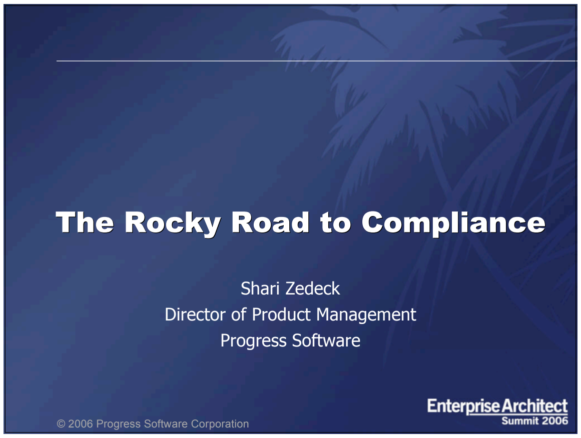
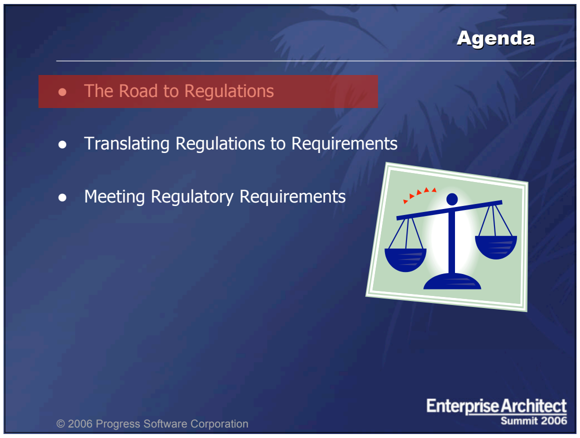


The Rocky Road to Compliance

Shari Zedeck
Director of Product Management
Progress Software

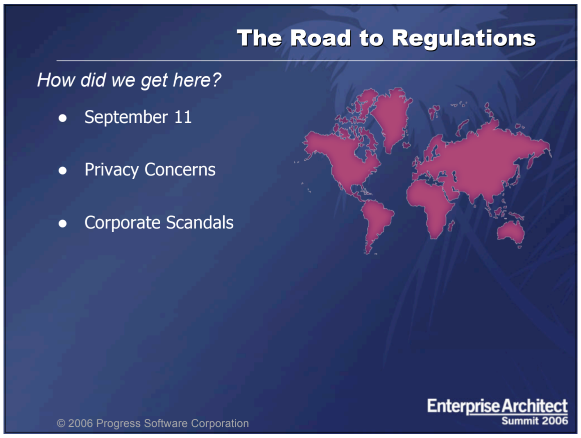
Enterprise Architect Summit 2006



Agenda

- The Road to Regulations
- Translating Regulations to Requirements
- Meeting Regulatory Requirements

Enterprise Architect Summit 2006

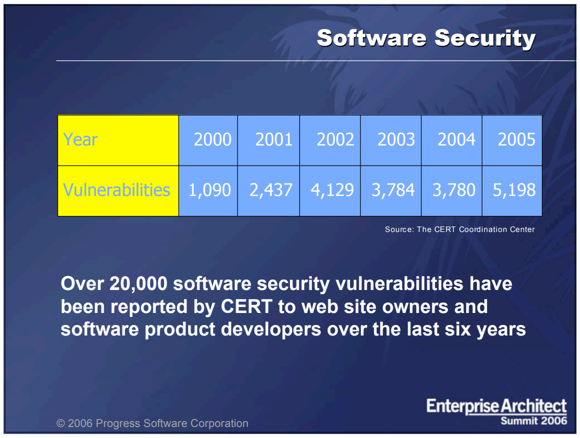


The Road to Regulations

How did we get here?

- September 11
- Privacy Concerns
- Corporate Scandals

Enterprise Architect Summit 2006



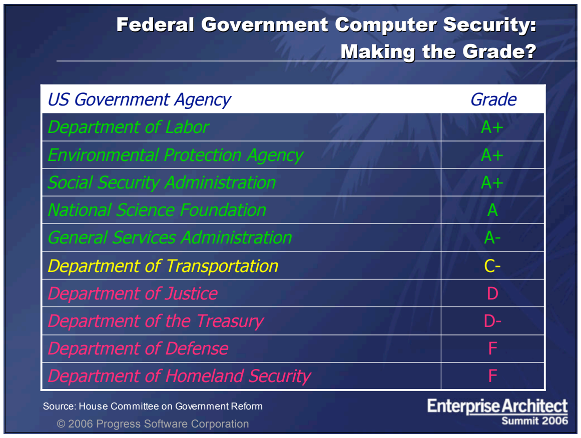
Software Security

Year	2000	2001	2002	2003	2004	2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,198

Source: The CERT Coordination Center

Over 20,000 software security vulnerabilities have been reported by CERT to web site owners and software product developers over the last six years

Enterprise Architect Summit 2006



Federal Government Computer Security: Making the Grade?

