IBM Systems and Technology Group University 2005

ON DEMAND BUSINESS™

© 2005 IBM Corporation

IBM Systems and Technology Group University 2005

Risk and Compliance

Course #:

David Medina
Architect, IBM Risk and Compliance Council

© 2005 IBM Corporation

IBM Systems and Technology Group University 2005

Risk and Compliance

ON DEMAND BUSINESS™

© 2005 IBM Corporation

Disclaimer

Clients are responsible for ensuring their own compliance with relevant laws and regulations. It is the client's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws, including but not limited to, the Sarbanes-Oxley Act, that may affect the client's business and any actions client may need to take to comply with such laws. IBM does not provide legal, accounting or audit advice or represent or warrant that its services or products will ensure that client is in compliance with any law.

The information contained in this presentation is provided “as is” without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of applicable agreements governing the use of IBM hardware, software or services.

© 2005 IBM Corporation

Agenda

- **Risk and compliance landscape**
- **IBM Risk and Compliance framework**
- **IBM's broad portfolio of offerings, solutions and services**

© 2005 IBM Corporation

Learning Objectives

At the conclusion of this material, you should be able to:

- Understand the risk and compliance issues facing your clients
- Learn who are the major stakeholders in an organization's compliance initiatives and how to sell to them
- Understand IBM's Risk and Compliance framework
- Understand how IBM's broad portfolio of offerings, solutions and services "snap to" the framework

© 2005 IBM Corporation

Business challenges your clients may be facing

Demonstrate compliance with multiple risk and compliance requirements

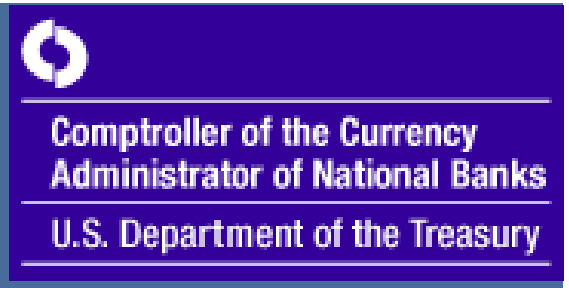
Generate business value from risk and compliance investments

Protect the privacy and security of critical information assets

© 2005 IBM Corporation

Regulations are not new

One of the oldest US Federal regulatory agency still in existence today is the Office of the Comptroller of the Currency (OCC). It was established in 1863 to charter and regulate national banks.



© 2005 IBM Corporation

They are just more numerous and complex

Regulatory and shareholder issues are requiring firms to re-evaluate their current compliance and risk management infrastructure

- **Basel II**
- **Sarbanes- Oxley**
- **USA PATRIOT Act**
- **FSA**
- **IAS**
- **FDA 21 CFR 11**
- **WEEE**
- **GLBA**
- **SEC 17a-3 & 17a-4**
- **NASD 3010 & 3110**
- **Proceeds of Crime Bill**
- **HIPAA**

© 2005 IBM Corporation

And traditional point solutions can be siloed and tactical

Leading point solutions may be adequate for initial, tactical compliance, but that approach can increase complexity and limitations over time

© 2005 IBM Corporation

What's needed is a more strategic approach

Compliance is a "journey" not a "destination" and organizations should adopt a risk and compliance framework that can be used as guidance for the creation of a regulatory compliance architecture

© 2005 IBM Corporation

Don’t just take our word for it

“By 2006, public companies that do not adopt a compliance management architecture will spend 50 percent more annually to achieve Sarbanes-Oxley compliance, according to Gartner”

Gartner Symposium/IT Expo 2004

March 31, 2004

© 2005 IBM Corporation

Why the framework is important to your clients

- Attempts to provide a holistic view of the elements required for compliance
- Describes the major components or building blocks of an end-to-end solution
- Spans all industries
- Spans multiple regulations across multiple geographies
- Provides a common language to facilitate collaboration
- Provides the basis for:
  - Identifying the scope of a project
  - Defining a roadmap for building a total solution
  - Identifying elements to decrease project risk
  - Address current infrastructure, tools and technologies to identify gaps

© 2005 IBM Corporation

Regulatory Taxonomy

Classification	Concepts contained within	Examples

Corporate Governance	• Financial Reporting
	• Transparency
	  o Business Controls
	  o Accountability
	  o Corporate and Accounting Fraud
	• Disclosure
	  o Financial Transactions
	  o Material Events
	  o Safety Information / Recalls
		1. SOX
		2. SEC Act of 1933, 1934
		3. TREAD
		4. IAS

Business Improvement	• Risk Mitigation • Regulatory Capital Requirements • Engineering Models	1. Basel II 2. CMMI 3. ISO 9000
Business Resilience	• Disaster Recovery • Availability	1. NFPA 1600 2. Check 21
Transaction Integrity	• Anti-Money Laundering • Anti-Terrorism • Broker Surveillance • Electronic Signatures	1. NASD 3010/3110 2. NASD 2711 3. NYSE 472 4. 21 CFR 11 5. Patriot Act
Information Protection	• Security • Privacy	1. HIPAA 2. GLBA 3. SB 1386 4. EU Data Privacy 5. FOIA 6. ISO 17799 7. NERC 1200 UAS
Information Lifecycle Management	• Information Management Standards • Retention Requirements • Recordkeeping Standards	1. OMB A-130 2. SOX 3. SEC 17a-4 4. DOD 5015.2 5. PRO 2 6. MoREQ 7. VERS 8. DOMEA 9. NOARK

© 2005 IBM Corporation

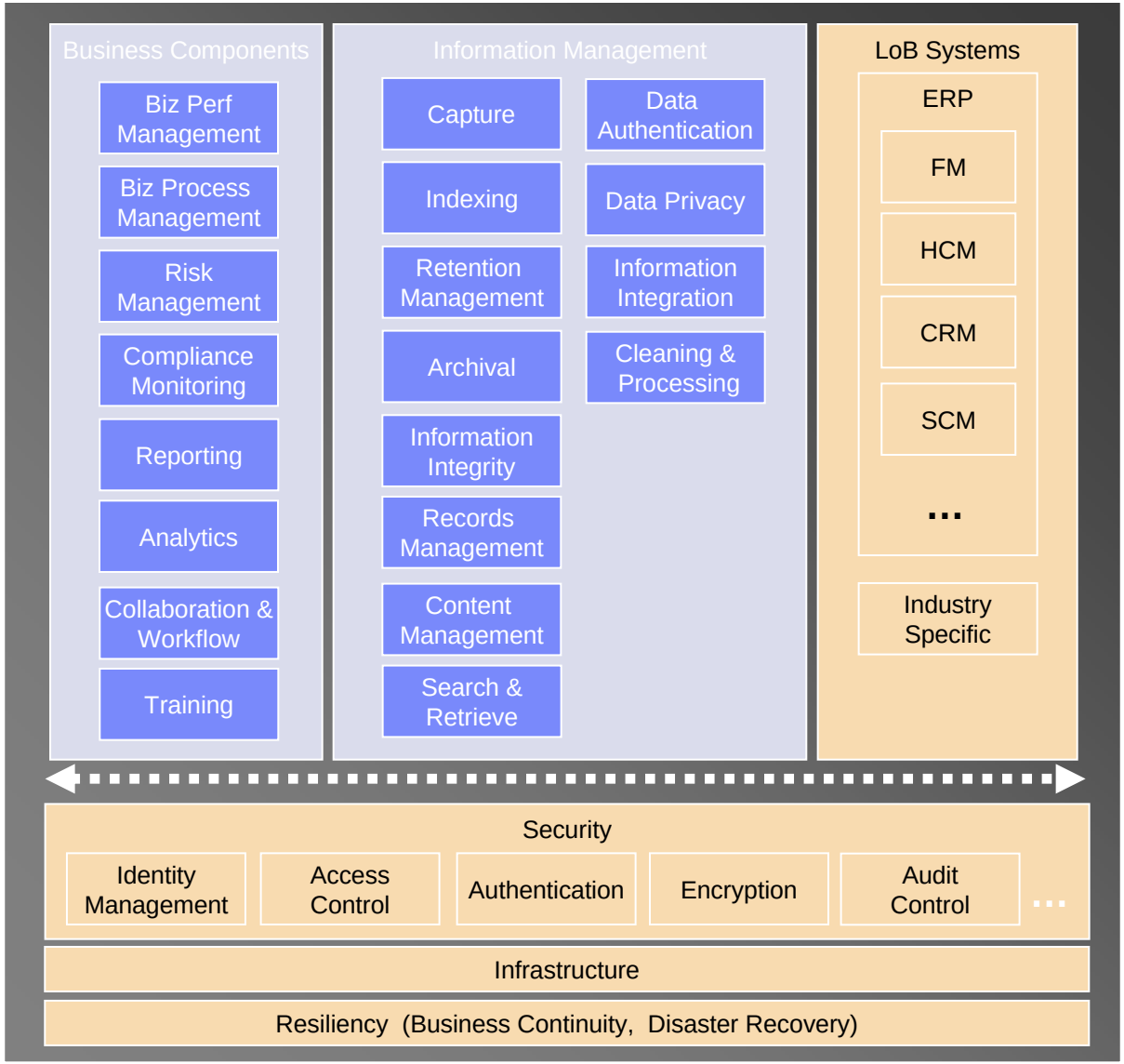
Risk and Compliance Framework Instructions

