

Coping with Compliance

An Overview of the Regulatory Landscape and its Impact on
Technology Implementations

Adrian J. Bowles, Ph.D.

**Object Management Group
Program Director, Regulatory Compliance
adrian@omg.org**

**Experture
Principal**



Agenda

- **Background**
 - Definition and scope of the problem
 - IT Impact by regulation-type
 - Survey of current regulations
- **Best Practices**
 - Risk management
 - Technology strategies
 - Building a defensible compliance strategy
- **Wrap-up**
 - Business benefits
 - What to expect for the rest of this decade
 - Recommendations

Definition and Scope of the Problem

IT Regulation - Any government rule that requires – directly or by implication – the creation of or modification to a system that is generally managed by IT.

Regulatory compliance costs IT departments \$billions annually

The US passes over 4,000 new final rules annually – dozens have significant IT impact.

Sarbanes-Oxley (SOX) impacts all US public firms (over 15,000) at a typical cost to IT of \$.5-1M annually

Basel II will cost over \$15B globally

Different jurisdictions have conflicting rules

e.g. privacy – US and Europe, different assumptions



IT Has a Dual Role in Compliance

● Internal

- **Some IT data and processes are subject to direct regulatory control**
 - **Application development (particularly in industries such as financial services and pharmaceuticals)**

● External

- **IT may acquire/develop/operate systems that are governed by regulators for other departments**
 - **Finance**
 - **Planning**
 - **Customer relationship management**

Communications is the Biggest Problem

- IT activities – monitoring, managing, protecting, and disclosing – are requirements for most major regulations
- IT is often informed – by legal or finance departments - as an afterthought, which complicates and delays compliance

Example

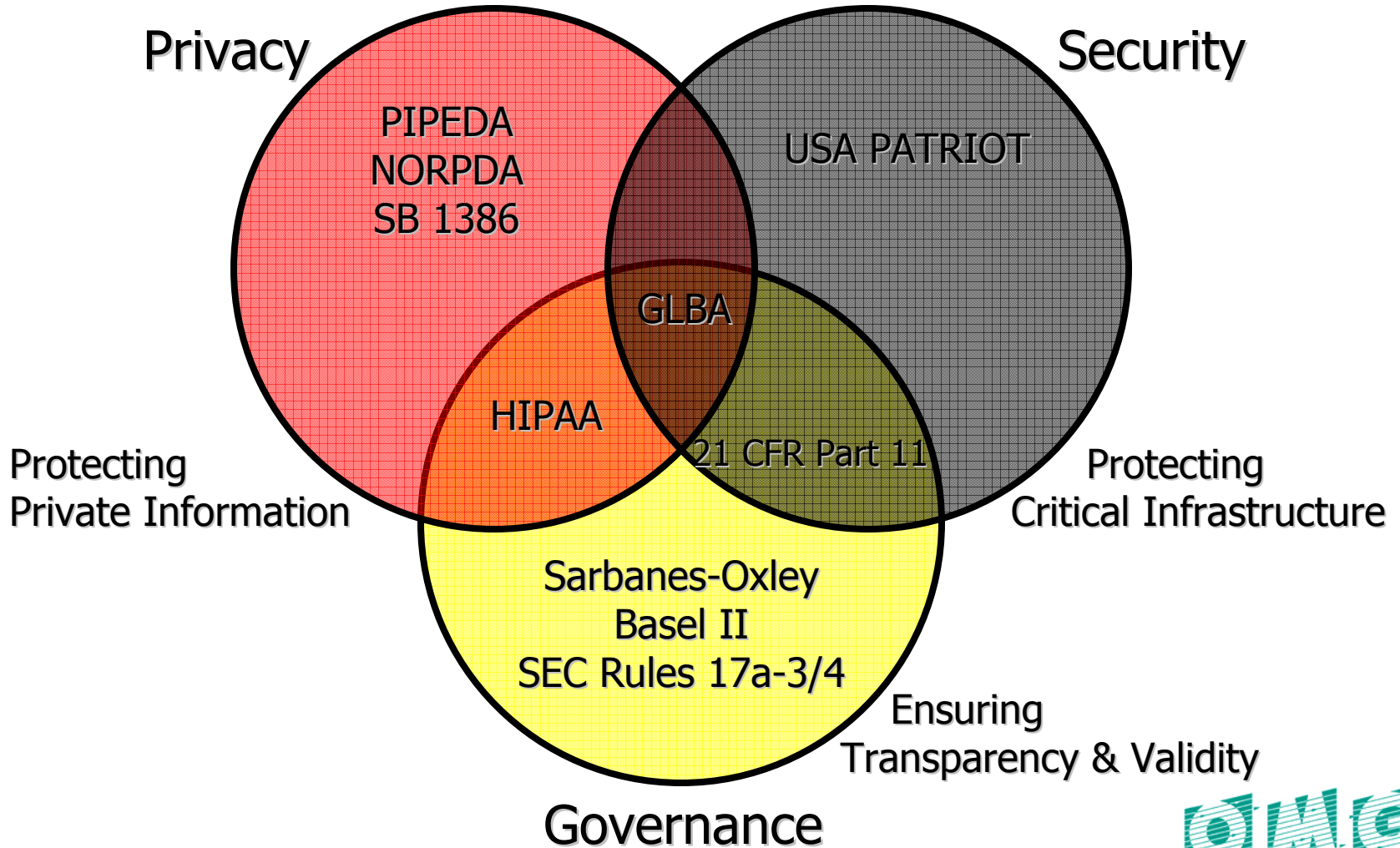
- Over 80% of CFOs responded to a survey that SOX would have little or no impact on IT budgets
- 100% of CIOs responded that SOX would have a significant impact on IT (budgets)