US Government Agency	*Grade*
Department of Labor	A+
Environmental Protection Agency	A+
Social Security Administration	A+
National Science Foundation	A
General Services Administration	A-
Department of Transportation	C-
Department of Justice	D
Department of the Treasury	D-
Department of Defense	F
Department of Homeland Security	F

Source: House Committee on Government Reform

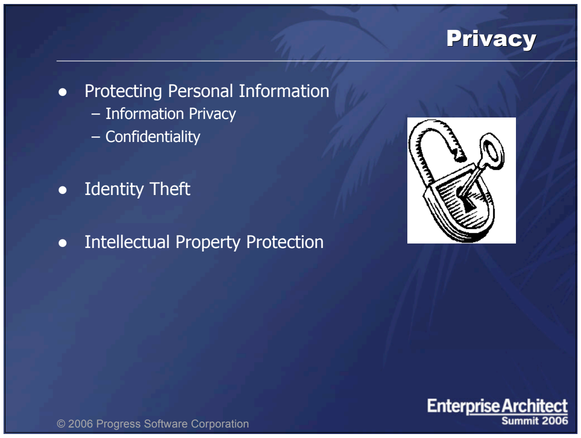
Enterprise Architect Summit 2006

Who Cares about Security?

Government Agencies and SIGs Worldwide

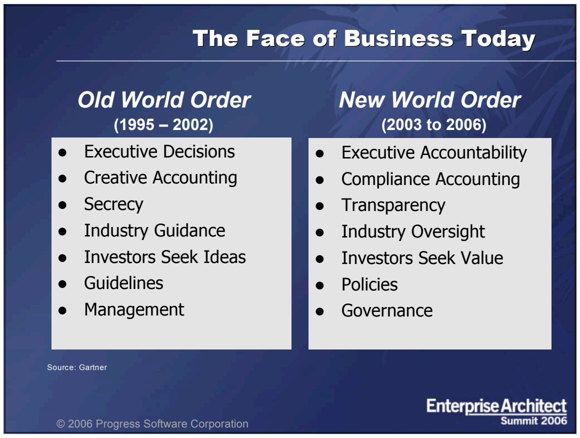
AusCERT
Australian Computer Emergency Response Team
U.S. Department of Homeland Security
Federal Computer Incident Response Center
NCS
IETF
NANOG
GSA U.S. General Services Administration
Public Safety and Emergency Preparedness Canada
National Security Telecommunications Advisory Committee (NSTAC)
FIRST
Forum of Incident Response and Security Teams
INTERNET SECURITY ALLIANCE

Enterprise Architect Summit 2006



Privacy

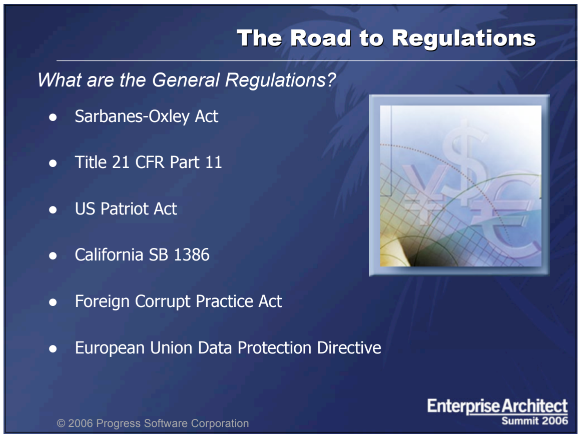
- Protecting Personal Information
  - Information Privacy
  - Confidentiality
- Identity Theft
- Intellectual Property Protection



The Face of Business Today

Old World Order (1995 – 2002)	*New World Order* (2003 to 2006)
Executive Decisions	Executive Accountability
Creative Accounting	Compliance Accounting
Secrecy	Transparency
Industry Guidance	Industry Oversight
Investors Seek Ideas	Investors Seek Value
Guidelines	Policies
Management	Governance

