An Executive Guide to Emerging IT Compliance Issues

Adrian Bowles, Ph.D.

Director of Research & Education
IT Compliance Institute
abowles@itcinstitute.com

IT Compliance Institute™

Agenda

- Background
  - Definition and scope of the problem
  - IT Impact by regulation-type
  - Survey of current regulations
- Best Practices
- Wrap-up

IT Compliance Institute™

Definition and Scope of the Problem

- Regulatory compliance costs IT $billions annually
  - The US passes over 4,000 new final rules annually
  - Sarbanes-Oxley (SOX) impacts all US public firms at a typical cost to IT of $.5-1M *annually*
  - Basel II will cost over $15B globally
  - A typical international bank may be governed by over 1000 regulations
  - Different jurisdictions have conflicting rules

ITCi
IT Compliance Institute™

Communications is the Biggest Problem

- IT activities are required for most major regulations, yet
- IT often hears about the requirements as an afterthought

Example

- Over 80% of CFOs thought SOX would have *little or no impact on IT budgets*
- 100% of CIOs said SOX would have *a significant impact on IT (budgets)*

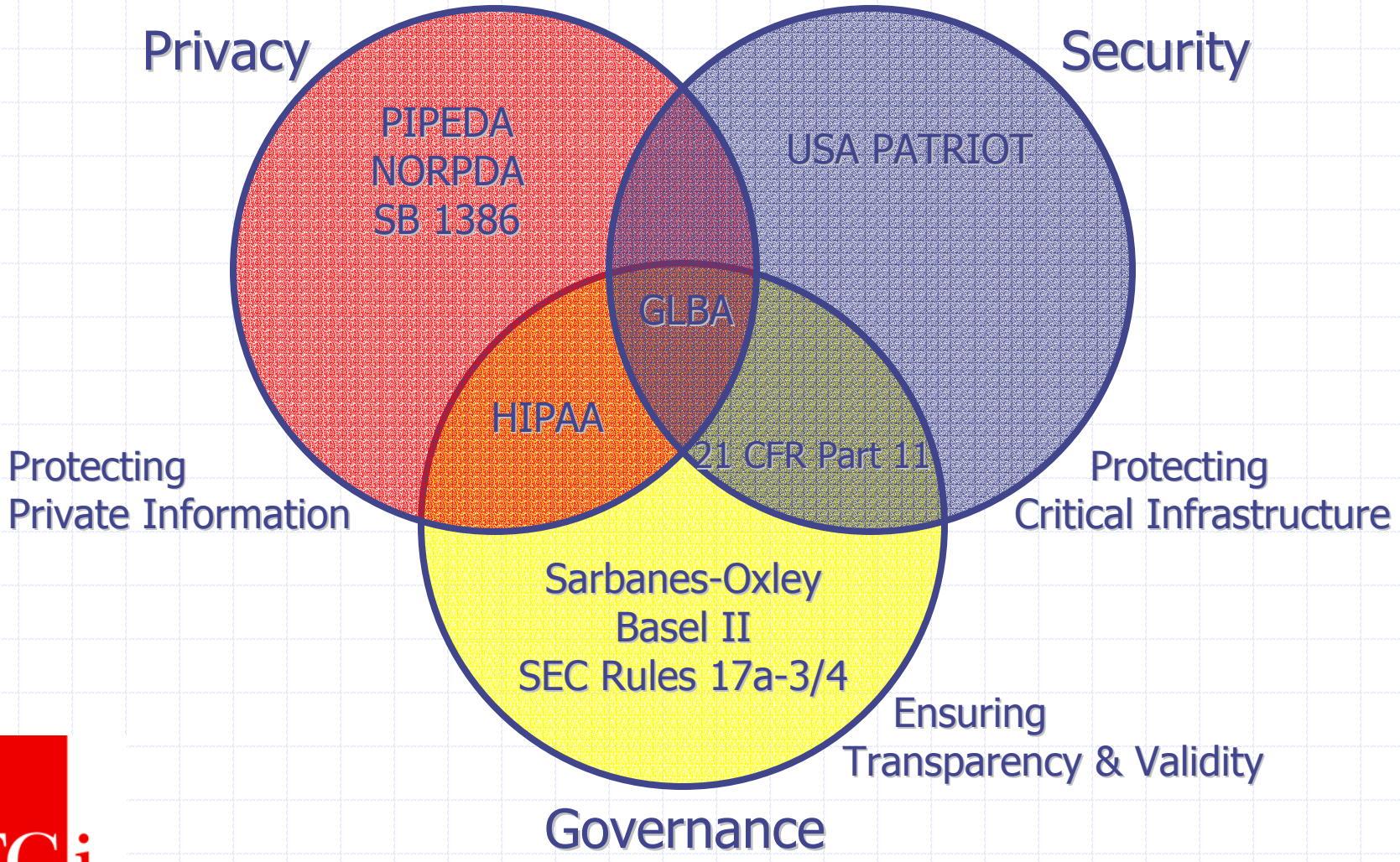
ITCi
IT Compliance Institute™

Major Categories of Regulations

- Governance
  - Transparency and validation of financial reporting
  - Records retention
  - Disaster recovery/business continuity
- Privacy
- Security
- Trade/Tariff
- Environmental

IT Compliance Institute™

Overlapping Intent & Requirements



IT Compliance Institute™

A Survey of Regulations

- Governance
  - Sarbanes-Oxley Act of 2002 (SOX) (US – Public (Listed) Companies)
  - UK Companies Bill (UK)
  - SEC Rules 17a-3 and 17a-4 (records retention for US – Financial Services)
  - Basel II – The New Capital Accord (International)
  - Gramm-Leach Bliley Act (US – Financial Services)
  - 21 CFR Part 11 (US – Health Care/Pharmaceuticals)
  - Health Insurance Portability and Accountability Act (HIPAA) US Health Care

- Security
  - 21 CFR Part 11 (US – Health Care/Pharmaceuticals)
  - USA Patriot Act *Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism* (US)
  - Electronic Signatures in Global and National Commerce Act (US)

ITCi
IT Compliance Institute™

A Survey of Privacy Regulations

- PIPEDA *Personal Info. Protection and Electronic Documents Act*
- UK Data Protection Act
- EU Data Protection Directive
- Personal Data Protection Act 25,326 – Argentina
- Hong Kong Personal Data (Privacy) Ordinance
- California Senate Bill 1386 (SB 1386)
- US Senate Bill 1350, *Notification of Risk to Personal Data Act*
- Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)