IT needs a seat at the table - a good compliance strategy requires cross-functional representation

Major Categories of IT Regulations

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

Overlapping Intent & Requirements



Resolving International Differences

- EC Directive on Data Protection October, 1998
 - prohibits the transfer of personal data to non-EU nations that do not meet the European “adequacy” standard for privacy protection.
- EU requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin.
- US relies on a mix of legislation, regulation, and self regulation.

As a result, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor — approved by the EU in July of 2000 — is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU **or facing prosecution by European authorities** under European privacy laws.

Source: <http://www.export.gov/safeharbor/>

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		★	★	★	

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)

● 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)



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* (NORPDA)**
- **Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)**

Sarbanes-Oxley: The 800 # Compliance Gorilla

- **Increasing responsibilities and liabilities for:**
 - **CEOs, CFOs, Ind. Auditors, Boards/Committees**
- **Internal Controls**
 - **Adequacy**
 - **Changes**
- **Auditors and management**
 - **Must report & attest to accuracy of financial statements and disclosures**
- **Applies to US public companies, private companies with public debt, and accounting firms**
- **Driven by the Enron, Tyco, and WorldCom fiascos**

Why is SOX a Big Deal for IT?

- **Huge communications disconnect with finance**
- **Insufficient documentation & evaluation of internal controls**
 - **Auditors must evaluate internal controls before attesting to financial statements**
- **1 in 10 companies have made financial restatements in the past five years (U.S. GAO study)**

Which Provisions Apply to IT?

- **302 – corporate responsibility for financial reporting**
 - **Is our financial data accurate?**
 - **Do we have transaction level detail if required?**
 - **Do we understand all the processes involved?**
 - **Can we close the books on time, do we trust the results?**
- **404 – annual management assessment of internal controls**
 - **How does our control structure operate?**
 - **Who is accountable?**
 - **Is it monitored?**
 - **Is it documented?**
- **409 – real-time disclosure of material changes**
- **802 – retention of relevant records for audits/reviews**

404 Management Assessment of Internal Controls

- **Must provide an annual certification of adequate internal controls, and outside auditor must attest to and report on management's financial controls**
- **Internal controls must be documented, tested, and monitored**
- **Requires**
 - **Effective document and process management**
 - **Data consistency and integrity, no “off ledger” transactions**

409 – Real Time Issuer Disclosures

...”Each issuer reporting...shall disclose to the public *on a rapid and current basis* such additional information *concerning material changes in the financial conditions or operations of the issuer*, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is *necessary or useful* for the protection of investors and in the public interest.”