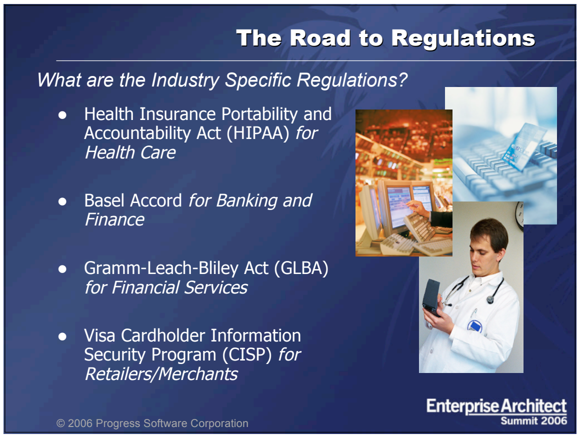
Source: Gartner



The Road to Regulations

What are the General Regulations?

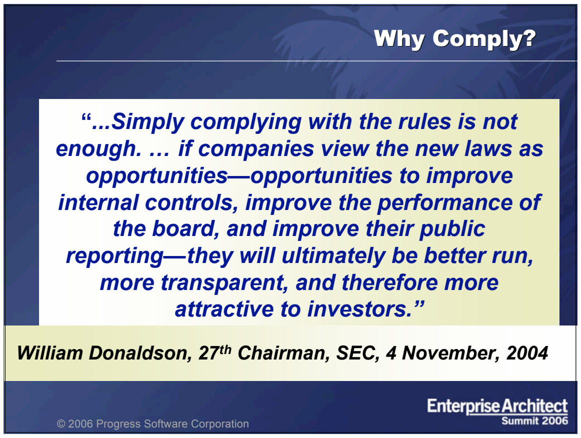
- Sarbanes-Oxley Act
- Title 21 CFR Part 11
- US Patriot Act
- California SB 1386
- Foreign Corrupt Practice Act
- European Union Data Protection Directive



The Road to Regulations

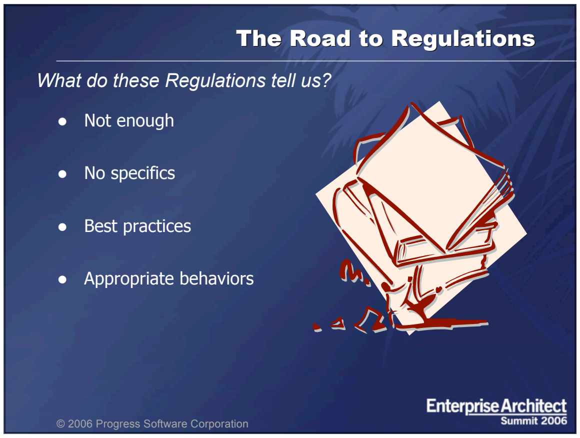
What are the Industry Specific Regulations?

- Health Insurance Portability and Accountability Act (HIPAA) *for Health Care*
- Basel Accord *for Banking and Finance*
- Gramm-Leach-Bliley Act (GLBA) *for Financial Services*
- Visa Cardholder Information Security Program (CISP) *for Retailers/Merchants*



Why Comply?

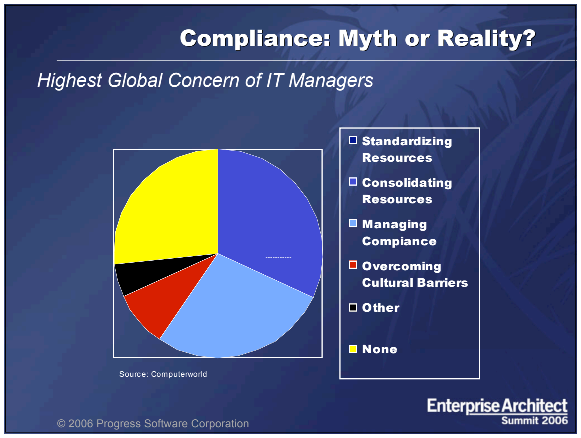
> ***"…Simply complying with the rules is not enough. … if companies view the new laws as opportunities—opportunities to improve internal controls, improve the performance of the board, and improve their public reporting—they will ultimately be better run, more transparent, and therefore more attractive to investors."***
>
> ***William Donaldson, 27th Chairman, SEC, 4 November, 2004***



The Road to Regulations

What do these Regulations tell us?

