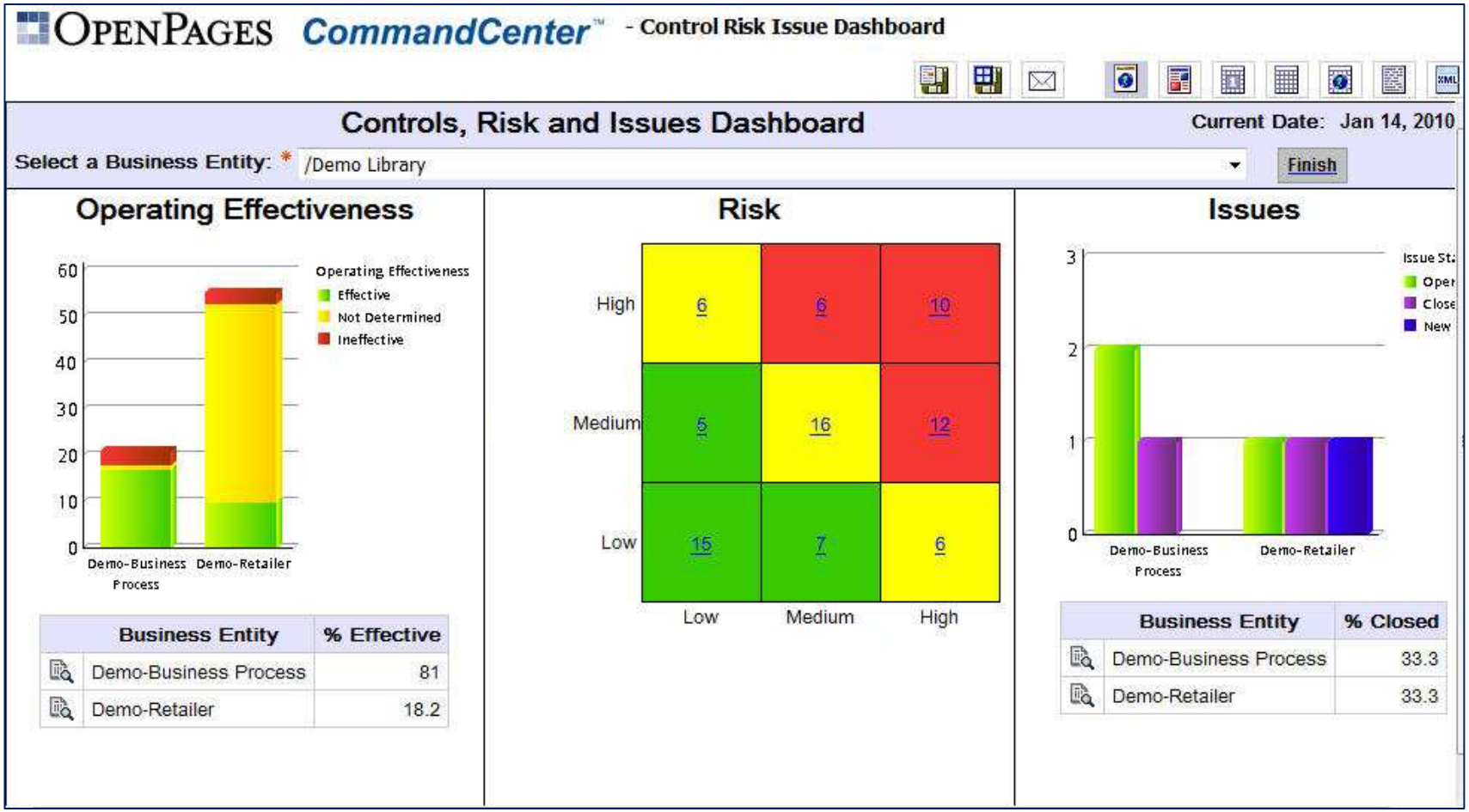
Business Entity: /Demo Library/Demo - Sustainability Assessment Model/Demo - Sustainability Assessment Model