Emphasis added

Best Practices – Technology Strategies

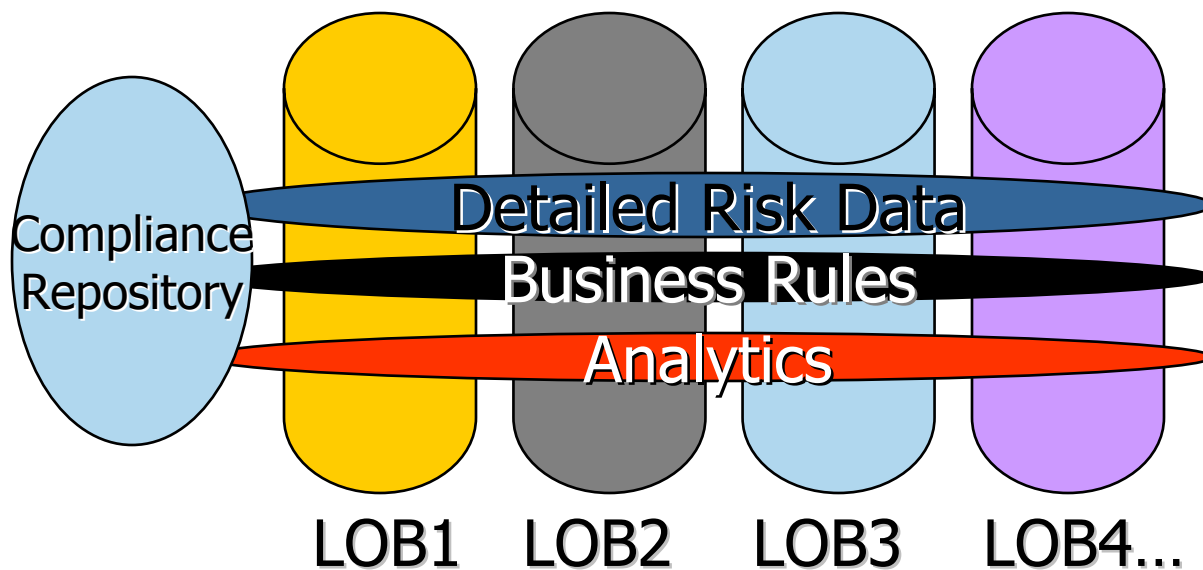
- **Build on/complement DR/Bus Continuity Strategies**
- **Factoring Regulatory Requirements**
 - **Privacy**
 - **Security**
 - **Governance (process monitoring)**
- to benefit from a common
 - **data model/user view**
 - **access/retention model**
 - **risk management approach**
- **Compliance Architectures**
 - **Integrated solutions**