- Not enough
- No specifics
- Best practices
- Appropriate behaviors

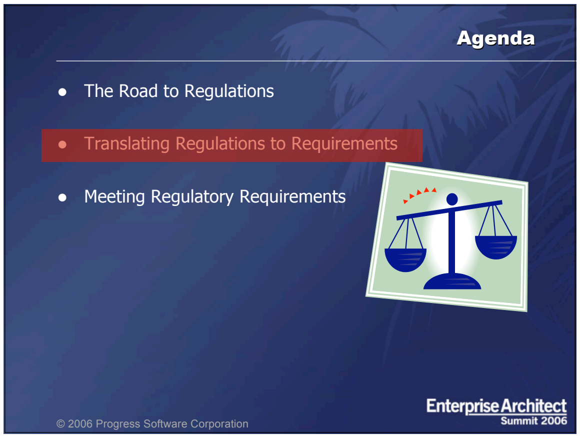


Compliance: Myth or Reality?

Highest Global Concern of IT Managers

Source: Computerworld

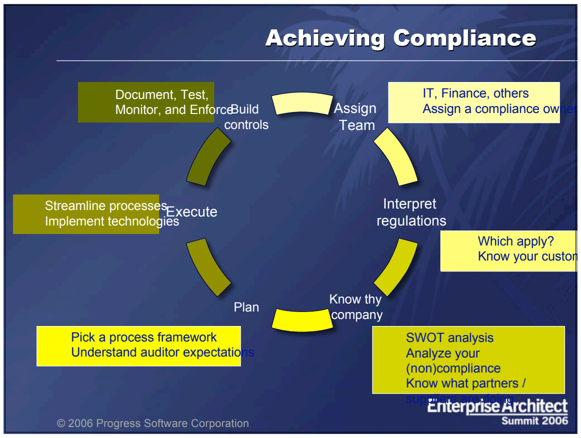
Enterprise Architect Summit 2006



Agenda

- The Road to Regulations
- Translating Regulations to Requirements
- Meeting Regulatory Requirements

Enterprise Architect Summit 2006



Achieving Compliance

Assign Team

IT, Finance, others
Assign a compliance owne

Interpret regulations

Which apply?
Know your custon

Know thy company

SWOT analysis
Analyze your (non)compliance
Know what partners / suppliers are doing

Plan

Pick a process framework
Understand auditor expectations

Execute

Streamline processes
Implement technologies

Build controls

Document, Test, Monitor, and Enforce

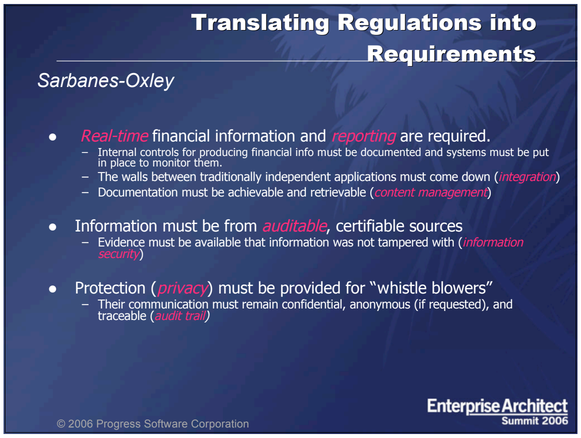
Enterprise Architect Summit 2006

Sarbanes-Oxley

What does it tell you?

- Leadership is accountable
- Conflicts of interest must be avoided
- Executive boards must include two Certified Public Accountants and three other "financially literate" members
- Companies must adopt standards of ethics and quality control for auditors and review compliance regularly
- Info gathered by the Board must remain confidential and privileged
- US SEC, Federal Reserve, and Treasury all have rights to administer necessary disciplinary action

Enterprise Architect Summit 2006

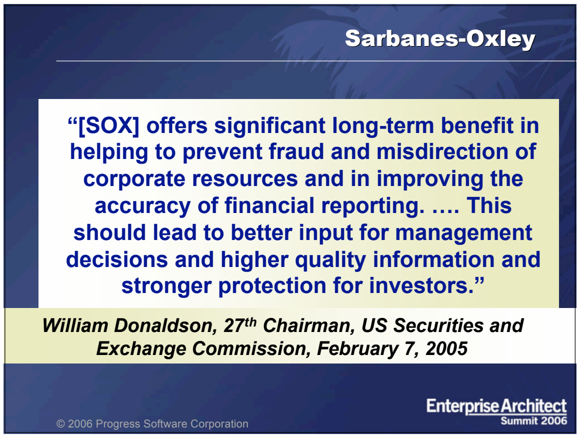


Translating Regulations into Requirements

Sarbanes-Oxley

- *Real-time* financial information and *reporting* are required.
  - Internal controls for producing financial info must be documented and systems must be put in place to monitor them.
  - The walls between traditionally independent applications must come down (*integration*)
  - Documentation must be achievable and retrievable (*content management*)
- Information must be from *auditable*, certifiable sources
  - Evidence must be available that information was not tampered with (*information security*)
- Protection (*privacy*) must be provided for "whistle blowers"
  - Their communication must remain confidential, anonymous (if requested), and traceable (*audit trail)*