Name	Description	Status	Start Date	End Date	Creator	Assessor	Reviewer
Current State - Governance (Sustainability)	Sustainability - Governance (Current State)	New	Nov 19, 2010	Dec 2, 2010	Rob Garagiola	Dtters_sustainu	Dtters_sustain
Current State - Technology (Sustainability)	Sustainability - Technology (Current State)	In Progress	Nov 10, 2010	Dec 1, 2010	Rob Garagiola	Dtters_sustainu	Dtters_sustain
Desired State - Governance (Sustainability)	Sustainability - Governance (Desired State)	Under Review	Nov 12, 2010	Nov 19, 2010	Rob Garagiola	Dtters_sustainu	Dtters_sustain
Desired State - Technology (Sustainability)	Sustainability - Technology (Desired State)	In Progress	Nov 9, 2010	Nov 17, 2010	Rob Garagiola	Dtters_sustainu	Dtters_sustain

© 2011 Deloitte Touche Tohmatsu Limited

2. Deliver services – Management Dashboard

- Risk Platform supports the creation of dashboards that can be configured for individual users or user groups.
- This feature offers a greater assurance that the most timely information is delivered to the correct resources.

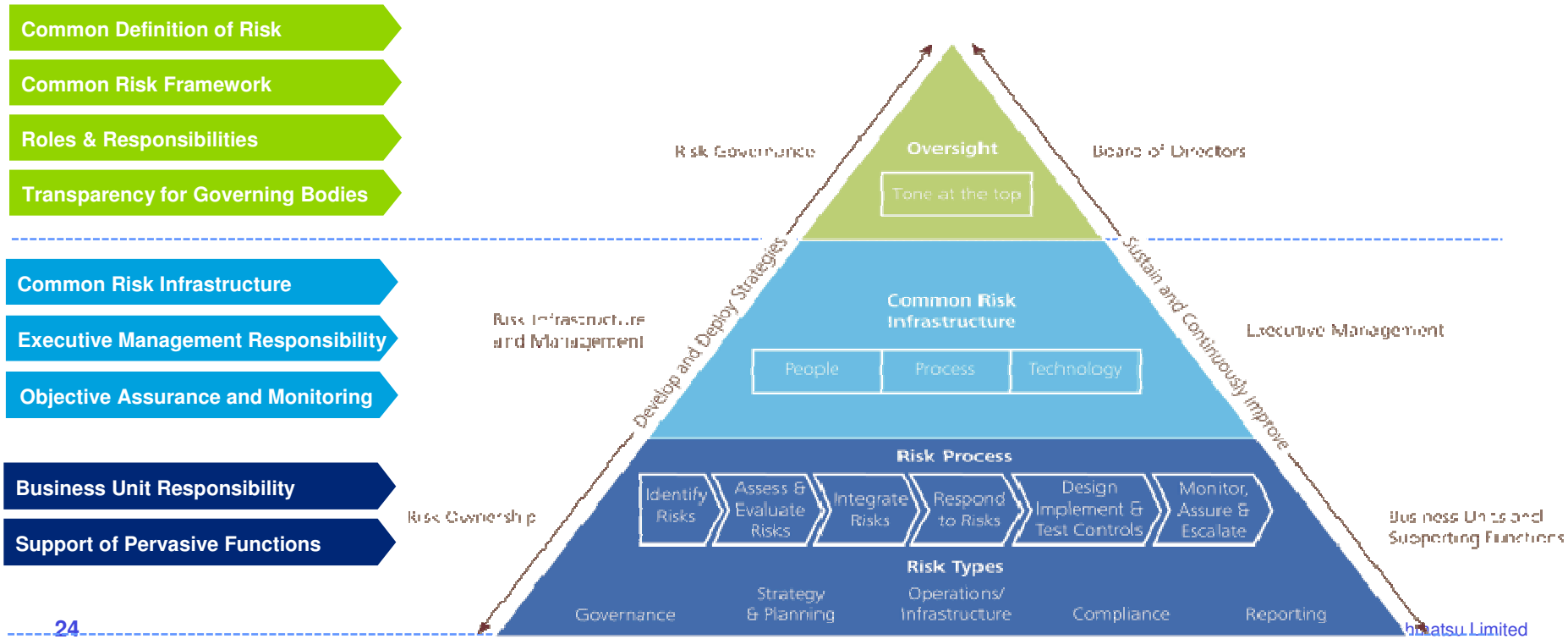


© 2011 Deloitte Touche Tohmatsu Limited

3. Demonstrate capabilities

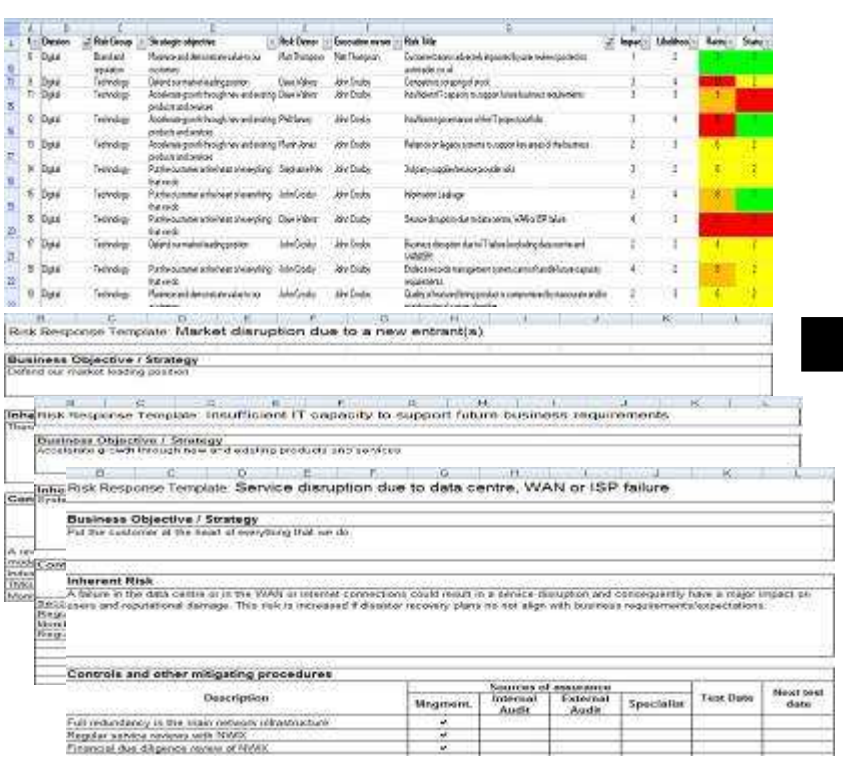
A platform to demonstrate our deep understanding of risk and regulatory compliance and the underlying technology needed to build an effective program to manage it.

