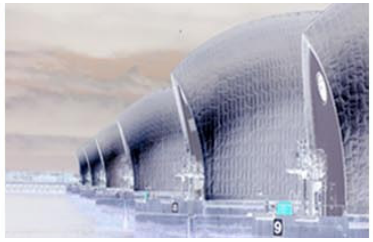
LOGICALIS
integration solutions

Technically Speaking!

What is Compliance?

Mark Wilson


Agenda

- Introductions
- Objectives
- IT “Feeling The Pressure” of Compliance
- Dictionary Term of Compliance
- What does it mean to us?
  - Software Compliance
  - Regulatory Compliance
- Software Compliance
- Regulatory Compliance
- Summary
- Questions

Introductions

- I am a mainframe technician with some knowledge of Security & Compliance
- I have been doing this for almost 30 years
- This session will look at the aspects of compliance from a zSeries technicians perspective, however, we do have to understand what compliance is and how it affects us all
- I don’t have all of the answers; but hopefully I will give you something to think about
- Happy to take questions as we go

Objectives

Give a high level overview of what compliance can mean

- Pointers to further reference material
- Look at some of the organisations driving much of the legislation
- Look at some of the tools available to help
- Give you something to think about!

IT "Feeling the pressure" of Compliance

A recent Computer Weekly article, discussed a recent survey of a 1,000 companies and found:

- Most IT departments are affected by compliance issues
- 43% of IT staff felt they were being put under unreasonable pressure by the business to support compliance for compliance sake
- More than 50% of the firms surveyed have had to invest in storage and data management systems to solve compliance issues
- The main complaints were the administrative overheads and resources required for compliance

The Dictionary term is?

- **Word:**
  - Compliance
- **Function:**
  - noun
- **Date:**
  - Circa 1630
- **Meaning:**
  - The act or process of complying to a desire, demand, proposal, or regimen or to coercion
  - Conformity in fulfilling official requirements
  - A disposition to yield to others
  - The ability of an object to yield elastically when a force is applied, flexibility

What does it mean for us?

Software Compliance

- Licenses
  - Do we have enough?
    - User/Seat based
    - Capacity based
  - Do we have any licenses at all?
  - Do we use any Shareware/Freeware?
    - What are the implications
  - Do we develop our own software?
    - What about open source
    - GNU public license
    - See: http://en.wikipedia.org/wiki/Gnu_public_license for further details

What does it mean for us?

Regulatory Compliance

- What rules apply?
  - Financial Services and Markets Act 2000
    - http://en.wikipedia.org/wiki/Financial_Services_and_Markets_Act_2000
  - Sarbanes-Oxley (SOX)
    - http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
  - Payment Card Industry Security Standards
    - http://en.wikipedia.org/wiki/PCIDSS

What does it mean for us?

Regulatory Compliance

- What rules apply?
  - Basel Accord or Basel II
    - http://en.wikipedia.org/wiki/Basel_II
  - Gramm-Leach-Billey (GLB)
    - http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act
  - Health Insurance Portability and Accountability (HIPAA)
    - http://en.wikipedia.org/wiki/HIPPA
  - UK Companies (Audit, Investigations and Community Enterprise) Act 2004

Software Compliance

LOGICALIS
integration solutions

Software Compliance

- Why?
- How?
- Benefits
- Tools

Software Compliance

Why?

- It makes sense
  - We need to understand:
    - What we have
    - How we use it
    - Who uses it
- Can have serious financial implications, both good and bad
- Software vendors need/want us to pay for what we use
- Software vendors find it easier to sell more of the same than a new product
  - Ask a salesperson
  - Often called low hanging fruit

Software Compliance

How?