- **The following slide(s) are interactive**
- **You must be in screen show mode for this to work**
- **Click on the “RUN” button below to activate the slides**
- **On the Framework slide click on a *regulation type* (located on the left side of the slide) to highlight the components that may be applicable. You can select / de-select as many as you like**
- **Click on any *component* to get its description and any product mappings**
- **On the Industry Solution slide click on a regulation to get the solution mappings**
- *NOTE:*
  - *When this presentation was opened you had to have selected the “Enable Macros” button for this feature to work*
  - *If you did not see this option, go to Tools->Options, select the “Security” tab then select the “Macro Security” button and select “Medium”, then re-open the presentation*

RUN

© 2005 IBM Corporation

Risk and Compliance Framework



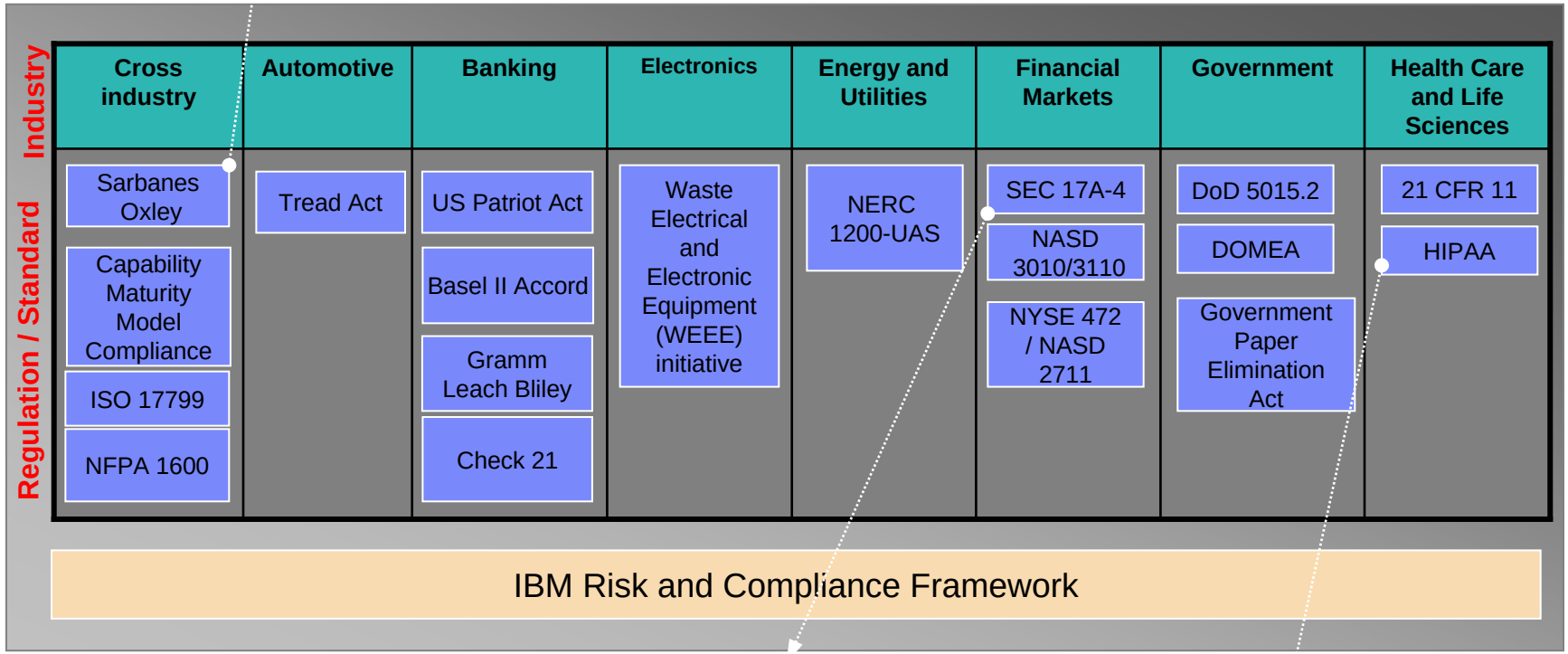
Primary Focus
Secondary Focus
Not Required