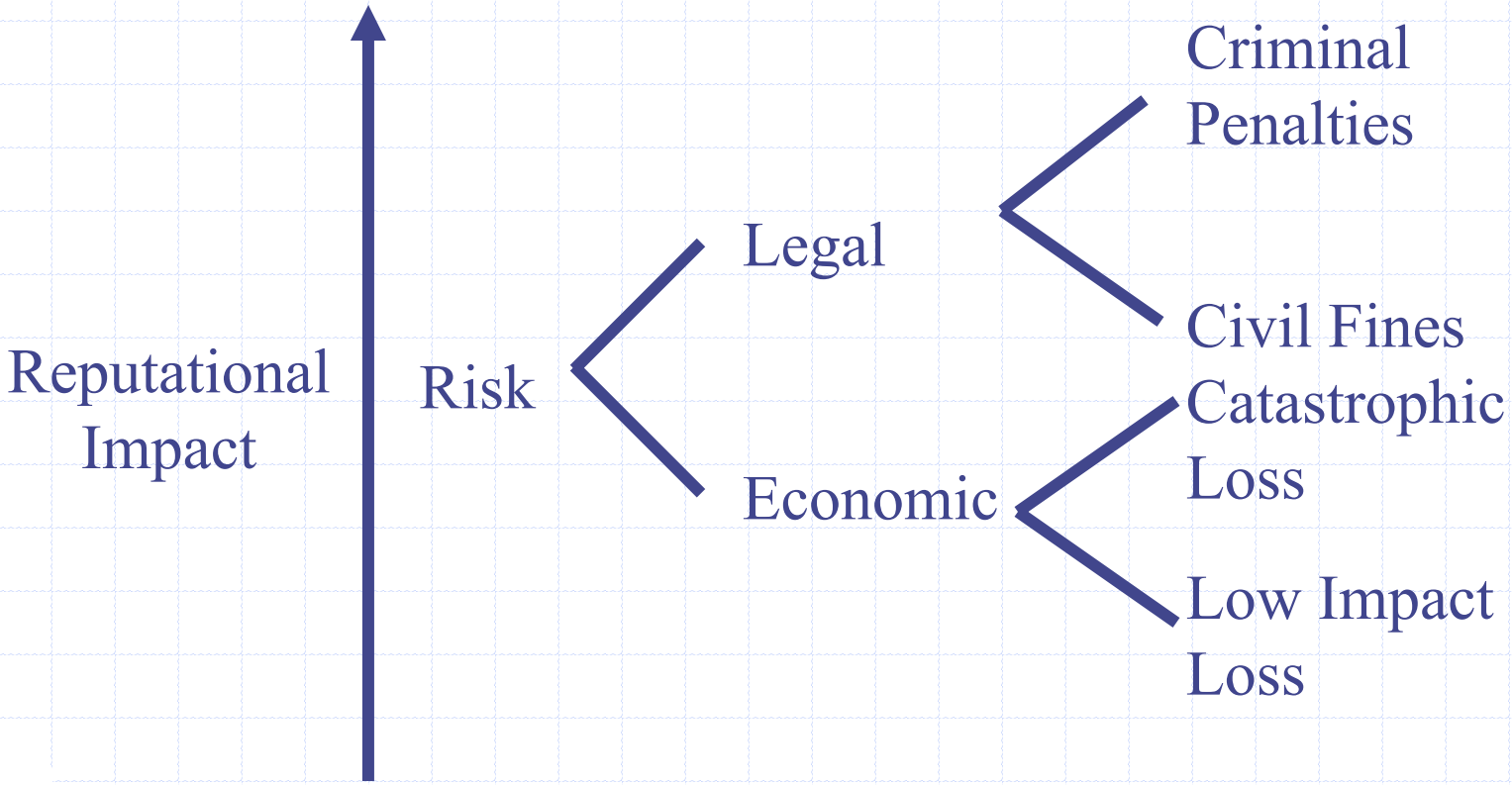
ITCi
IT Compliance Institute™

Agenda

- Background
- Best Practices
  - Risk management
  - Technology strategies
- Wrap-up

IT Compliance Institute™

Best Practices - Risk Management



IT Compliance Institute™

Internal Risks

A Survey of Risk Parameters for Compliance Teams				
Type of Risk	**Example**	**Regulatory Class**	**Mitigation Strategy**	**Skills Required**
Internal				
Operational	Improper or inaccurate accounting entries, errors of commission or omission when transferring data between systems	Governance	Formal monitoring and reporting processes	Auditing, process management
	Improper disposal of hazardous waste (including dumping computers)	Environmental	Outsourcing disposal	Legal - need to identify all potential
Security	Breach of perimeter or internal defenses which results in loss of control or data	Security, privacy business continuity, disaster recovery	Policies for critical data handling and backup, redundant processes and storage	Physical security, logical security, cryptography, archiving/recovery

IT Compliance Institute™

External Risks

A Survey of Risk Parameters for Compliance Teams				
Type of Risk	**Example**	**Regulatory Class**	**Mitigation Strategy**	**Skills Required**
External				
Market / Event	Vendor or platform failure (adopters of Next computers in financial services)	Governance	Hedge, code escrow, open source, open standards	Technical - always have an alternative strategy for critical vendor - supplied solutions
	Global or market-wide events, volatility, loss of market confidence	Governance	Frequent reviews of strategic assumptions, rule-based monitoring of business intelligence systems with alerts to give early warning, environmental / situational awareness, hedging strategies, increased reserves	Strategic view, backed up by a deep understanding of economics and chaos theory
	Competitive threats	Governance	Short-cycle strategy reviews	Corporate strategy based on a flexible model that responds to new challenges, otherwise competitors will create "material changes in conditions" that must be disclosed

Best Practices – Technology Strategies

- Factoring regulatory requirements to benefit from a common
  - data model/user view
  - access/retention model
  - risk management approach
- Compliance architectures
  - Integrated solutions