Enterprise Architect Summit 2006



Sarbanes-Oxley

> **"[SOX] offers significant long-term benefit in helping to prevent fraud and misdirection of corporate resources and in improving the accuracy of financial reporting. …. This should lead to better input for management decisions and higher quality information and stronger protection for investors."**

William Donaldson, 27th Chairman, US Securities and Exchange Commission, February 7, 2005

Enterprise Architect Summit 2006

Gramm-Leach-Bliley Act

What does it tell you?

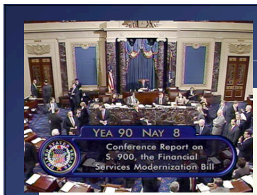
- Financial institutions must disclose their information privacy and information sharing policies
- Differentiate between "public" and "non-public" personal financial information
- Ensure the confidentiality of customer information:
  - Security of customer records and information
  - Protection against threats (on the security and integrity of data)
  - Prevention of unauthorized access / use of data that would cause inconvenience to or harm to a customer

Translating Regulations into Requirements

Gramm-Leach-Bliley Act

- Customers believe that personal financial info should be private - *make sure privacy policies are clear*
- Corporate customers demand similar protection for their financial info – *ensure its security / confidentiality*
- Background check internal staff to limit their becoming significant sources of sensitive info leaks (*security*)
- All points through which sensitive information pass must be *protected equally*, or all are liable
- Third-party service providers are subject to the same *risk management* and *information privacy policies* for transactions as if you were performing them directly – know your partners

Gramm-Leach-Bliley


YEA 90 NAY 8
Conference Report on S. 900, the Financial Services Modernization Bill

"The Gramm-Leach-Bliley Act … creates wholly new financial services organizations in America.

"Americans today spend about $350 billion on financial services – on fees and charges and interest. … there are tens of billions of dollars of savings for the American consumer that will be produced by the reforms of this bill."

Senator Phil Gramm – November 4, 1999

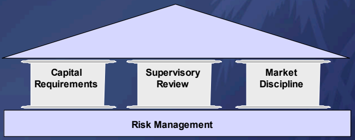
Basel Accord

What does it tell you?

- Banks and financial institutions must regulate risk
- Risk oversight, review and management procedures must be evaluated periodically
- Certain event types require risk assessment and regulatory treatment:
  - Internal and external fraud
  - Employment practices and workplace safety
  - Clients, products and business practices
  - Damage to physical assets
  - Business disruption and system failures

Translating Regulations into Requirements

Basel – The International Convergence of Capital Measurement and Capital Standards

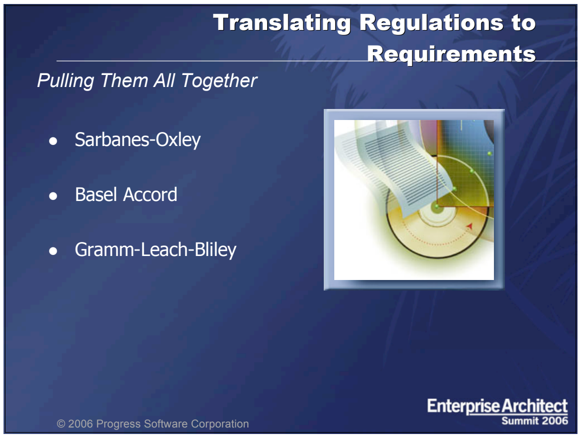


- Identifying, assessing, mitigating, transferring, controlling and monitoring credit, market and operational risks require information sharing via advanced *analytics*, *reporting*, and *integration* -- across an enterprise.

Basel Accord

"Basel provides banks with .. incentives … to improve their risk management systems and processes. The framework will help … ensure that capital supervision continues to serve as a cornerstone to safety and soundness in the banking system. Both … make banks more resilient, less sensitive to the ups and downs of the business cycle, and better able to serve as a source of credit and growth for businesses and consumers."