© 2005 IBM Corporation

R&C framework supports mapping to offerings

To help you address IT issues and process associated with compliance

Lotus Workplace for Business Controls & Reporting

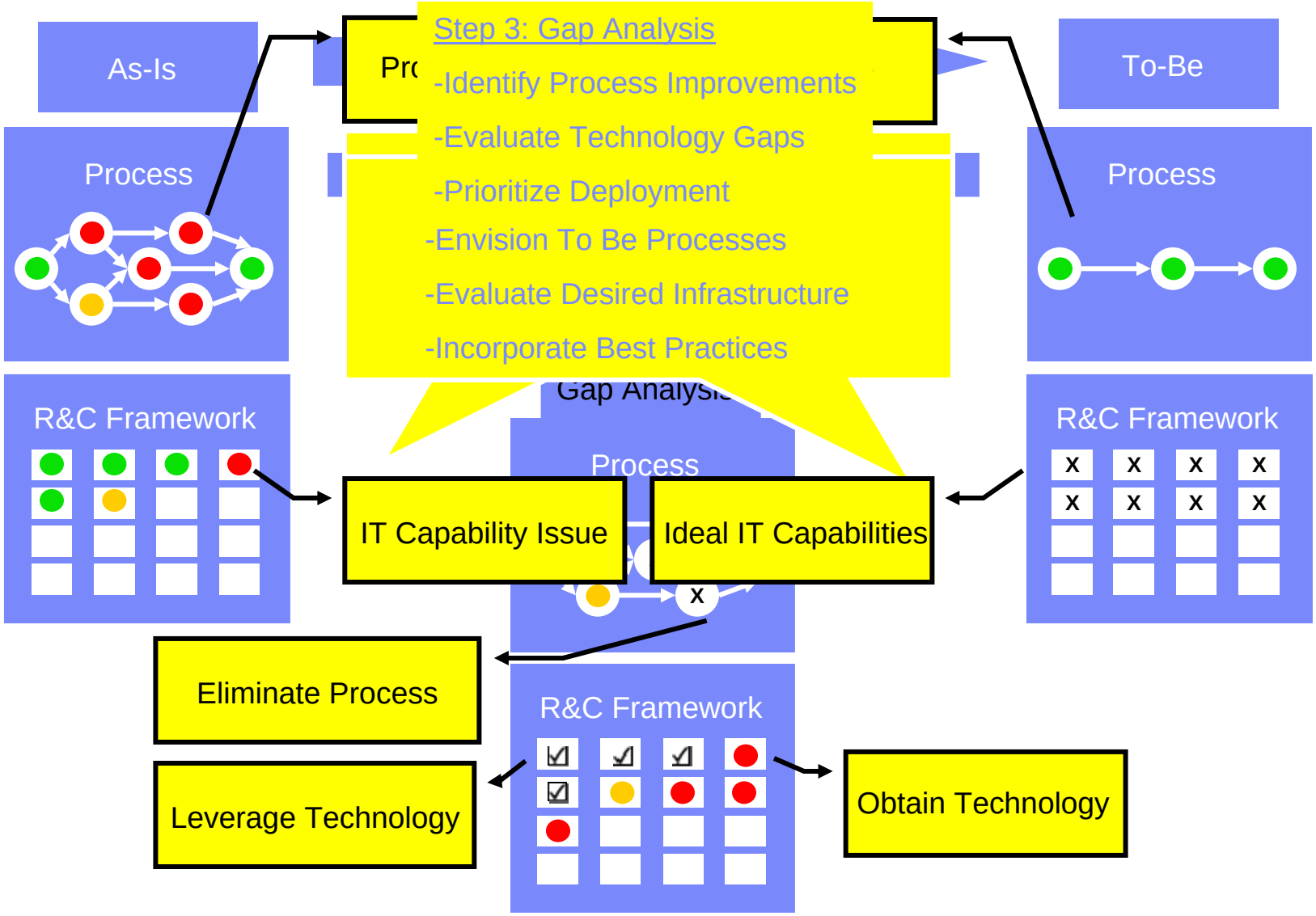


DB2 Content Manager for Message Monitoring & Retention, IBM TotalStorage DR550

IBM Tivoli Privacy Manager, DB2 Content Manager for Privacy

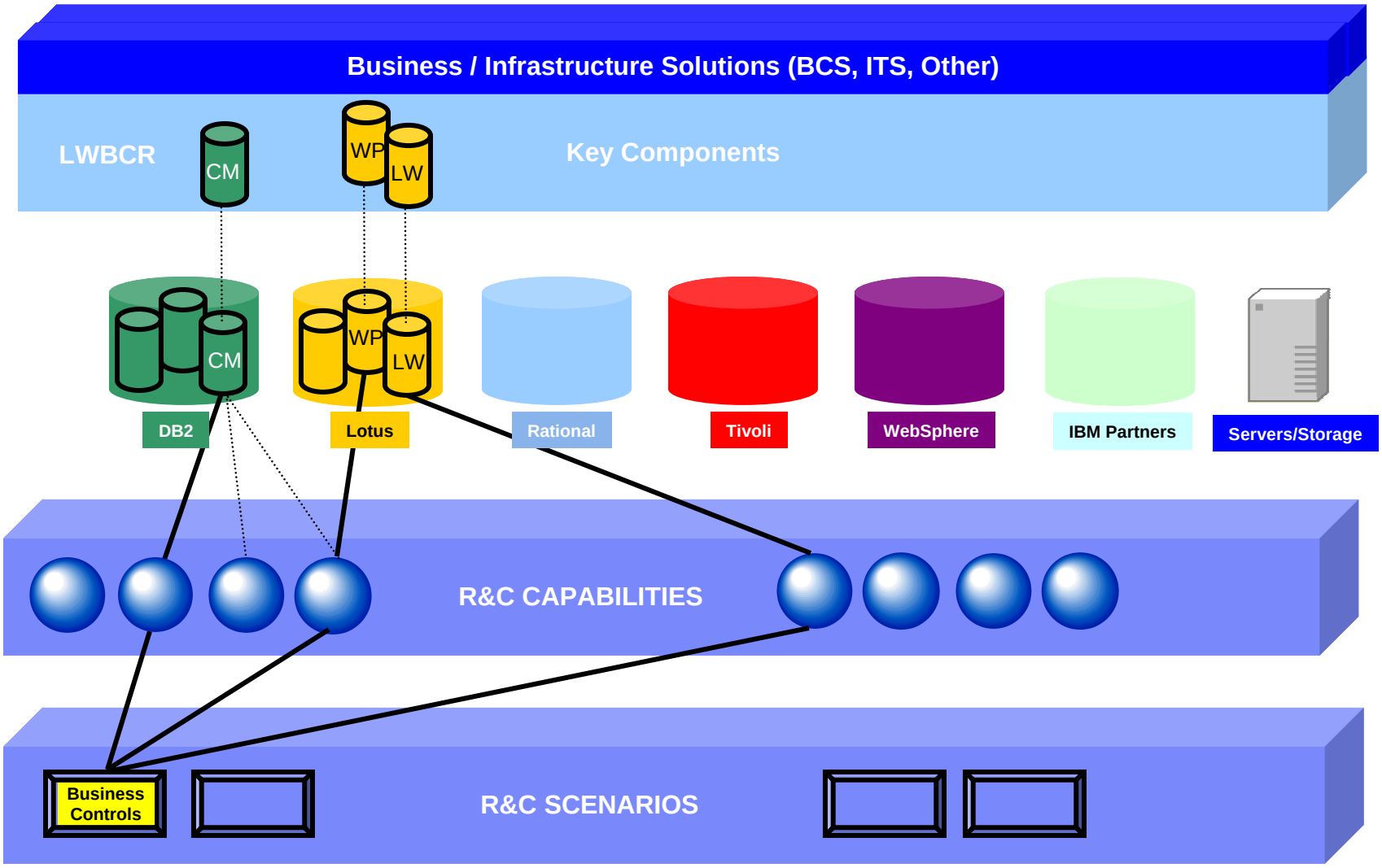
© 2005 IBM Corporation

The Assessment - Use of Framework



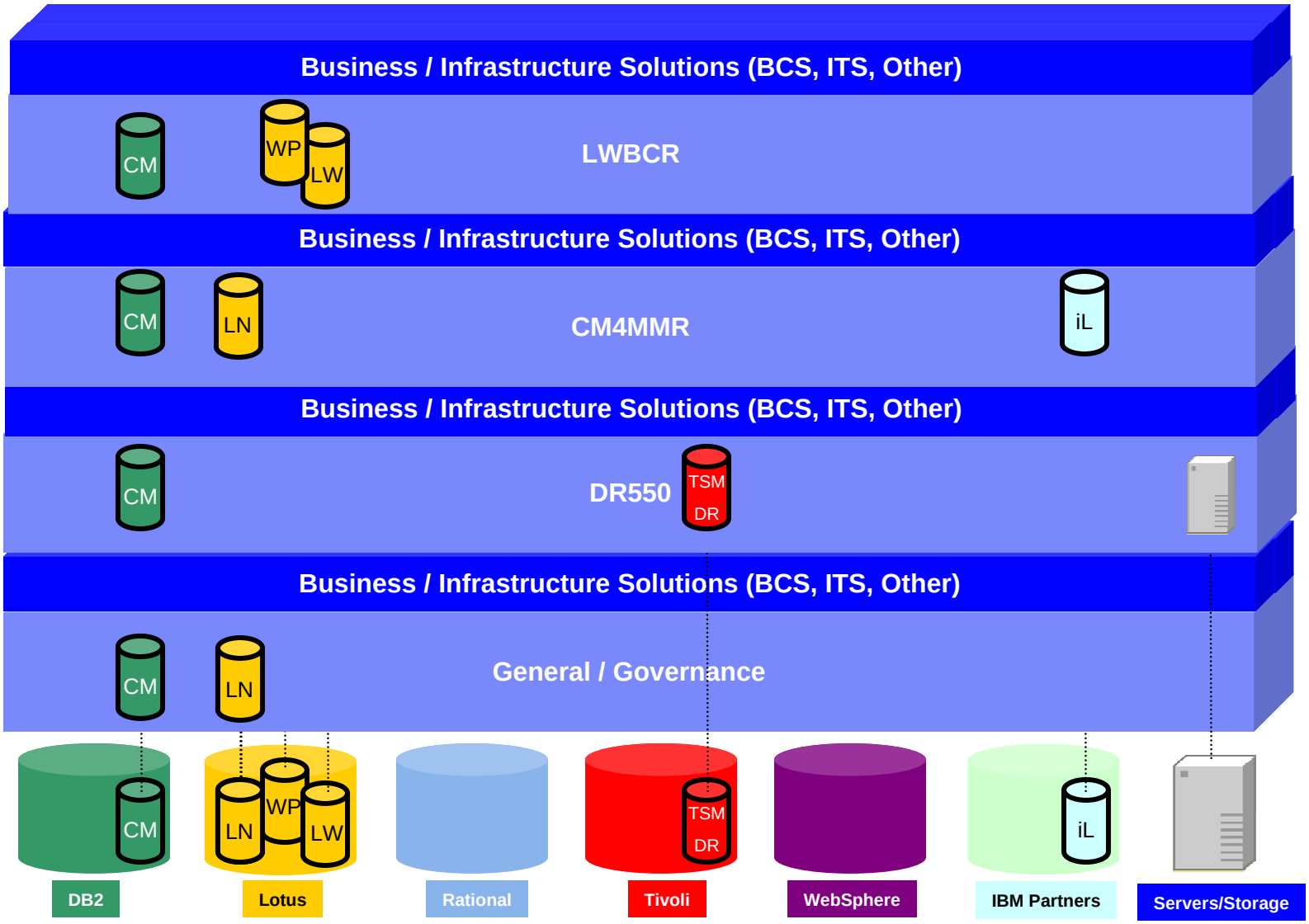
© 2005 IBM Corporation

Solution Integration Example - 1



© 2005 IBM Corporation

Solution Integration Example - 2



© 2005 IBM Corporation

IBM Workplace for Business Controls and Reporting

Regulation	**The Sarbanes-Oxley Act of 2002 11 Sections e.g. 404, 409, 802, etc (all not supported today)**
Business Pain	**Management's inability to assess internal controls by fiscal year end 2004**
Target Customers	▪ **$75 M + Reported Revenue** ▪ **Public Traded Companies registered with SEC**
Influencer / Decision Maker / Who to Call On	**1.Power Sponsor – CEO, COO, CFO, Corp. Compliance Officer** **2.Decision Maker – VP of Risk Management VP of Plans & Controls, VP of Internal Audit, Controller, Committee** **3.Influencers – CIO, CTI, Director of IT, Corp. Records Mgr**
What the Solution Does	**Enables the documentation & evaluation of business processes that contribute to the financial statements.**
Solution Stack	**Lotus Workplace Business Controls & Reporting (Single Offering – Embedded Content) + optionally DB2 Records Manager**
Web Links	**http://www.lotus.com/products/product5.nsf/wdocs/bcghomepage**