- Create the inventory
  - Automatically if possible
  - The spreadsheet still works
- Track the usage
  - Will needs tools for this
  - Report on a Monthly or Bi-Monthly basis
- Review the license agreements
  - Understand the limitations
  - Understand the impact of changes
    - Hardware Consolidation
    - Operating system upgrades
- Some organisations have a dedicated software asset management team(s), that cover the whole enterprise

Software Compliance

Benefits

- Pay for what you use
  - Why pay for software that just sits on the shelf
  - Why pay £1,000's for a piece of software used by one person
    - Unless of course it's business critical
  - Helps defeat the myth that the mainframe is expensive
    - We all know that the mainframe delivers the best TCO of all available servers
- Your Auditors are starting to look at this and also how efficient the IT department is!
  - Terms often used are:
    - Best Practices
    - Efficiency
    - Inventory management

Software Compliance

IBM Tools

- Tivoli License Compliance Manager
  - IBM Tivoli License Compliance Manager (TLCM) identifies software inventory, measures use activity, and automatically links complex license entitlements to help manage software costs and license compliance in the distributed environment. This software asset management solution enables IT to align software spending with business priorities.
    - http://www-306.ibm.com/software/tivoli/products/license-mgr/
- Tivoli Contract Compliance Manager
  - IBM Tivoli Contract Compliance Manager is an IT Contract Management product that helps users to achieve the efficient management of the contractual and financial details of IT agreements. Tivoli Contract Compliance Manager can help users manage software costs and contract compliance. This software asset management solution helps IT to align software spending with business priorities. The information provided can help organizations reduce software costs and compliance risk, and to allocate additional resources to priority projects.
    - http://www-306.ibm.com/software/tivoli/products/contract-compliance-mgr/

Software Compliance

3rd Party Tools

- CA Unicenter Asset Management
  - Managing the Usage and Ownership of IT Assets.
  - Unicenter® Asset Management delivers comprehensive knowledge of IT assets across your enterprise and allows you to monitor software usage on desktops, servers and other client devices. With full-featured asset tracking capabilities, it automates critical IT management processes, including discovery of network assets, inventory, maintenance activities, license administration and cross-platform reporting.
    - http://www3.ca.com/solutions/SubSolution.aspx?ID=4570
- CA Unicenter Asset Portfolio Management
  - Managing Contracts and Ownership
    - http://www3.ca.com/solutions/Product.aspx?ID=4343
- BMC® Remedy® Asset Management
  - Helps you lower IT costs, manage compliance, and improve your return on capital with an operational approach to life cycle, inventory, contract, and cost controls of IT assets.
    - http://www.bmc.com/products/proddocview/0,2832,19052_19429_22743814_121270,00.html
- Compuware Changepoint
  - Provides an integrated view of IT that allows you to effectively manage your projects, applications, people and client relationships.
    - http://www.compuware.com/solutions/it-portfolio-management.htm