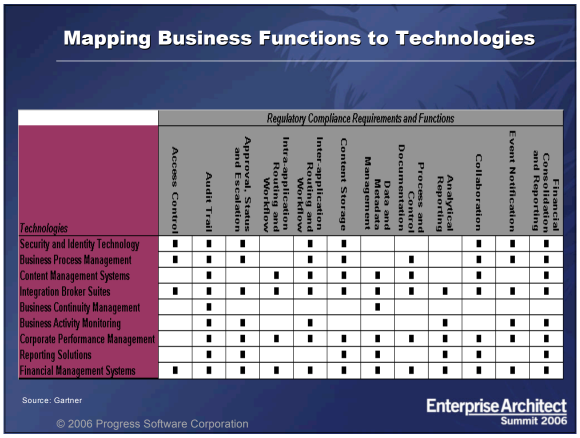
Jaime Caruana, Governor of the Bank of Spain and Chairman of the Basel Committee, 11 November 2004



Translating Regulations to Requirements

Pulling Them All Together

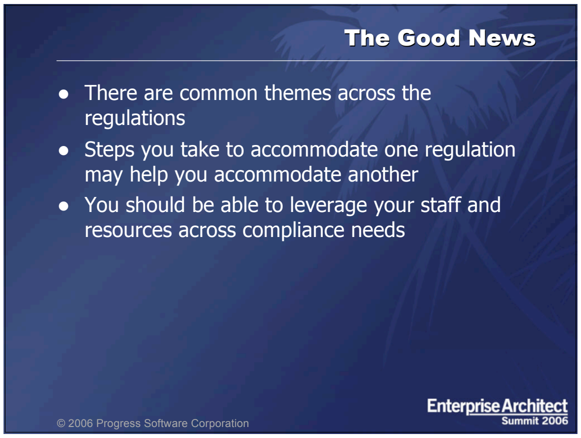
- Sarbanes-Oxley
- Basel Accord
- Gramm-Leach-Bliley



Mapping Business Functions to Technologies

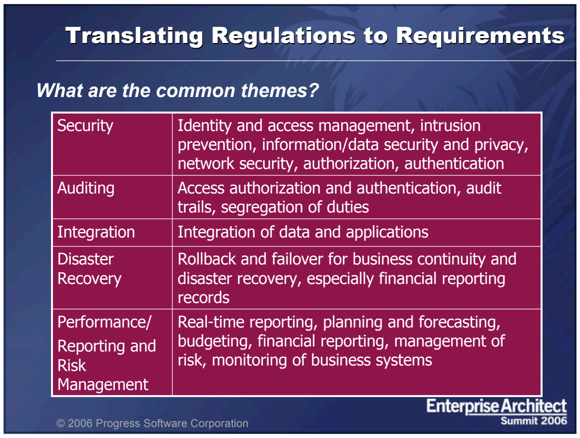
	Regulatory Compliance Requirements and Functions											
Technologies	Access Control	Audit Trail	Approval, Status and Escalation	Intra-application Routing and Workflow	Inter-application Routing and Workflow	Content Storage	Data and Metadata Management	Process and Control Documentation	Analytical Reporting	Collaboration	Event Notification	Financial Consolidation and Reporting
Security and Identity Technology	■	■	■		■	■				■	■	■
Business Process Management	■	■	■		■	■		■		■	■	■
Content Management Systems		■		■	■	■	■	■		■		■
Integration Broker Suites	■	■	■	■	■	■	■	■	■	■	■	■
Business Continuity Management		■					■					
Business Activity Monitoring		■	■		■				■		■	■
Corporate Performance Management		■	■	■	■	■	■	■	■	■	■	■
Reporting Solutions		■	■			■	■		■	■		■
Financial Management Systems	■	■	■	■	■	■	■	■	■	■	■	■

Source: Gartner



The Good News

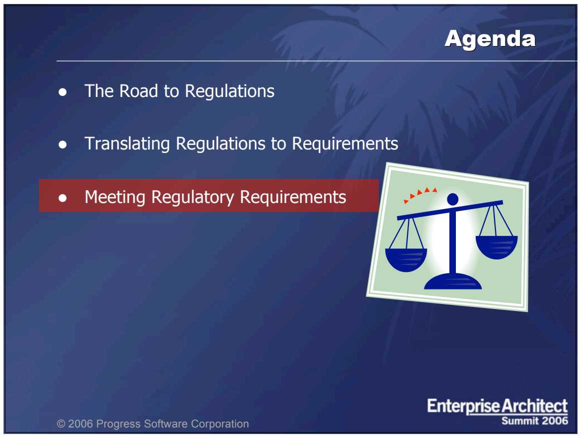
- There are common themes across the regulations
- Steps you take to accommodate one regulation may help you accommodate another
- You should be able to leverage your staff and resources across compliance needs