© 2005 IBM Corporation

IBM Content Manager for Message Monitoring and Retention

Regulation	**SEC 17-a-4 / NASD 3010, 3110**
Business Pain	**Capture and preserve all correspondence (Incoming and outgoing mail – paper and electronic, Audio and Video & Web content) involved in investment trading between Brokers, Traders, and Dealers and their customers**
Target Customers	**All Financial Services, Banks, Insurance Organizations involved in Broker Dealer Investments**
Influencer / Decision Maker / Who to Call On	1.Power Sponsor – CEO, COO, CFO, Corp. Compliance Officer, 2.Decision Maker – VP of Risk Management, VP of Internal Audit, Committee 3.Influencers – Corp. Legal Counsel, CIO, CTI, Director of IT, Corp. Records Mgr
What the Solution Does	**Enables customer to capture, analyze, and apply retention as appropriate to message communications with customers regarding investment transactions.**
Solution Stack	**DB2 Content Manager, DB2 Records Manager, Tivoli Storage Manager, iLumin Assentor Message Manager**
Web Links	**External: http://www-306.ibm.com/software/data/cm/solution_cmmmr.html**

© 2005 IBM Corporation

IBM DB2 Records Manager

Regulation	**DoD 5015.12, PRO, SOX, HIPPA, SEC/NASD, FDA 21CFR11, EPA, FERC, NRC, Tread Act, OSHA**
Business Pain	**Regulatory, Legal, and Business Driven Records Retention Requirements**
Target Customers	**All regulated industries, state, local, and federal government agencies**
Influencer / Decision Maker / Who to Call On	**1.Power Sponsor – CEO, COO, CFO, CCO, Corp. Legal Counsel** **2.Decision Maker – VP of Risk Management, VP of Internal Audit, CIO, Committee** **3.Influencers – CTI, Director of IT, Corp. Records Mgr**
What the Solution Does	**Enables the application of formal, structured retention and disposition rules to the organization's business information. These rules can be based on any combination of time and/or event.**
Solution Stack	**DB2 Records Manger (Single Product) integrated with one or more content repositories and business applications**
Key Web Links	**External: http://www-306.ibm.com/software/data/cm/cmgr/rm/**

© 2005 IBM Corporation

IBM DB2 Content Manager for Research Compliance

Regulation	**NASD 2711 / NYSE 47**
Business Pain	**Compliance with government regulations around the area of dissemination and reuse of financial research.**
Target Customers	**Brokers, dealers, mutual fund companies and companies who manage funds and portfolios, financial advisor firms, financial research companies**
Influencer / Decision Maker / Who to Call On	**Power Sponsor – CEO, COO, CFO, Corp. Compliance Officer** **Decision Maker – VP of Risk Management, VP of Plans & Controls, VP of Internal Audit, Controller, Committee** **Influencers – CIO, Fund Managers, Analyst Managers**
What the Solution Does	**Ingests financial information from sources, and makes it available to analysts for reuse and republishing in a controlled and auditable process to ensure fair distribution.**
Solution Stack	**DB2 Content Manager, DB2 Document Manager, and IBM services.** **Optional – DB2 Records Manager**
Web Links	**External: http://www-306.ibm.com/software/data/cm/industry_researchcomply.html**

IBM TotalStorage DR550

Regulation	**The Sarbanes-Oxley Act of 2002 11 Sections e.g. 404, 409, 802, etc (all not supported today); E-mail archiving and data retention (SEC 17a-4; NASD 3010/311**
Business Pain	**Growing challenge of managing and securing retention managed data and other critical information assets with operational efficiency.**
Target Customers	▪ **$75 M + Reported Revenue** ▪ **Public Traded Companies registered with SEC**
Influencer / Decision Maker / Who to Call On	**1.Power Sponsor – CEO, COO, CFO, Corp. Compliance Officer** **2.Decision Maker – VP of Risk Management VP of Plans & Controls, VP of Internal Audit, Controller, Committee** **3.Influencers – CIO, CTI, Director of IT, Corp. Records Mgr**
What the Solution Does	**Designed to facilitate compliance with the most stringent regulatory requirements in the most flexible and function-rich manner. It helps mange and simplify the retrieval of the ever increasing amount of data that organizations must retain for strict records retention regulations.**
Solution Stack	**Tivoli Storage Manager for Data Retention**
Web Links	**External url:** **http://www.storage.ibm.com/disk/dr/index.html**

IBM WebSphere Business Integrator for HIPAA

Regulation	**Health Insurance Portability and Accountability Act (HIPAA)**
Business Pain	**Exchange transactions in a secure, real-time, batch environment**
Target Customers	▪ **Life Science** ▪ **Health Care**
Influencer / Decision Maker / Who to Call On	**1.Power Sponsor – CEO, COO, CFO, Corp. Compliance Officer** **2.Decision Maker – VP of Risk Management VP of Plans & Controls, VP of Internal Audit, Controller, Committee** **3.Influencers – CIO, CTI, Director of IT, Corp. Records Mgr**
What the Solution Does	**IBM WebSphere Business Integration for HIPAA offers solutions that meet healthcare organizations' HIPAA needs and deliver improved results through implementation of a proven, reusable and supportable integration technology. It is designed to allow healthcare companies to securely exchange transactions in simultaneous real-time and batch environments.**
Solution Stack	**WebSphere Business Integration Trading Partner Interchange Adapters; WebSphere Data Interchange; WebSphere Business Integration Server**
Web Links	**External url: http://www-306.ibm.com/software/info1/websphere/index.jsp?tab=solutions/wbiinshipaa&S_TACT=103BHW06**

© 2005 IBM Corporation

Conclusion

- Compliance is a continuous process, not a project
- Sustainability of compliance needs to be an integral part of any compliance strategy
- Companies that put in place a compliance architecture may receive significant benefits
- Risk is an integral part of compliance

© 2005 IBM Corporation

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCO, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/30, VM/ESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/VM

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

LINUX is a registered trademark of Linux Torvalds

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation

* All other products may be trademarks or registered trademarks of their respective companies.