Benefits of a Common View

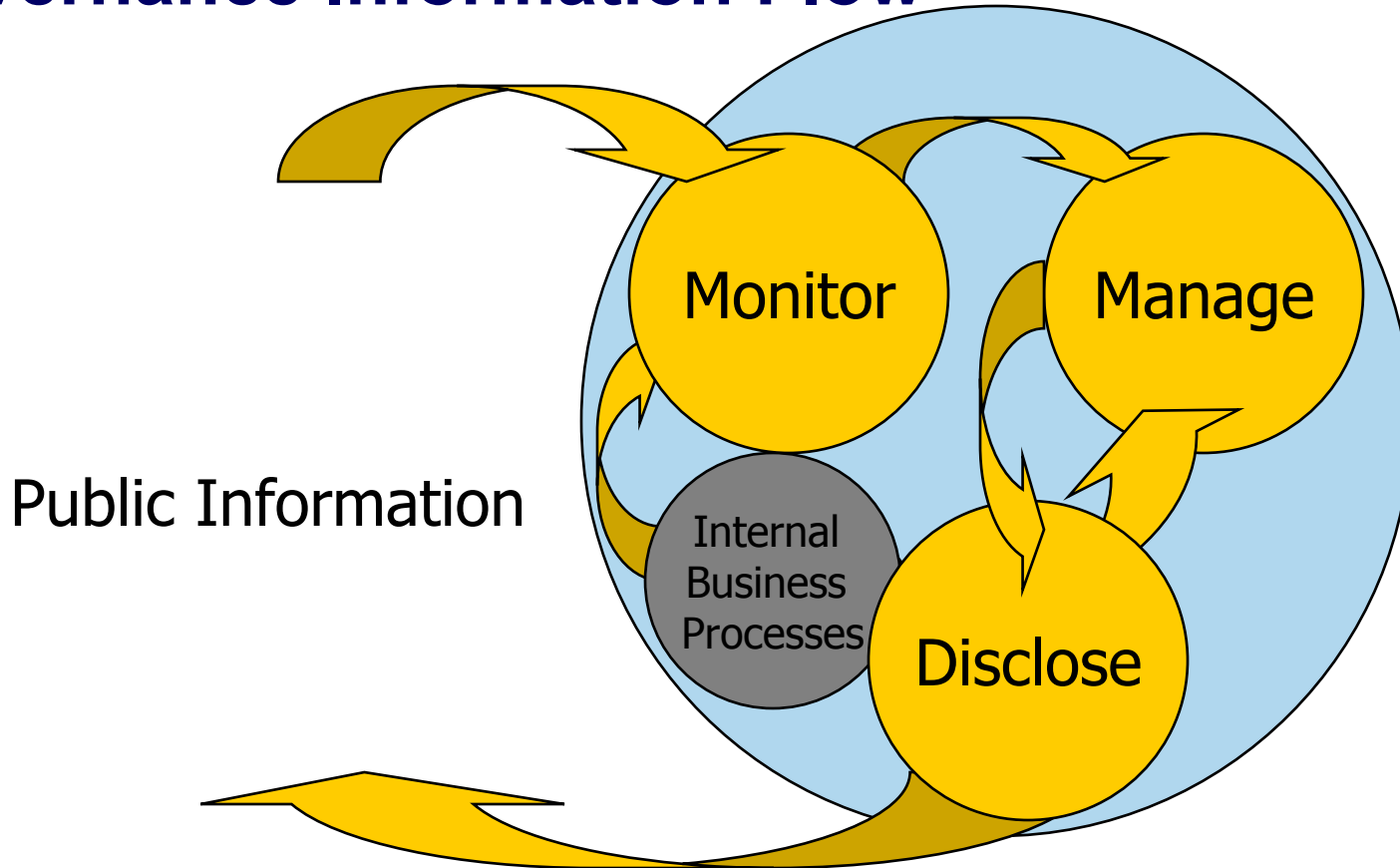
Aggregation: Who has the big picture vs. who needs it?

Issues

- Data quality
- ◆ Consistent
- ◆ Current
- ◆ Complete



Governance Information Flow



Sarbanes-Oxley is...a LOT like Basel II...