Translating Regulations to Requirements

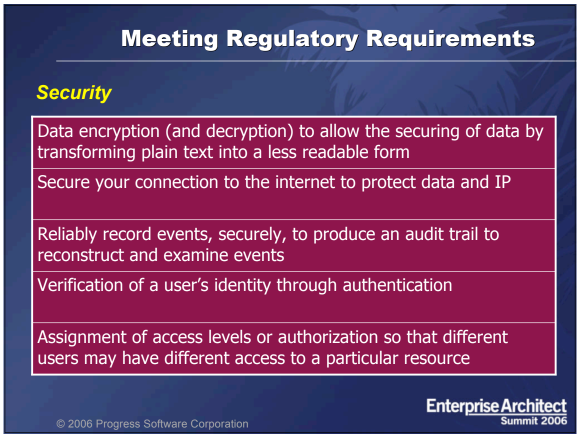
What are the common themes?

Security	Identity and access management, intrusion prevention, information/data security and privacy, network security, authorization, authentication
Auditing	Access authorization and authentication, audit trails, segregation of duties
Integration	Integration of data and applications
Disaster Recovery	Rollback and failover for business continuity and disaster recovery, especially financial reporting records
Performance/ Reporting and Risk Management	Real-time reporting, planning and forecasting, budgeting, financial reporting, management of risk, monitoring of business systems



Agenda

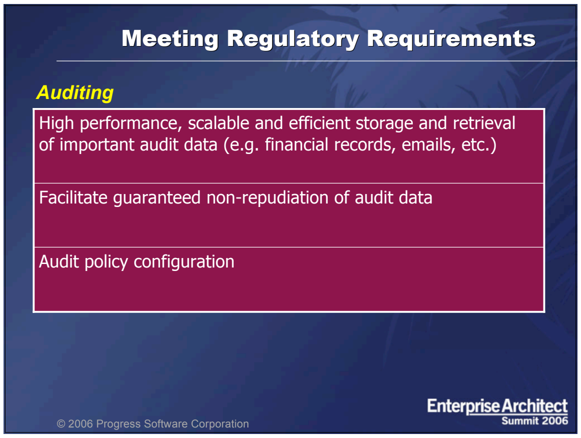
- The Road to Regulations
- Translating Regulations to Requirements
- Meeting Regulatory Requirements



Meeting Regulatory Requirements

Security

Data encryption (and decryption) to allow the securing of data by transforming plain text into a less readable form
Secure your connection to the internet to protect data and IP
Reliably record events, securely, to produce an audit trail to reconstruct and examine events
Verification of a user's identity through authentication
Assignment of access levels or authorization so that different users may have different access to a particular resource

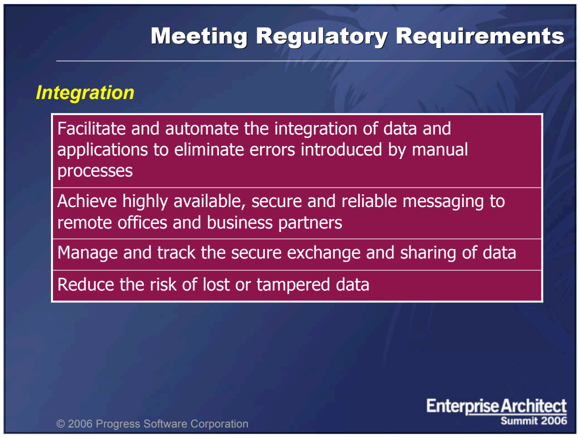


Meeting Regulatory Requirements

Auditing

High performance, scalable and efficient storage and retrieval of important audit data (e.g. financial records, emails, etc.)
Facilitate guaranteed non-repudiation of audit data
Audit policy configuration

Enterprise Architect
Summit 2006

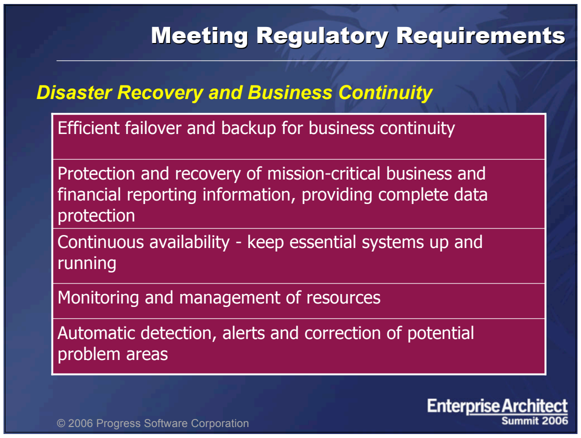


Meeting Regulatory Requirements

Integration

Facilitate and automate the integration of data and applications to eliminate errors introduced by manual processes
Achieve highly available, secure and reliable messaging to remote offices and business partners
Manage and track the secure exchange and sharing of data
Reduce the risk of lost or tampered data