NOTES:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

© 2005 IBM Corporation

BACKUP CHARTS

© 2005 IBM Corporation

Risk and Compliance Data

- **The following slide contains a spreadsheet that identifies components that may be applicable to clients by regulation type**
- **The components included in the spreadsheets were selected by using the following criteria**
  - *If the functionality was explicitly mentioned in a regulation*
  - *If the functionality was implied by a regulation, or necessary for generally accepted best practices*

  Each column contains the regulation type
- **Each row contains the name of a component**
- **Each component has the following designation per regulation type**
  - *1 – Area of primary focus*
  - *2 – Area of secondary focus*

© 2005 IBM Corporation

Risk and Compliance Components per Regulation Type

	Corporate Governance	Business Improvement	Business Resilience	Transaction Integrity	Information Protection	Information Lifecycle Mgt
Biz Perf Mgt	2	2				
Biz Process Mgt	2	2		2	2	
Risk Mgt	1	1	2	2	2	
Comp. Monitoring	1	2	1	1	1	2
Reporting	1	1	2	1	1	1
Analytics	1	1	2	2		2
Collab/Workflow	1	2	2	1		2
Training	2			1	1	
Capture	1		2	1	2	1
Indexing	2	2	2	2	2	1
Retention Mgt	1		1	1	2	1
Data Authentication	1		2	1	1	2
Archival	1	2	2	2	1	1
Info Integrity	1		2	2	2	2
Info Integration	2	2		2	2	2
Records Mgt	2		2	2	1	1
Data Privacy	1			2	1	
Content Mgt	2		2	2	2	1
Search/Retrieve	1		2	1	2	1
Clean/Proc		2	2	2		2
LoB Systems	1	1	1	1	1	
Security	1	1	1	1	1	1
Identity Mgt	1	1	1	1	1	1
Access Control	1	1	1	1	1	1
Authentication	1	1	1	1	1	1
Encryption	2	2	2	2	1	2
Audit Control	1	1	1	1	1	1
Infrastructure	1	1	1	1	1	1
Resiliency	1	1	1	1	1	1

© 2005 IBM Corporation

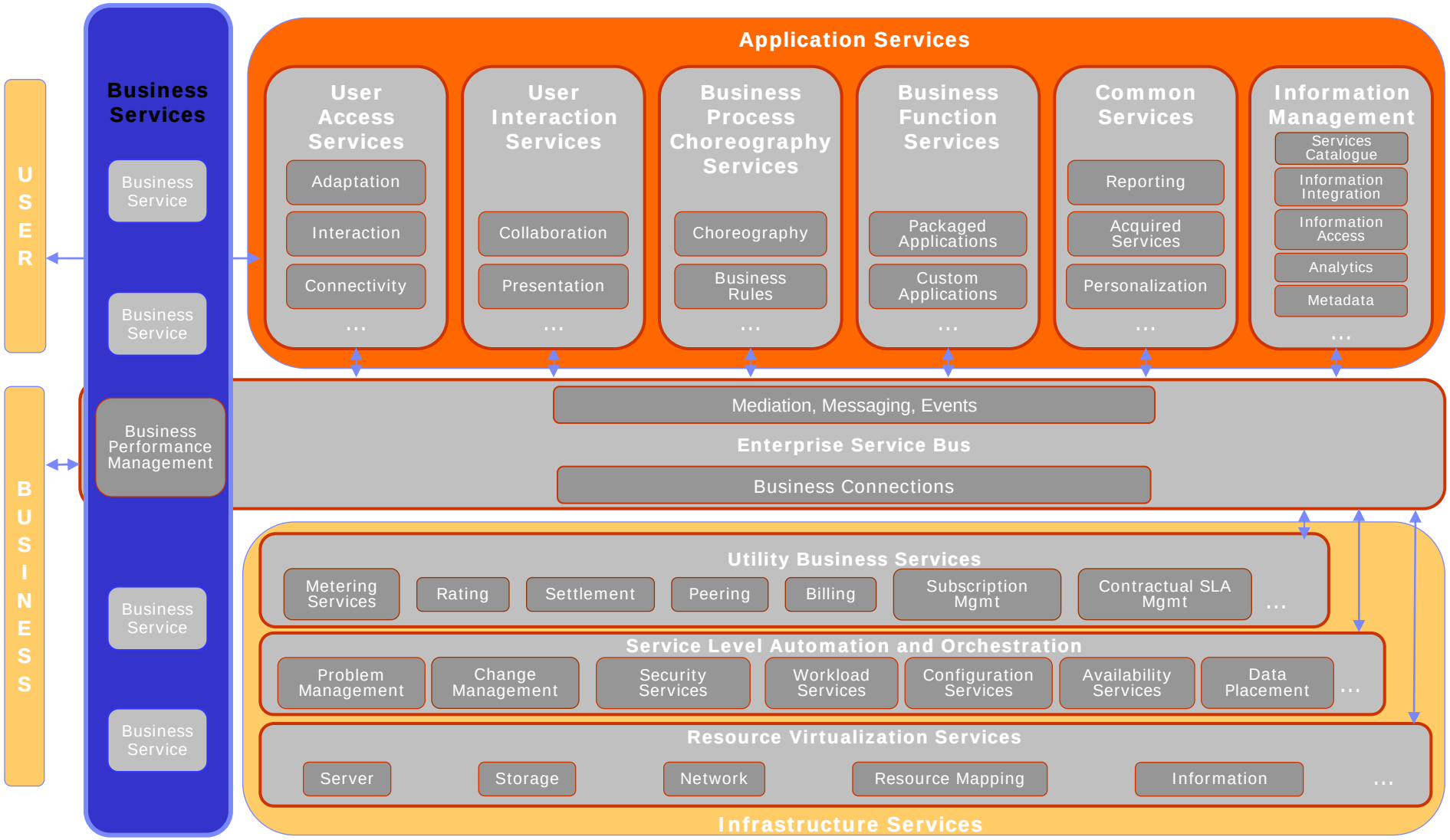
Risk and Compliance Framework Mappings

- **The following slides show how the Risk and Compliance framework maps to other architecture and frameworks**
- **It highlights what areas of these architectures and frameworks should be focused on when creating a compliance architecture**

- ***NOTE***
  - *These slides contain animations, so you should be in screen show mode to view them*