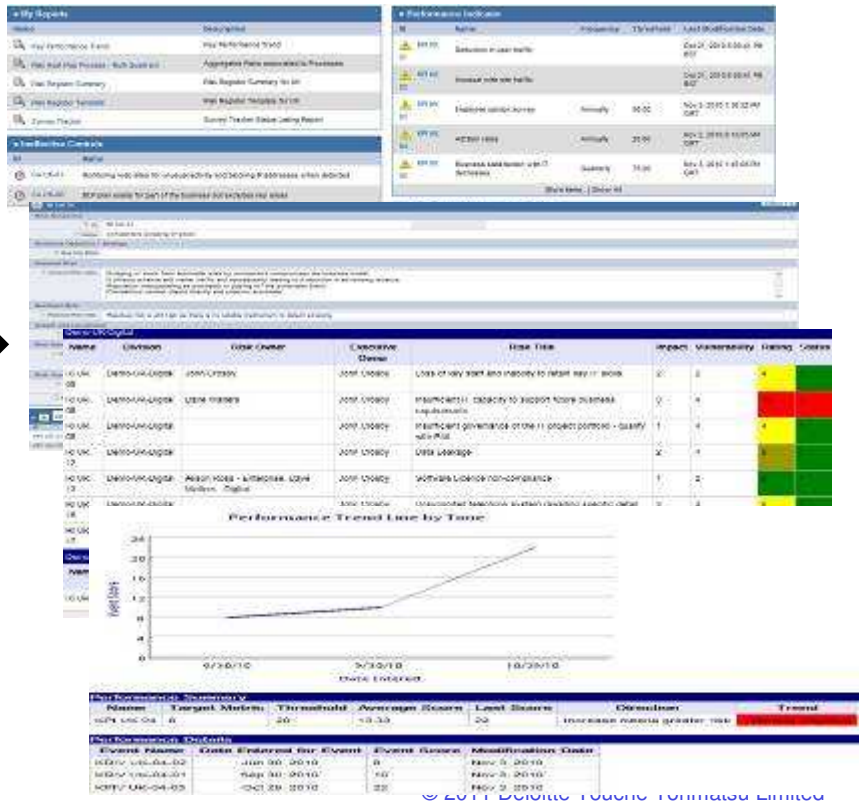
- Provides a live, configurable environment to demonstrate risk management and compliance concepts to our clients
- Environment to showcases Deloitte's capabilities in understanding and implementing technology that addresses client's risk and regulatory needs.



Risk Platform Use Case – Risk Registers Enablement

Current State	Technology Enabler
• Excel based process burdensome to the business with a lot of administration	• Web based easy to use platform with a central repository • Create an efficient and effective process which can expand with our business
• Security, version, change control issues	• Check in/out single version with history
• Limited transparency • Limited audit trail • Limited manual reporting and no central repository	• Extensible security model to support roles and responsibilities • Full audit trail • World Class reporting engine
• No Workflow or automation	• Workflow and automatic email notification