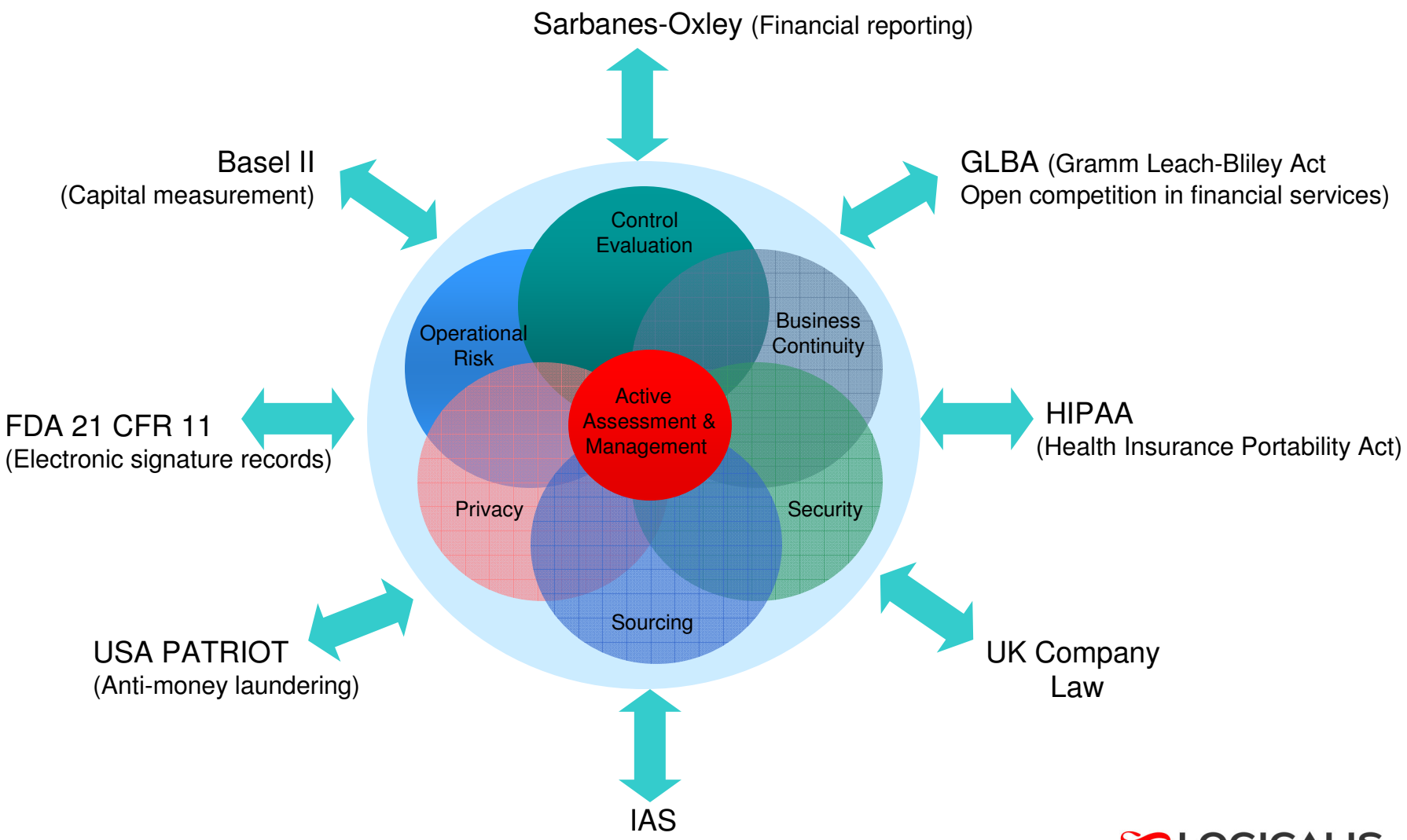
Regulatory Compliance

LOGICALIS
integration solutions

Regulatory Compliance

- Regulatory Compliance
- What are the rules?
  - What is SOX?
  - What is the FSA?
  - What is PCIDSS?
- What do I need to do?
- How do I do it?
- Tools

Regulatory Compliance



LOGICALIS
integration solutions

Regulatory Compliance

Governance Risk Compliance (GRC)

- Mandate the use of industry standard internal control frameworks - **Governance**
- Assess effectiveness of an organisation's controls
- Regular independent assessments and audit reports to regulators
- Improve corporate accountability
- Reduce operational and business **Risk**
- Demonstrate **Compliance** with controls
- You will see **GRC** in lots of IBM and Industry presentations and Papers

Regulatory Compliance

Architecture

Business Continuity

- Business Continuity
- Backup/ Archives
- Information Lifecycle
- Disaster Recovery
- Data Protection
- Data Retention
- Service Continuity
- Availability Management
- Network Management
- Scalability

Security

- Privacy
- Infrastructure Security
- Identity Management
- User Access Controls
- Data Security
- Digital/Video Surveillance
- Intrusion Detection
- Vulnerability
- Risk Management

Service Management

- Incident & Problem Mgt
- Service Level Management
- Change Management
- Configuration Management
- Release Management
- Availability Management
- Capacity Management
- Financial Management
- Security Management
- Asset Management

Regulatory Compliance

What are the rules?