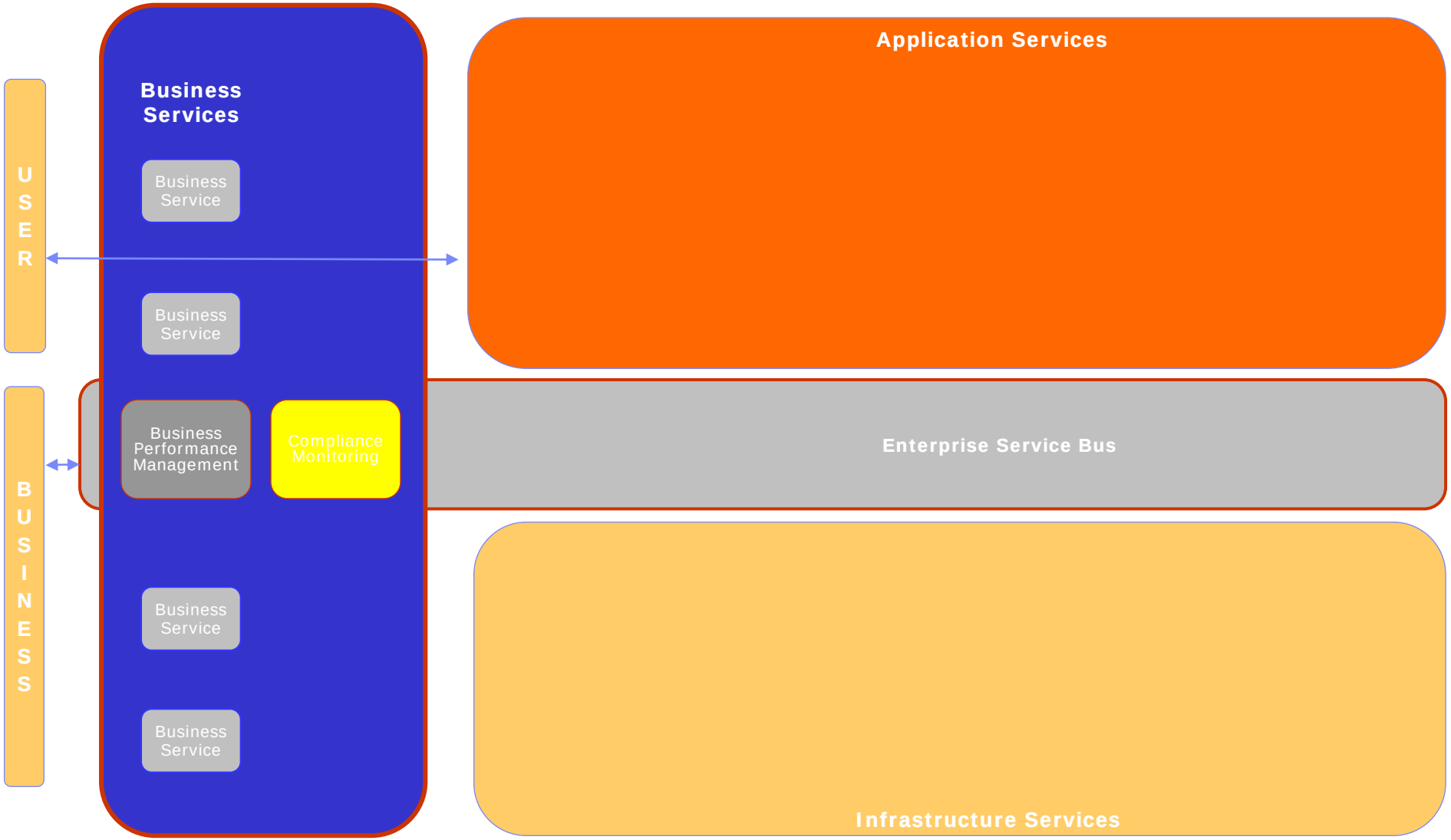
© 2005 IBM Corporation

Risk and Compliance Framework mapping to the On Demand Operating Environment



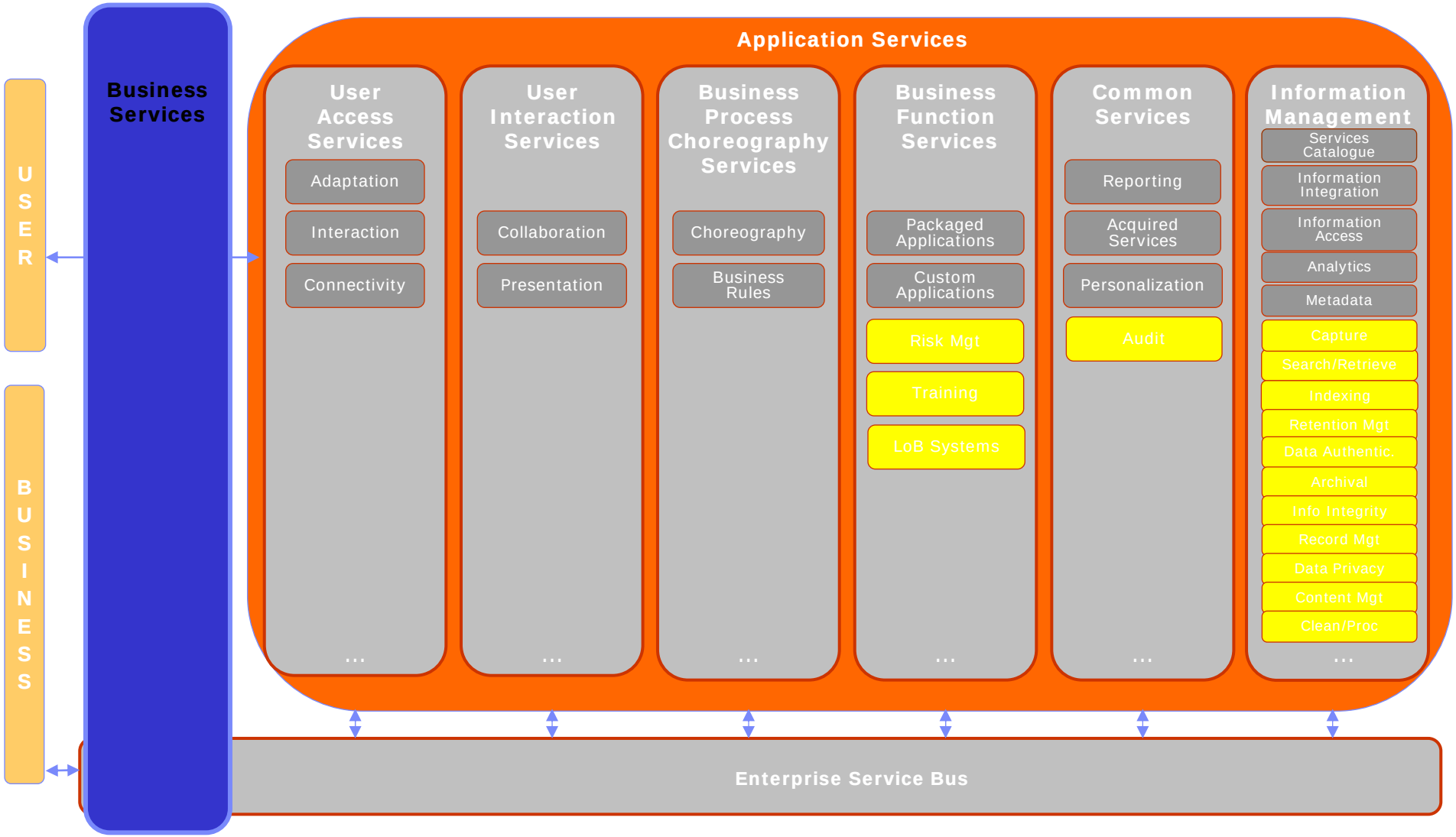
© 2005 IBM Corporation

Risk and Compliance Framework mapping to the On Demand Operating Environment



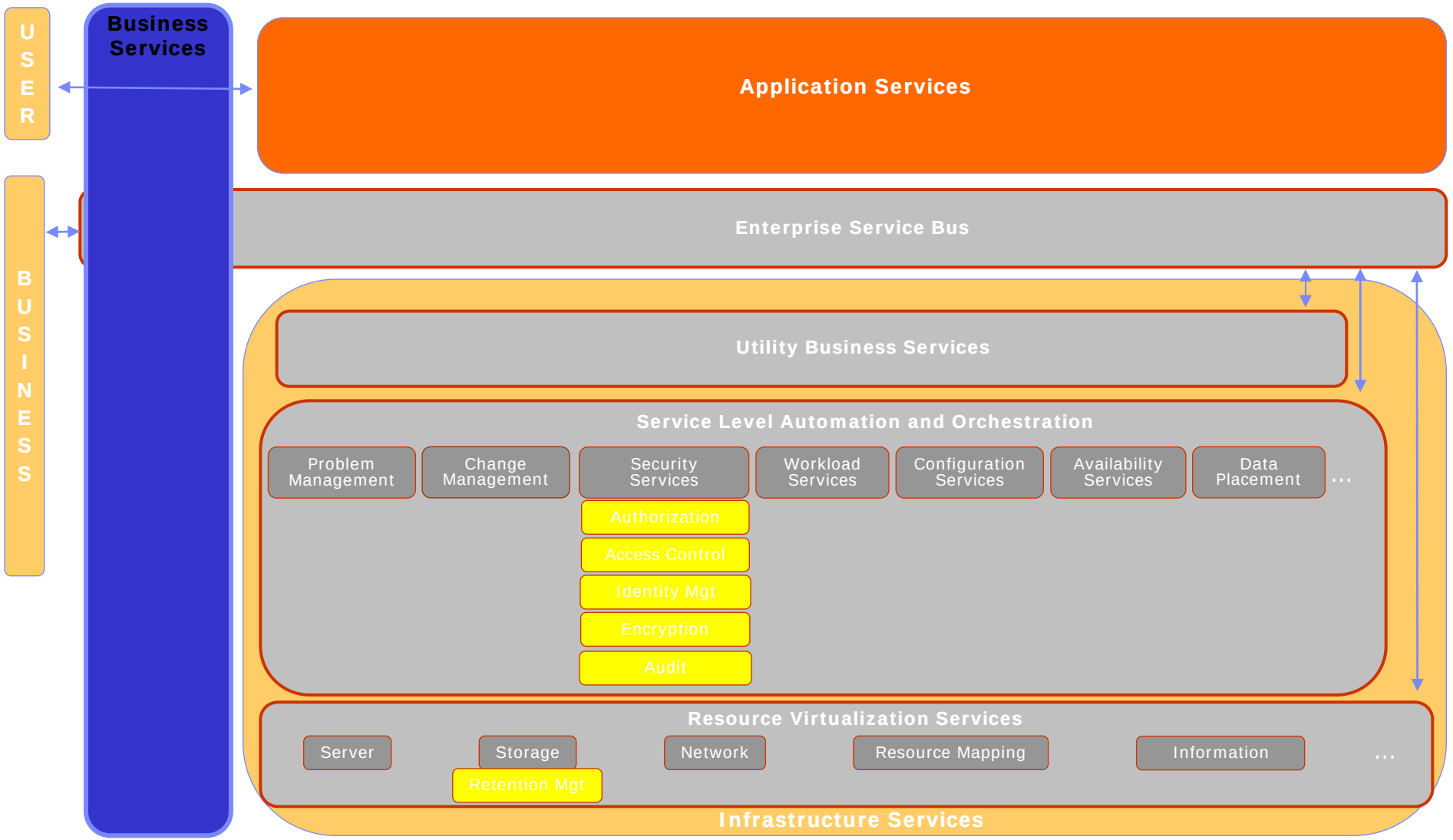
© 2005 IBM Corporation

Risk and Compliance Framework mapping to the On Demand Operating Environment



© 2005 IBM Corporation

Risk and Compliance Framework mapping to the On Demand Operating Environment



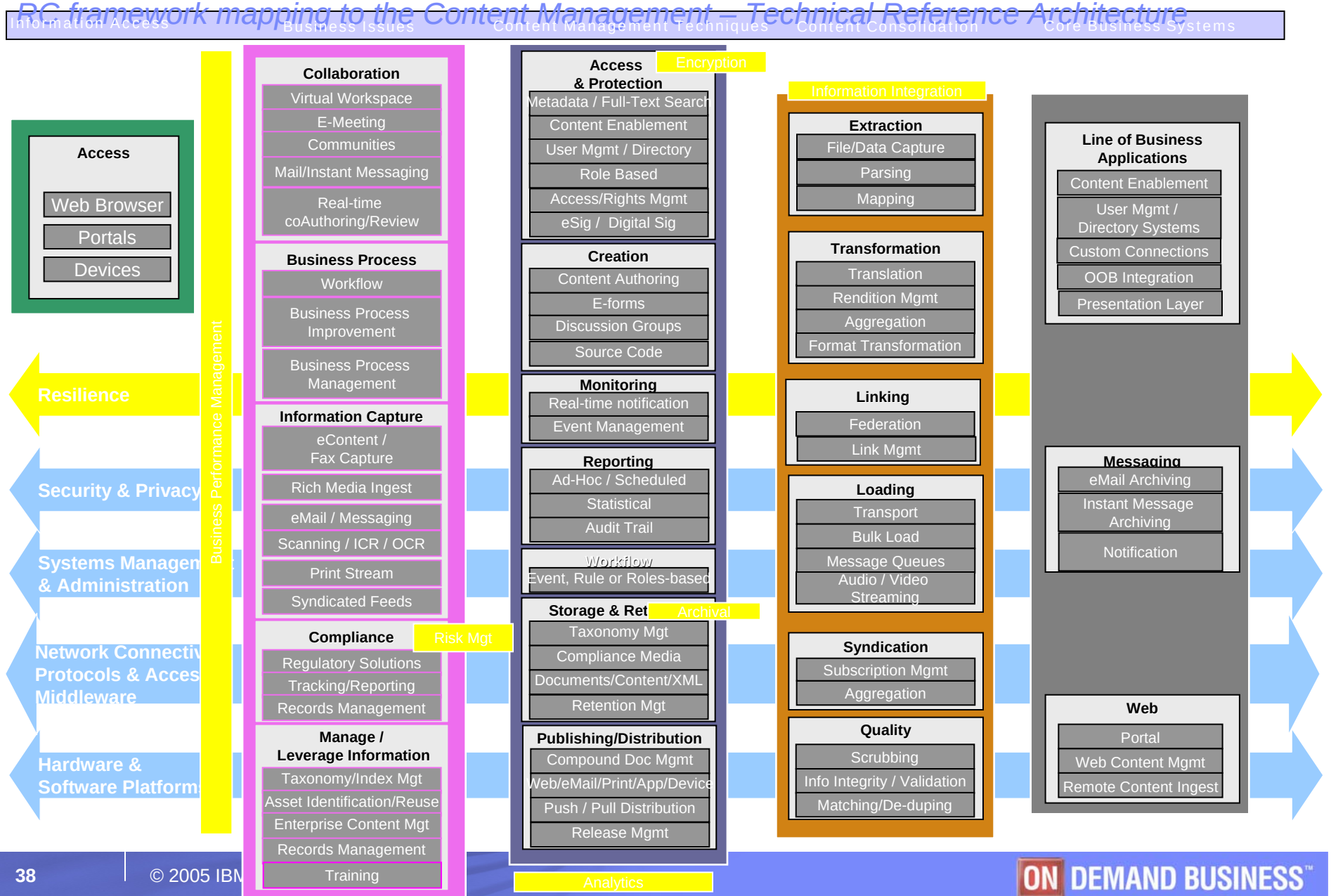
© 2005 IBM Corporation

Risk and Compliance Framework mapping to the ODOE capabilities

	Business Modeling	Process Transformation	Access	Collaboration	Application and Information Integration	Business Process Management	Availability	Security	Optimization	Provisioning	Policy-based Orchestration	Business Service Management	Resource Virtualization