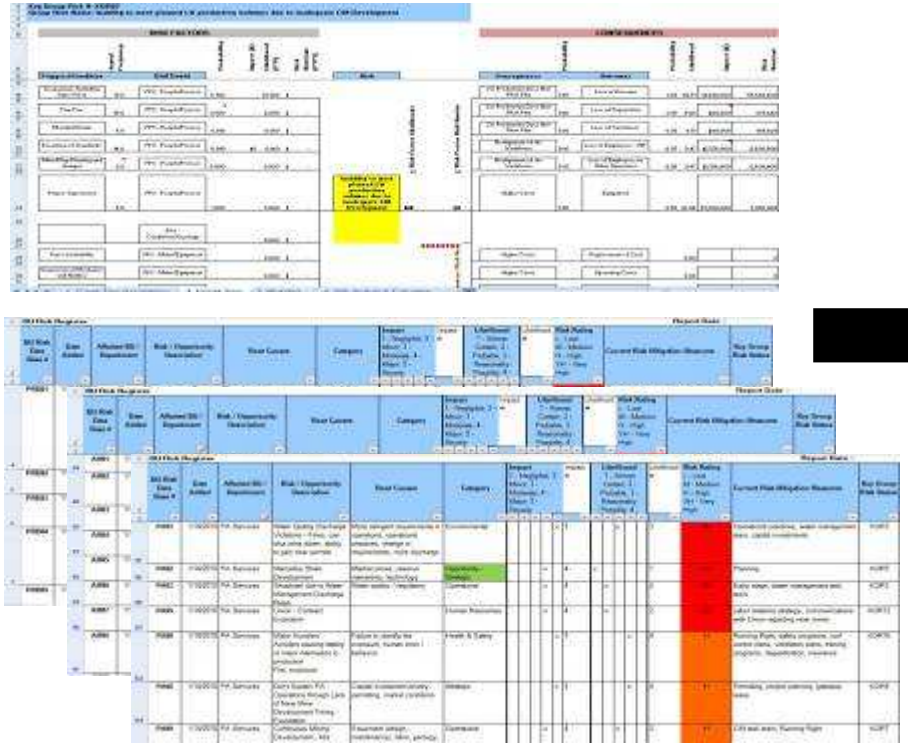


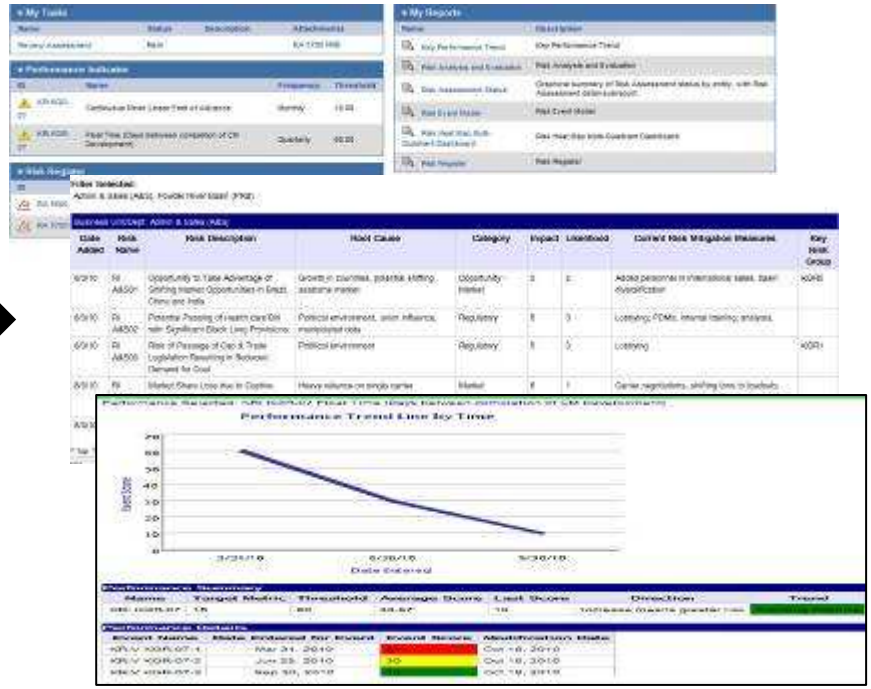


© 2011 Deloitte Touche Tohmatsu Limited

Risk Platform Use Case – Risk Assessment

Current State	Technology Enabler
• Excel based process burdensome to the business with a lot of administration	• Web based easy to use platform with a central repository • Create an efficient and effective process which can expand with our business
• Security, version, change control issues	• Check in/out single version with history
• Limited transparency • Limited audit trail • Limited manual reporting and no central repository	• Extensible security model to support roles and responsibilities • Full audit trail • World Class reporting engine
• No Workflow or automation	• Workflow and automatic email notification