- Typical consultative answer – It depends!
- "What's the old saying about the consultant, your watch and the time?"
- It depends on your industry
- The majority of zSeries sites are governed by SOX and the FSA
  - Hopefully that's most of the audience!
- Some sites will be effected by PCIDSS
- You need to understand what rules are in place
- You also need to know who is responsible within your organisation

Regulatory Compliance

What is SOX?

- American Law drafted by Senator Paul Sarbanes and Congressman Michael Oxley designed to enforce corporate accountability and responsibility
- The Act has granted the SEC increased regulatory control, lengthened the statute of limitations and imposed greater criminal and compensatory punishment on executives and companies that do not comply
- The process of implementing a Sarbanes-Oxley compliance program can be translated into a list of requirements that may result in a change to your current governance structure, procedures, and/or processes
- For simplicity, I have summarised the impacts under the following four headings and have included a list of key components of the Act in the notes pages of the presentation
  - *Corporate accountability and responsibility*
  - *Internal procedures and controls*
  - *Audit and accounting*
  - *Enhanced disclosure and reporting requirements*

Regulatory Compliance

What is the FSA?

- The Financial Services Authority (FSA) is an independent non-governmental body, given statutory powers by the Financial Services and Markets Act 2000. They are a company limited by guarantee and financed by the financial services industry, the Treasury appoints the FSA Board
- The Financial Services and Markets Act has four statutory objectives:
  - market confidence: maintaining confidence in the financial system
  - public awareness: promoting public understanding of the financial system
  - consumer protection: securing the appropriate degree of protection for consumers
  - reduction of financial crime: reducing the extent to which it is possible for a business to be used for a purpose connected with financial crime

Regulatory Compliance

What is PCIDSS?

- The Payment Card Industry Data Security Standard (PCIDSS)
- What's is all about?
  - Governs how credit card data is secured
  - Covers all users who store credit card data
  - Comes into effect on the 30th June
  - Members include
    - Visa, Mastercard, American Express
  - Consists of 12 requirements that covering items such as:
    - Protection of data & Vulnerability management
    - Network Security & Access Control
- Sets requirements for the storage and monitoring of credit card information
  - Currently 4 levels, based on the volume of credit card transactions
  - At the highest level the company can be audited quarterly
  - At a cost of up to £10,000 per audit

Regulatory Compliance

What do I need to do?

- The best way is to follow a set of industry recognised standards. Four common standards are:
  - **COSO**
    - Committee of Sponsoring Organisations of the Treadway Commission
  - **ISO**
    - International Standards Organisation
      - ISO 9001 quality controls
      - ISO 27001 (17799) IT Security framework
  - **CoBIT**
    - IT Controls framework
  - **ITIL**
    - IT Support framework

Regulatory Compliance

CoBIT controls linked to standards for SOX

Figure 1—Control Processes

CobiT Control Objective Heading	PCAOB IT General Control Heading: Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

- **IT controls may already exist**
- **Need consistency and quality control**
- **Evidential material lacking**
- **Controls maybe Silo'd today**
- **Cost of compliancy is escalating**
- **Need a holistic approach**
- **Culture change involved**

Regulatory Compliance

What are Controls?

- COSO Definition of Internal Control
  - Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and efficiency of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations
  - Key Concepts
    - Internal control is a process. It is a means to an end, not an end in itself
    - Internal control is effected by people. It's not merely policy manuals and forms, but people at every level of an organisation
    - Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board
    - Internal control is geared to the achievement of objectives in one or more separate but overlapping categories