Enterprise Architect
Summit 2006

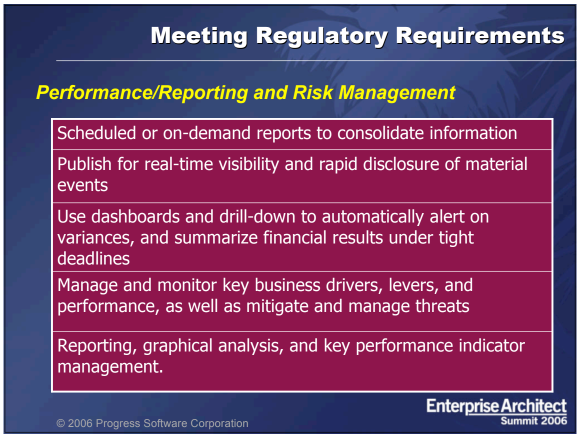


Meeting Regulatory Requirements

Disaster Recovery and Business Continuity

Efficient failover and backup for business continuity
Protection and recovery of mission-critical business and financial reporting information, providing complete data protection
Continuous availability - keep essential systems up and running
Monitoring and management of resources
Automatic detection, alerts and correction of potential problem areas

Enterprise Architect
Summit 2006

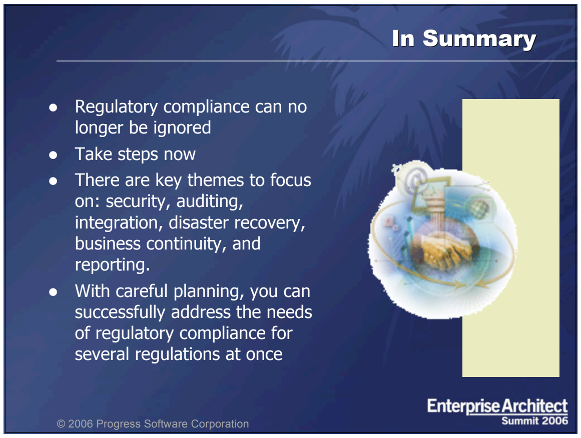


Meeting Regulatory Requirements

Performance/Reporting and Risk Management

Scheduled or on-demand reports to consolidate information
Publish for real-time visibility and rapid disclosure of material events
Use dashboards and drill-down to automatically alert on variances, and summarize financial results under tight deadlines
Manage and monitor key business drivers, levers, and performance, as well as mitigate and manage threats
Reporting, graphical analysis, and key performance indicator management.

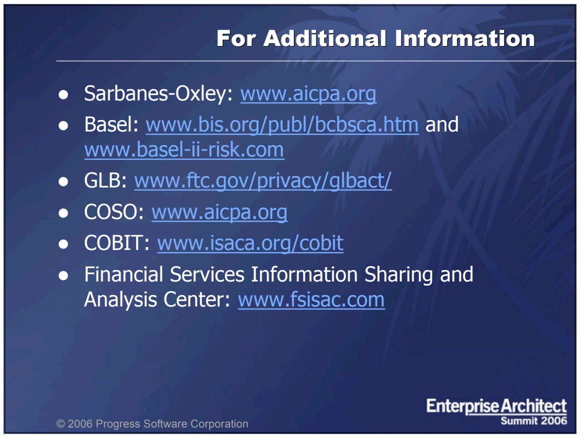
Enterprise Architect
Summit 2006



In Summary

- Regulatory compliance can no longer be ignored
- Take steps now
- There are key themes to focus on: security, auditing, integration, disaster recovery, business continuity, and reporting.
- With careful planning, you can successfully address the needs of regulatory compliance for several regulations at once

Enterprise Architect
Summit 2006



For Additional Information

- Sarbanes-Oxley: www.aicpa.org
- Basel: www.bis.org/publ/bcbsca.htm and www.basel-ii-risk.com
- GLB: www.ftc.gov/privacy/glbact/
- COSO: www.aicpa.org
- COBIT: www.isaca.org/cobit
- Financial Services Information Sharing and Analysis Center: www.fsisac.com

Enterprise Architect
Summit 2006

Thank you for your time!

Enterprise Architect
Summit 2006