IT Compliance Institute™

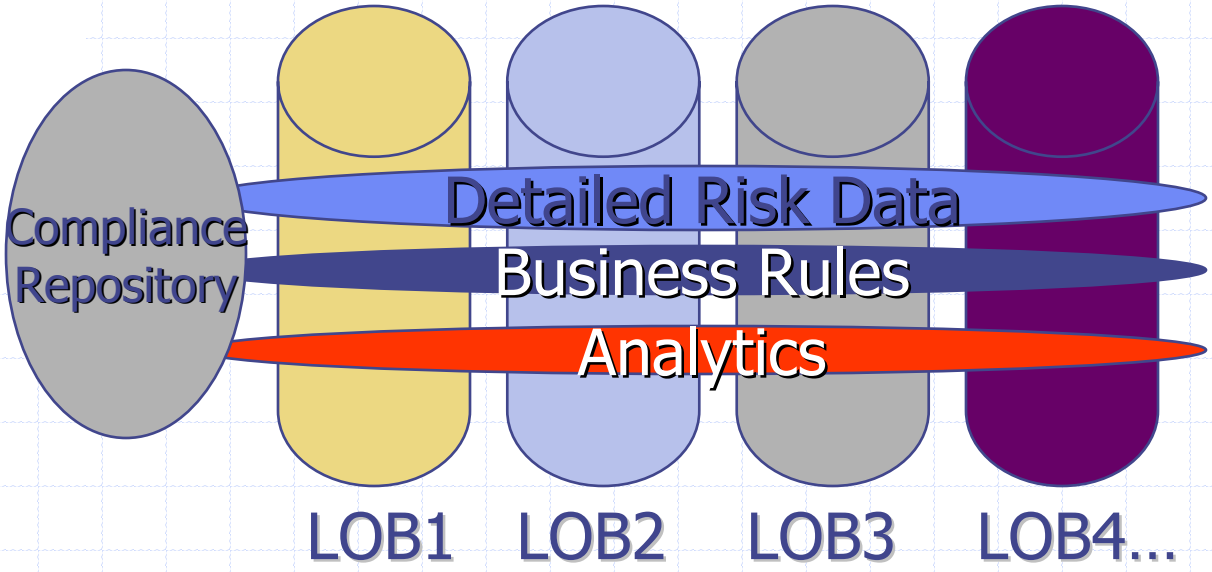
IT Impact by Regulation Type

IT Impact		Type of Regulation				
		Privacy	Security	Governance	Environmental	Trade/Tariff
Storage and access control	Email/IM	★	★	★	★	★
	Customer data (CRM)	★	★	★		★
	Partner Data			★		★
	Planning Data/ERP			★		
	Financial Data			★		
	Operational Data (ERP)		★	★	★	
	Analytics/BI	★		★		
Process management	Workflow		★	★	★	