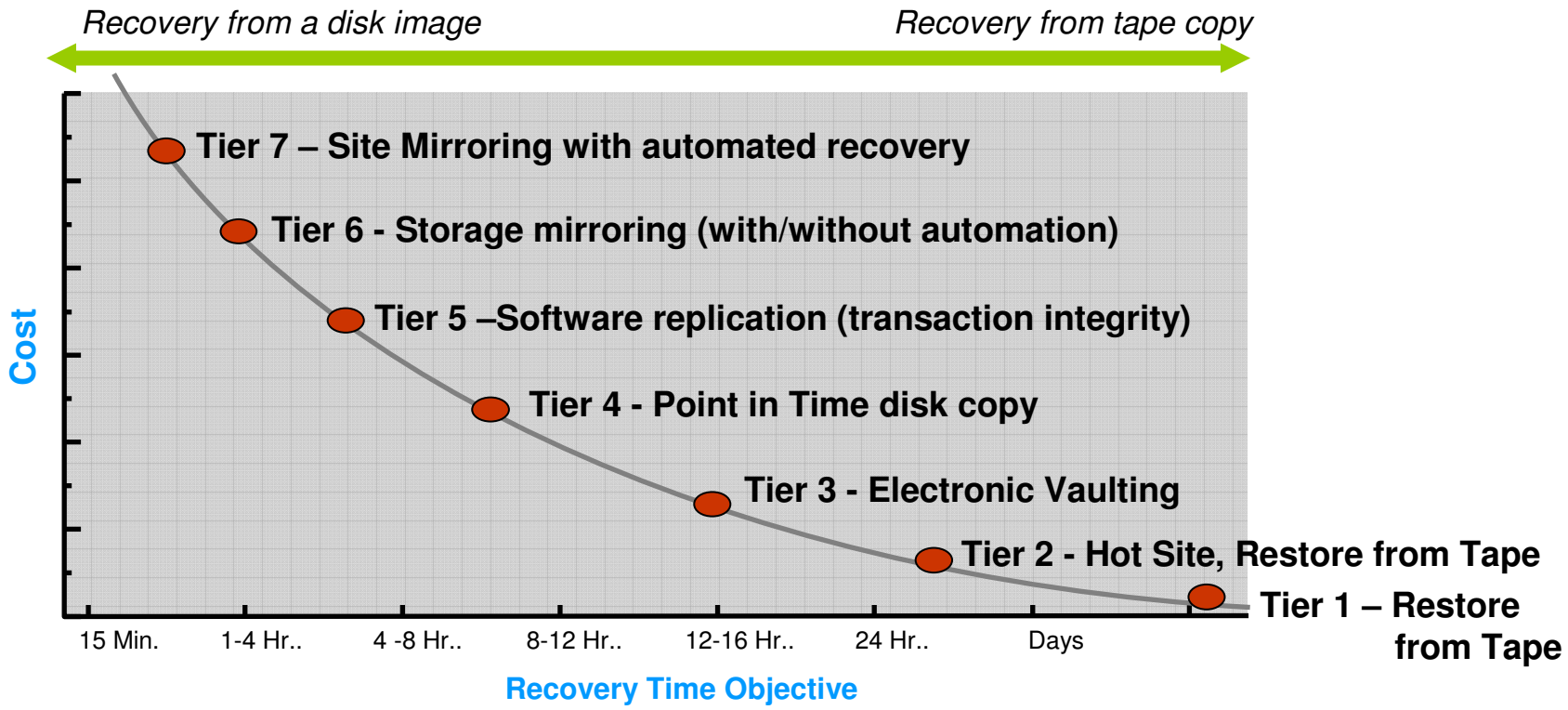
Regulatory Compliance

How do I do it?