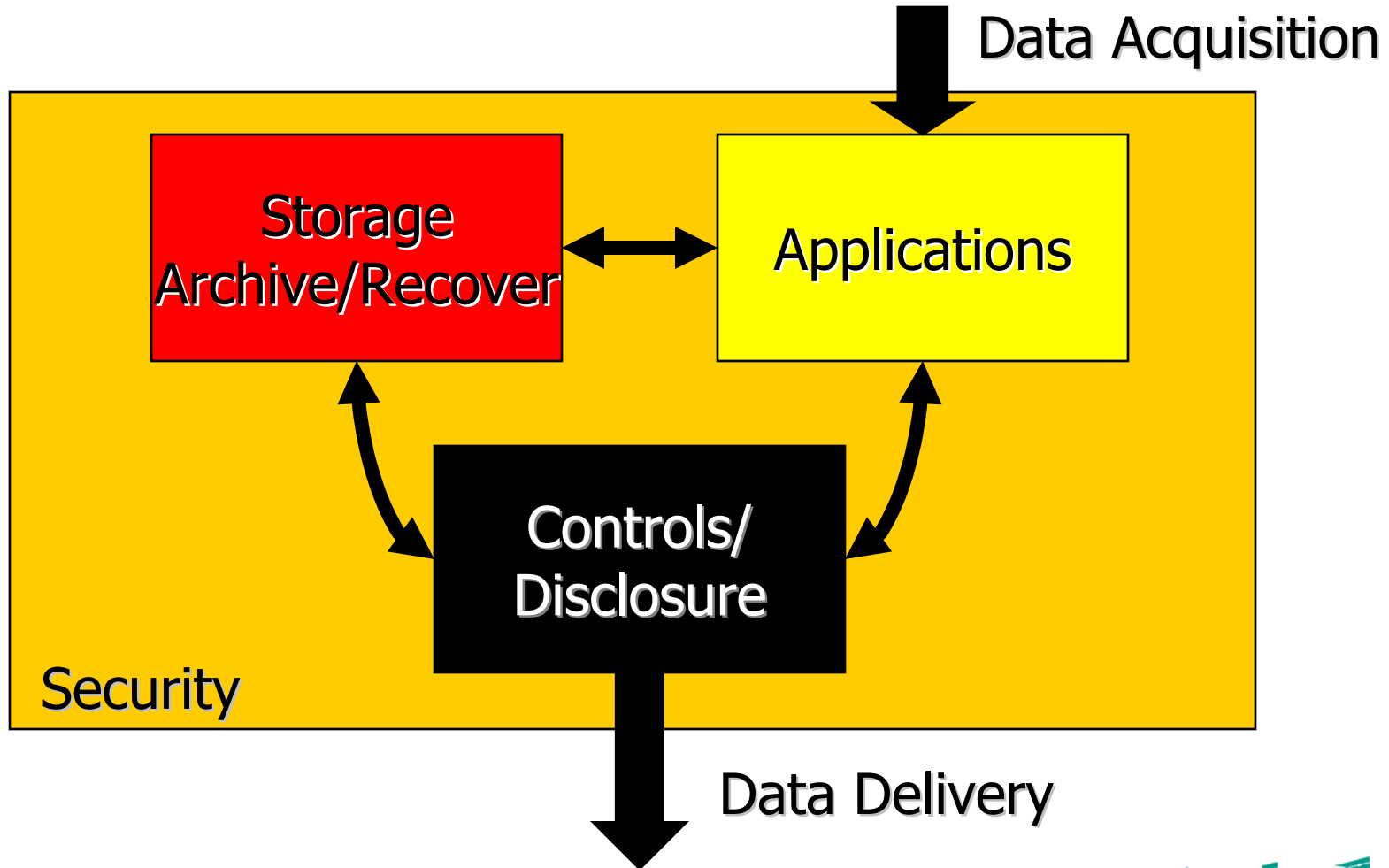
Best Practices - Off the Shelf

- **Use Commercial Compliance Architecture Whenever Possible**
- **Use Highest Level Granularity Integrated Components/Solutions**

Using Integrated Solutions

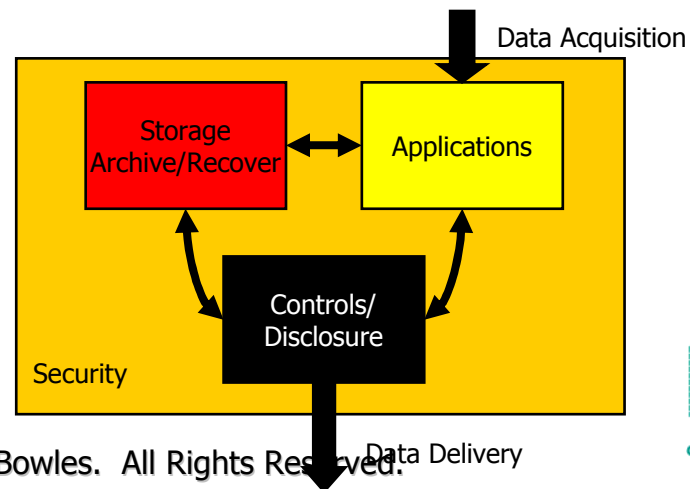
- **Simplify**
- **Remove redundancies**
- **One truth is better than two**