ITCi
IT Compliance Institute™

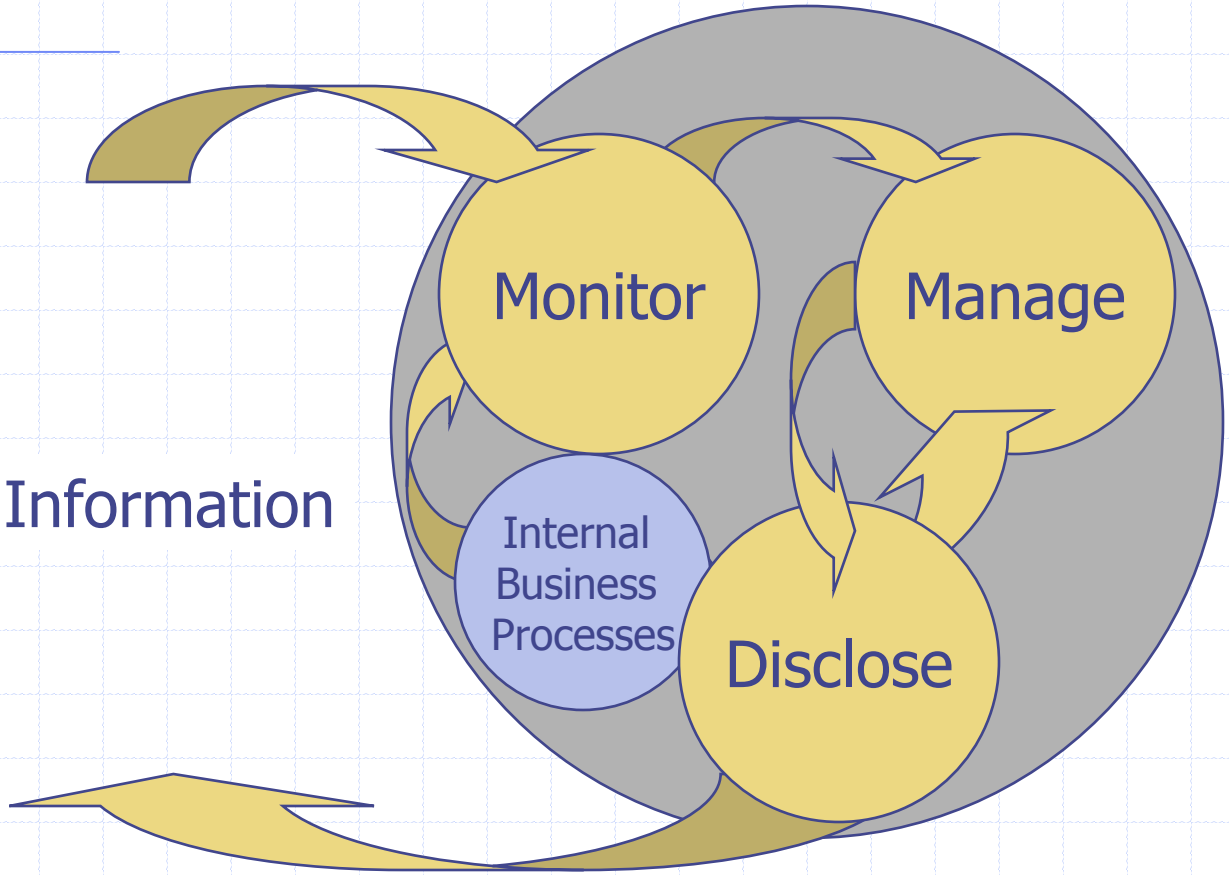
Benefits of a Common View

- Aggregation: Who has the big picture vs. who needs it?
- Issues
  - Data quality
    - Consistent
    - Current
    - Complete