Biz Perf Mgt	x	x		x	x	x							
Biz Process Mgt						x							
Risk Mgt	x			x		x							
Comp. Monitoring	x			x		x							
Reporting													
Analytics						x							
Collab/Workflow			x	x									
Training				x									
Capture					x	x							
Indexing					x								
Retention Mgt						x							
Data Authentication					x			x					
Archival						x							
Info Integrity					x								
Info Integration					x								
Records Mgt						x							
Data Privacy					x	x							
Content Mgt					x								
Search/Retrieve					x								
Clean/Proc					x								
LoB Systems													
Security								x					
Identity Mgt								x					
Access Control								x					
Authentication								x					
Encryption								x					
Audit Control								x					
Infrastructure													
Resiliency							x	x					

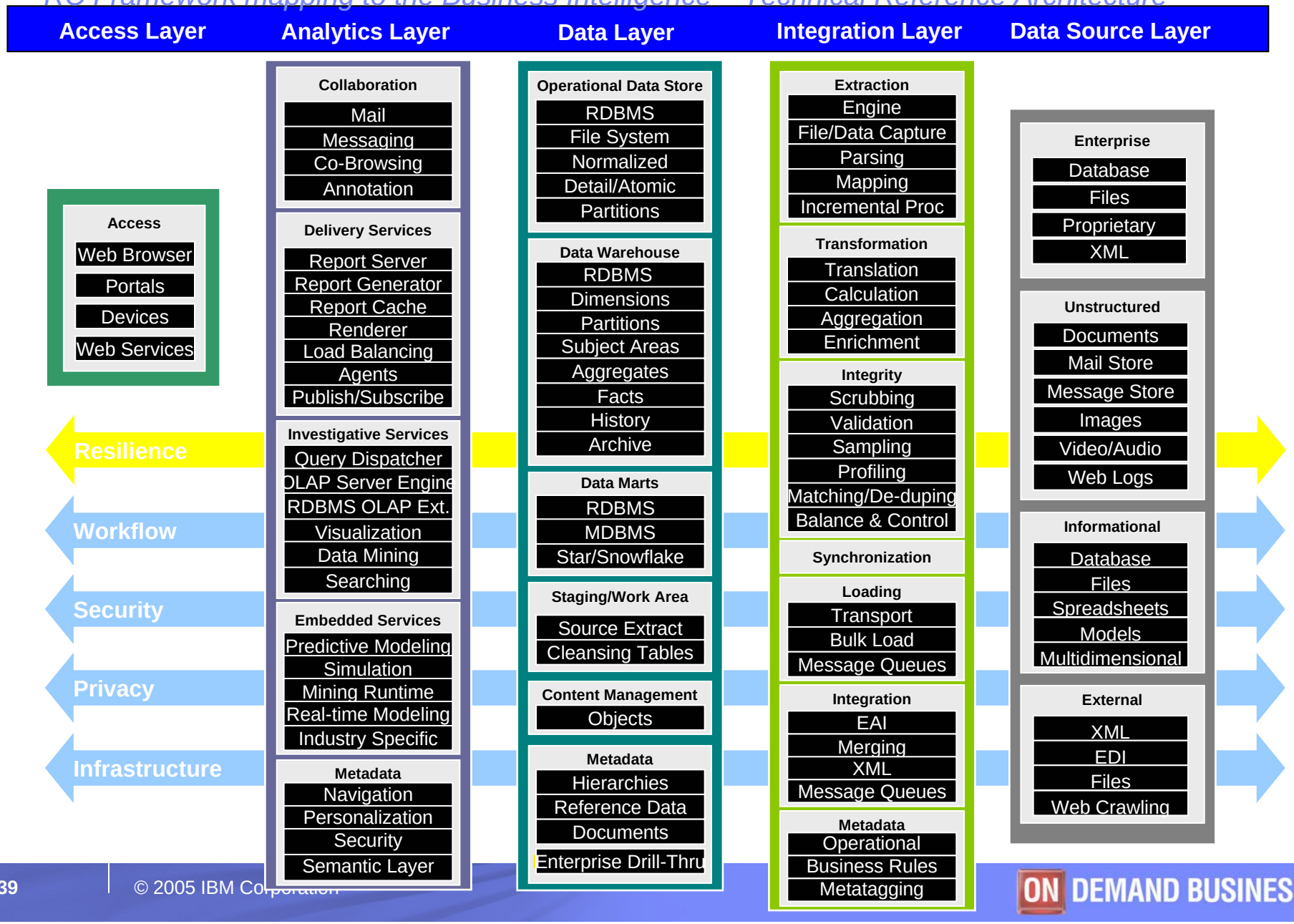
© 2005 IBM Corporation

RC framework mapping to the Content Management – Technical Reference Architecture