© 2011 Deloitte Touche Tohmatsu Limited

Risk Platform Use Case – Sustainability Assessment

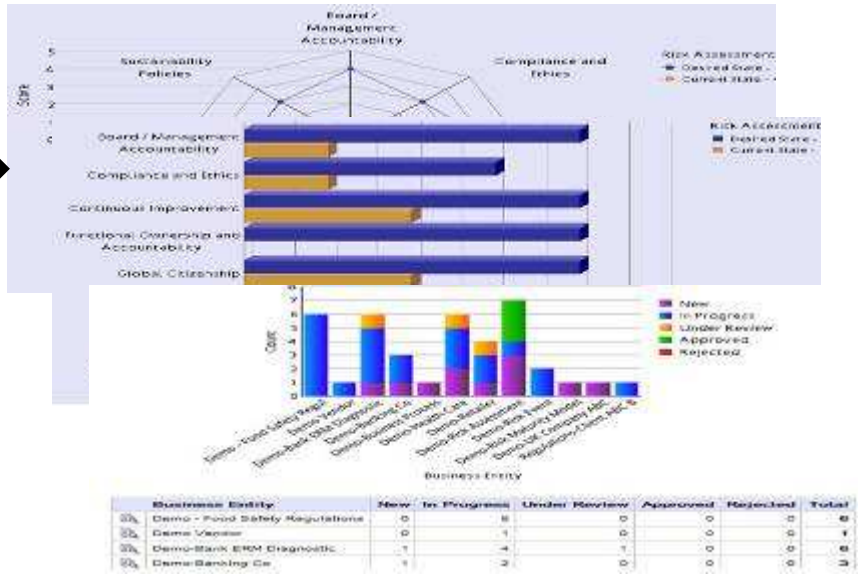
Functions/Benefits	

• Leverage Deloitte's Sustainability Model
  • Governance, Workplace, Workforce, Supply Chain
  • Products & Services, Technology
• Benchmark current state against desired state
	• Web based easy to use platform with a central repository
	• Create individual portals based on roles and responsibilities
	• Create an efficient and effective process which can expand with your business

• Automatically push out assessments to responsible parties • Develop a sustainable operating model	• Ability to conduct offline assessments and upload the results • Improve business unit visibility to risk information
• Provide transparency and full audit trail •Increase visibility into BU processes to enable proactive risk management • Flexible security model based on business needs	• Ability to leverage and create various real-time dashboard sand operational reports • Ability to aggregate / rollup or drill-down on the information
• Automate risk processes and reporting	• Built-in project management reporting

Distribute/ Assess / Capture

Monitor / Report / Aggregate/ Sustain



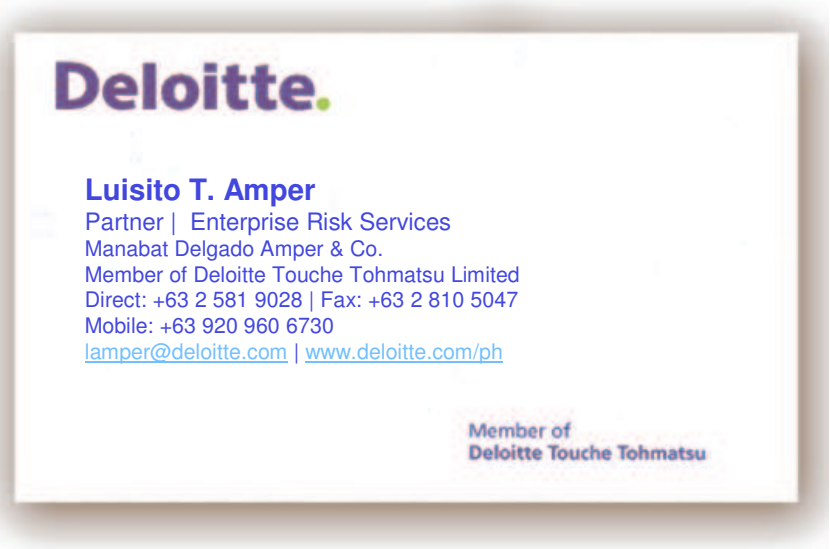
© 2011 Deloitte Touche Tohmatsu Limited

Risk Technology Implementation Program – Common Pitfalls

- Lack of proactive leadership commitment/governance
- Inadequate access to senior management
- Unclear roles and responsibilities (Ownership, transition plans, change management, training, maintenance, approvals)
- Lack of clear definition of project scope
- Moving targets of business or project during implementation
- No signed commitment (contract, statement of work, change orders) for work underway
- Lack of proactive monitoring of third party involvement
- Unnecessary level of technical complexity/over engineering
- Unclear understanding of and agreed upon end results (reporting, dashboard, access)
- Lack of appropriate personnel skill sets

© 2011 Deloitte Touche Tohmatsu Limited

Contact Information



© 2011 Deloitte Touche Tohmatsu Limited

© 2011 Deloitte Touche Tohmatsu Limited