IT Compliance Institute™

Governance Information Flow

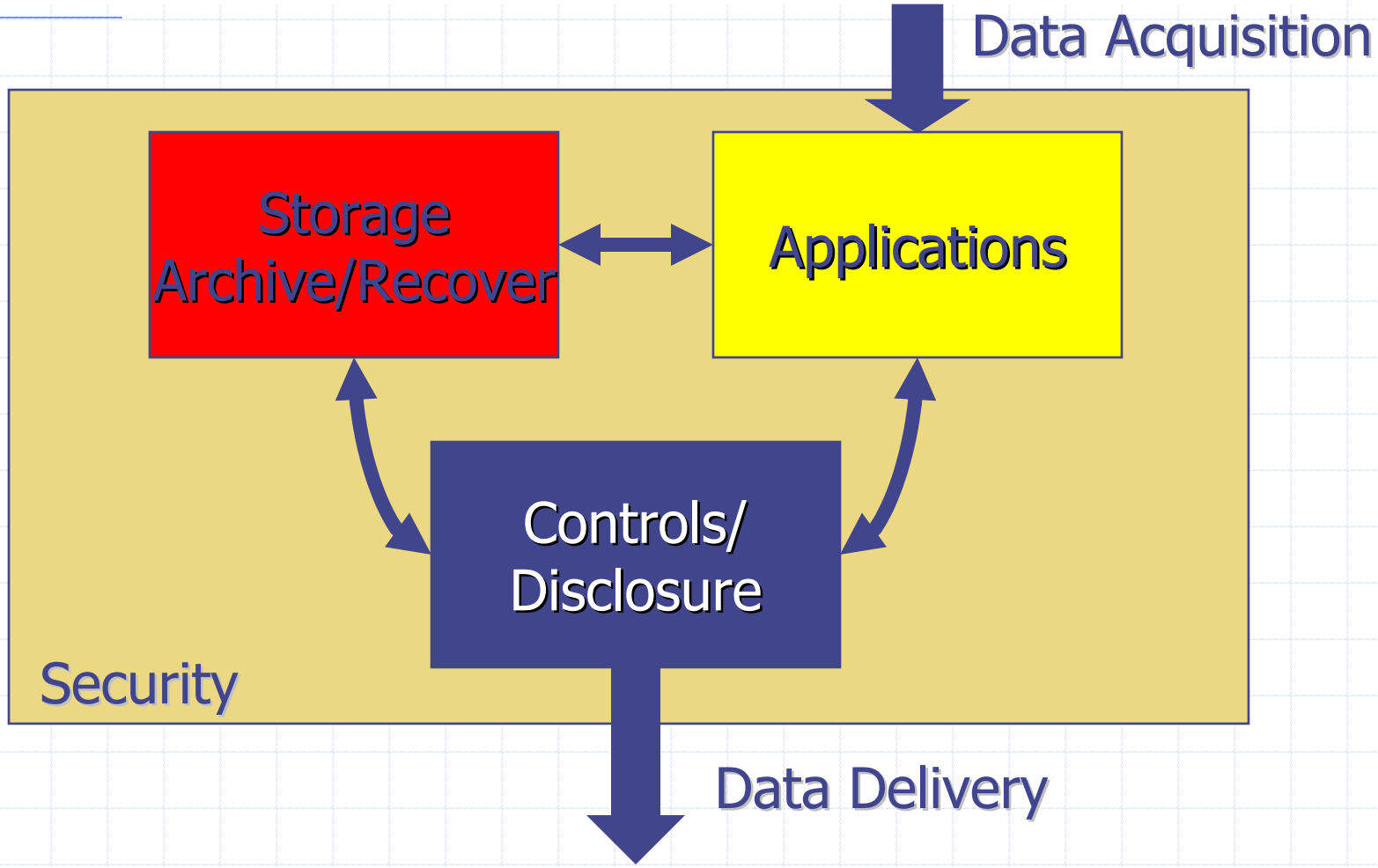


Public Information

Sarbanes-Oxley is…a LOT like Basel II…

IT Compliance Institute™

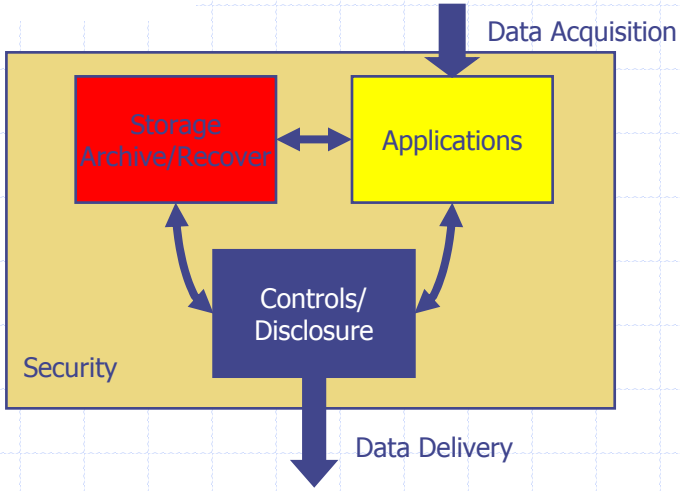
An Architecture for Compliance



IT Compliance Institute™

Benefits of a Commercial Compliance Architecture

- Lower Cost & Risk
- Higher Quality, More Flexible
- Better Defensive Position



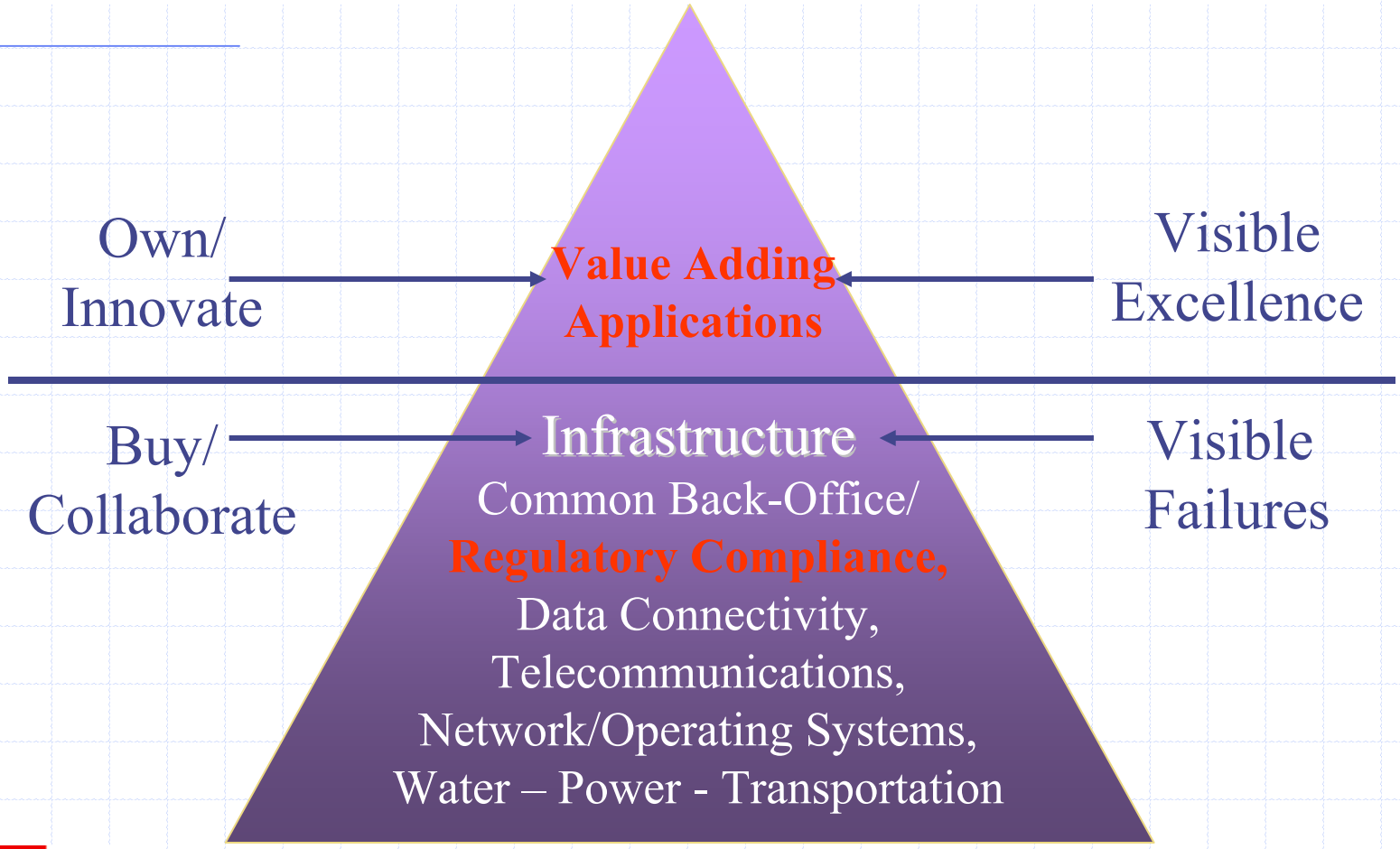
ITCi
IT Compliance Institute™

Building a Defensible Compliance Strategy

Strategy	Lines of Defense
Build it yourself	"I made a mistake."
Buy packages	"No one else did it better."
Collaborate – with vendors and competitors	"Nobody could do it better."

IT Compliance Institute™

User Strategy: Focus Where Customers Notice



ITCi
IT Compliance Institute™

Agenda

- Background
- Best Practices
- Wrap-up