An Architecture for Compliance



Benefits of a Commercial Compliance Architecture

- **Lower Cost & Risk**
 - Development costs borne by vendor once, used many times
 - Input from vendor clients increases confidence that all needs are met
- **Higher Quality, More Flexible**
 - Sharing the non-differentiating infrastructure allows inputs from competitors
- **Better Defensive Position**
 - Working with an industry leader or collaborating with competitors provides a stronger basis for acceptance by outside auditors and regulators



Building a Defensible Compliance Strategy

Three Lines of Defense

- "I made a mistake."
- "No one else did it better."
- "Nobody could do it better."

“I Made A Mistake”

(so, sue me)

Build your own solutions.

Benefits	Risks
Full control over the process, possibly the fastest and cheapest route for some regulations, if the appropriate infrastructure is in place.	In the event that a firm is found to be out of compliance, this is the worst possible scenario, and maximum penalties may apply. It also has the greatest potential for reputational risk, in addition to punitive risks.

“I Bought A Mistake”

(so, sue me and I'll sue the vendor)

Benefits	Risks
<p>When a packaged solution exists, maintenance of the process should be less expensive. <i>If the solution achieves significant market share, the defensive position of the firm is enhanced in the event of non-compliance.</i></p> <p>Keeping up to date with regulations is a very challenging task. <i>If this application were to be built in house, the organization would have to devote a minimum of one full-time employee to this. Regulations may change frequently</i></p> <p>Vendors may also provide some best practices for maintaining compliance. <i>And, their solutions may offer improvements (automation) over current processes.</i></p>	<p>This option entrusts, <i>but cannot delegate</i>, some aspects of compliance to a third party. Typical vendor due diligence concerns are magnified based on potential exposure, including reputational risk.</p>

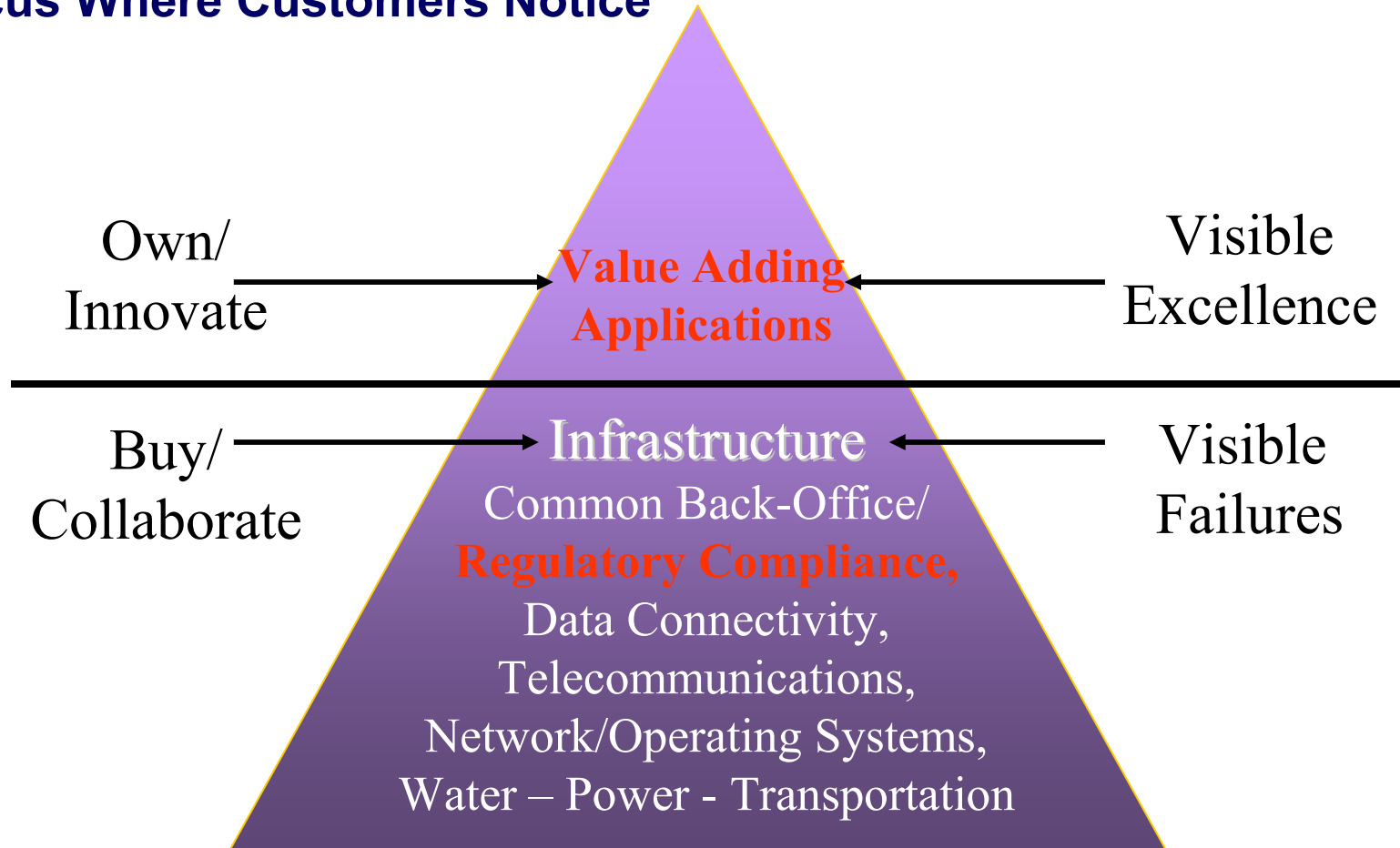
“Nobody could do it better.”