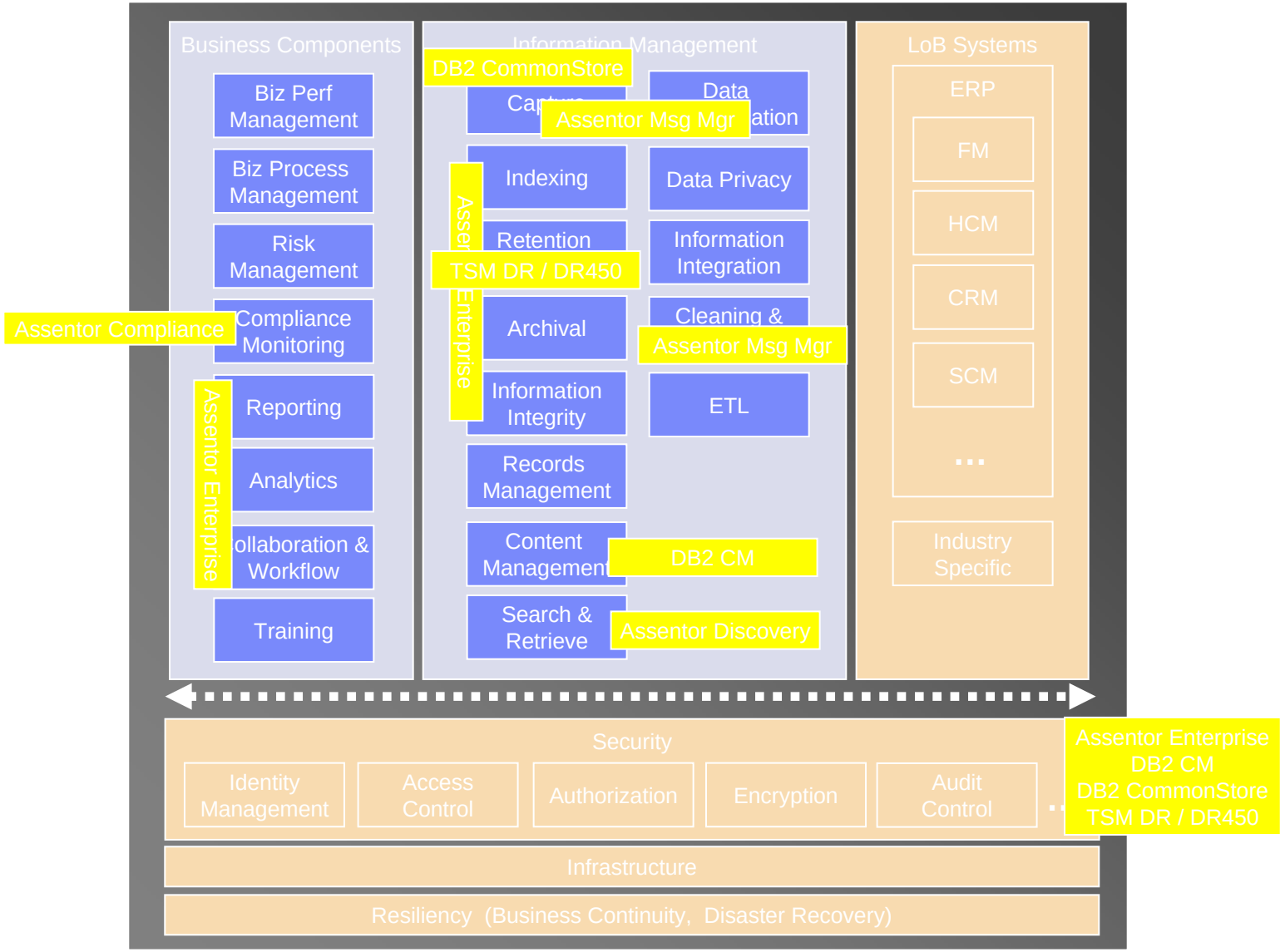
© 2005 IBM

RC Framework mapping to the Business Intelligence – Technical Reference Architecture



© 2005 IBM Corporation

RC Framework mapping of the Content Manager for Message Monitoring and Retention Solution



© 2005 IBM Corporation

Risk and Compliance Framework (Misc. Data)

- **Double click on the glossary to view the definition of the terms included on the risk and compliance framework**

Glossary

Microsoft Excel Worksheet

- **The following spreadsheet contains the product mappings used in the interactive slides**

- ***NOTE***

© 2005 IBM Corporation

Contributors

Name	Business Unit	Job Responsibility
Birgit Pfitzmann/Zurich/IBM	CHQ/Research	Fed Identity Mgmt, Privacy, Web Svcs Security
Jurij R Paraszczak/Watson/IBM	CHQ/Research	CTO VC Relation, Dir VC Relations EBO
Steven Y Wang/Somers/IBM	CHQ/Strategy	Corp Strategy Staff
Brian E Engesser/Somers/IBM	IGS	Marketing
Juliette Paquin/Boulder/IBM	IGS/Application Management Services	Channel Manager, Portals, Content and e-Commerce
Scott Sumner-Moore/San Francisco/IBM	IGS/Application Management Services	Senior IT Architect, Portals, Content and e-Commerce
Larry W Gosselin/Atlanta/IBM	IGS/Business Consulting Services	BCS Financial Mgt / BI Global Alliances & Tech Director
David G Wood/Cedar Rapids/IBM	IGS/Integrated Technology Services	Managing Consultant, Business Resilience and Continuity Ser
David Weeshoff/Los Angeles/IBM	Sales & Distribution	Check Processing Systems Strategy (Check 21)
Jonathan M Rosenoer/San Francisco/IBM	Sales & Distribution	Global Head of Op. Resilience & Risk Sol. - FSS
Paul B Morris/Southbury/IBM	Sales & Distribution	Risk & Compliance Program Mgmt Office - IBM Global Solutio
Robert F Jacobs/Norwalk/IBM	Sales & Distribution	Regulatory, Global Pharma
Tim McCrimmon/Raliegh/IBM	Software Group	Program Director, On Demand Marketing
Fredrik Carlegren/Raleigh/IBM	Software Group	Strategy & Executive Communications; on demand Operating
Marc-Thomas Schmidt/Somers/IBM	Software Group/Application Integration Middleware	Distinguished Engineer, Enterprise Service Bus (ODOE)
Pat G O'Sullivan/Ireland/IBM	Software Group/Application Integration Middleware	IFW Development Manager (BDW)
Wayne A Perry/Silicon Valley/IBM	Software Group/Application Integration Middleware	Senior Marketing Manager, SWG Industry Solutions
Frederik Soendergaard-Jensen/Somers/IBM	Software Group/Database Management	Director, IBM Risk & Compliance Council
Lisa Leahy/Charlotte/IBM	Software Group/Database Management	Channel Manager, IBM Risk and Compliance Council
Paul R Friedberg/Boston/IBM	Software Group/Database Management	Project Manager, IBM Risk and Compliance Council
Stan Muse/Atlanta/IBM	Software Group/Database Management	Solution Architect (ISSD BP Tech. Enablement) (Basel)
Teresa Bradford/Raleigh/IBM	Software Group/Database Management	Marketing Manager, IBM Risk & Compliance Council
Francine R Frazer/Costa Mesa/IBM	Software Group/Database Management	BI Solutions Strategy and Architecture
Harold Moss/Westford/IBM	Software Group/Lotus	Program Engineering Mgr Industry Solutions (SOX)
Donald Cronin/Raleigh/IBM	Software Group/Tivoli	Corporate Security Strategy Team
Steven Adler/Somers/IBM	Software Group/Tivoli	Program Dir, Enterprise Privacy Solutions
Toby Marek/San Jose/IBM	Software Group/Tivoli	Stg Management Architecture and Technology
Alan Stuart/White Plains/IBM	Systems Group	Chief Strategist and BLE, Data Retention Solutions

© 2005 IBM Corporation