  - Business Benefits
  - What to expect for the rest of this decade
  - Recommendations

IT Compliance Institute™

IT Compliance Business Benefits

Regulation Type/Systems Impact	Business Benefits

- Governance
  - Consolidation/Upgrades
  - Integrated records retention
- Privacy/Security
  - Consolidated customer information

- Better planning
- Know your customer better
- Faster time to market
- Better communications
- Reduced maintenance costs
- Reduced risk

ITCi
IT Compliance Institute™

What to expect for the rest of the decade

Regulations

- Incremental changes in every category (gov/priv/sec…)
- New vertical market regulations
- New geo-specific regulations, will gradually converge

Technology

- Focus on integrated solutions (hardware, software, services)
- Improved & integrated dashboard and scorecard products
- Focus on storage - retention/recovery

ITCi
IT Compliance Institute™

Recommendations

- Prioritize tasks by risk & business benefit
- Consolidate compliance planning/monitoring
- Use an integrated compliance architecture

Questions

Adrian Bowles

Director of Research & Education

IT Compliance Institute

abowles@itcinstitute.com

www.itcinstitute.com

IT Compliance Institute™

Glossary of Acronyms

- BI – Business Intelligence
- CFO – Chief Financial Officer
- CFR – Code of Federal Regulations (US)
- CIO – Chief Information Officer
- CRM – Customer Relationship Management
- ERP – Enterprise Resource Planning
- GLBA – Gramm Leach Bliley Act
- HIPAA – Health Insurance Portability and Accountability Act
- IM – Instant Messaging
- PIPEDA – Personal Information Protection and Electronic Documents Act (Canada)
- SEC – Securities Exchange Commission (US)
- SOX – Sarbanes Oxley Act

ITCi
IT Compliance Institute™