(so sue us all and shut down our industry)

Benefits	Risks
Peers are in the best position to develop common best practices. In the event of non-compliance, a penalty to one participant results in a penalty to all.	Minimized if sharing partners have similar reputations in one's market.

Collaborate & Share: If a group of leading firms collaborates to develop best practices for compliance and fails, it may serve as an informal proof of difficulty or regulatory ambiguity. It would be much more difficult to extract the maximum penalty from each of them than if any one individually came up with the same solution and failed alone.

Focus Where Customers Notice



IT Compliance Business Benefits

Regulation Type/Systems	Impact	Business Benefits
<ul style="list-style-type: none"> ● Governance <ul style="list-style-type: none"> ● Consolidation/Upgrades <ul style="list-style-type: none"> ▪ Business Intelligence/Analytics ▪ Financial management (general ledger, ERP) Content management ▪ Workflow ● Integrated records retention ● Privacy/Security <ul style="list-style-type: none"> ● Consolidated customer information 	<ul style="list-style-type: none"> ● Better planning <ul style="list-style-type: none"> ● More accurate & timely information ● Better access to historical information ● Know your customer better <ul style="list-style-type: none"> ● Identify new patterns and business opportunities ● Identify cross-selling opportunities ● Improve customer confidence ● Faster time to market ● Better communications <ul style="list-style-type: none"> ● With business partners (suppliers and customers) ● Between lines of business ● Reduced maintenance costs ● Reduced risk 	

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
 - Self-documenting, secure applications (access-aware)

Summary of Recommendations

- **Factor requirements to leverage commonalities,**
 - Eliminate redundancies in data, processes, and systems
- **Automate Auditing efforts**
 - Data
 - Procedures & Testing
- **Collaborate/partner/acquire whenever feasible**
 - Participate in the discovery and dissemination of emerging best practices and standards
 - Highest level components/systems
 - Leverage standards: *de jure* when available, *de facto* as interim

Questions?

Adrian J. Bowles, Ph.D.

**Object Management Group
Program Director,
Regulatory Compliance
adrian@omg.org**

**Experture
Principal**