- **Business Continuity**
  - Business Continuity Tiers
  - Protect the Business
- Security & Access Management

Regulatory Compliance

Business Continuity Tiers

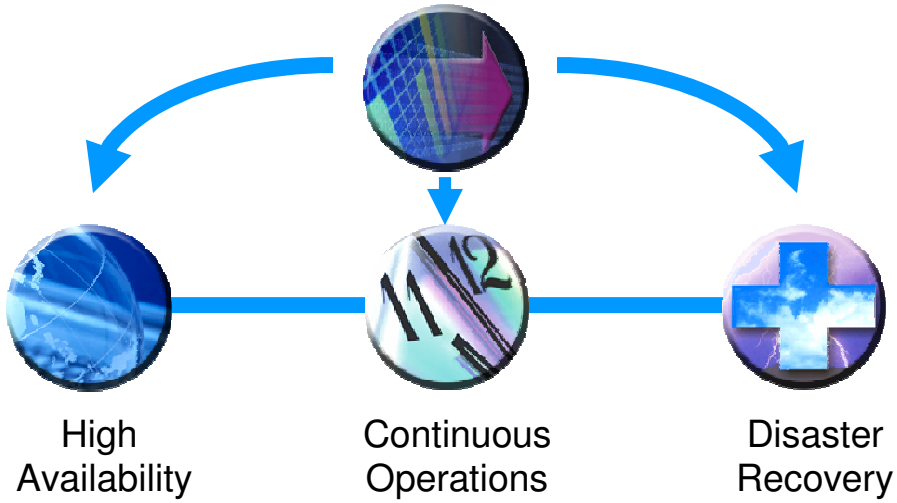


LOGICALIS integration solutions

Regulatory Compliance

Business Continuity - Protect the Business

- Help reduce business risk, by increasing resilience
- Help secure and protect business information
- Stay competitive and maintain market readiness
- Protection of critical Business data
- Recovery is predictable and reliable
- Operations continue after a disaster
- Costs are predictable and manageable
- **Its all about confidence that we can and will recover!**



LOGICALIS integration solutions

Regulatory Compliance

Business Continuity

- Testing, Testing and even more Testing!
- Regular testing of the process
- Validating the replicated data if at Tier 4 and above
- Get independent 3rd party to perform different parts the test
  - Proves process & documentation are up to date
  - Gives a level of comfort that recovery can take place even if key personnel are missing
- Perform a test without warning
  - Invoke DR at 15:00 on a Sunday afternoon
    - What about Bank Holiday test – Only joking!
    - Middle of the school holidays

Regulatory Compliance

Recent IBM Redbook on the Subject:

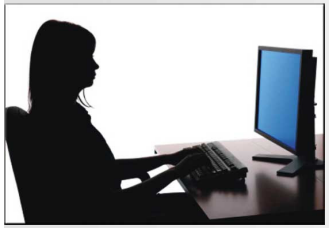
- IBM System Storage Business Continuity: Part 1 Planning Guide
- Can be found at:
  - Hopefully on the Handout CD; if not at :-
  - http://www.redbooks.ibm.com/abstracts/sg246547.html?Open

Regulatory Compliance

How do I do it?

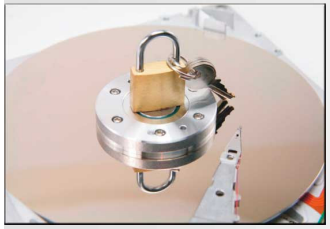
- Business Continuity
  - Business Continuity Tiers
  - Protect the Business
- **Security & Access Management**

Regulatory Compliance - Security & Access Management



Identify when an privileged user accesses private records

Protect sensitive data with encryption solutions



Prevent unauthorized applications from attacking system integrity

Validate that medical records are kept private

Prevent a DBA from accessing payroll records

- **According to a recent IBM survey, 64% of CIOs surveyed see security compliance and data protection as one of the most significant challenges facing IT organizations.**
- **86% of internal security incidents are perpetrated by a company's most privileged and technical users such as administrators, outsourcers, consultants, or other power users.***
- **Between February 2005 and 2006, almost 104 million data records of U.S. residents have been exposed due to security breaches.****

LOGICALIS integration solutions

Regulatory Compliance

Should be based on least privileged access

- What does this mean?
  - Users should only have access to the resources they need to do their job
- Typically called Role Based Access Control (RBAC)
- Each implementation will be subtly different, however, any RBAC project needs:
  - Buy in from the business as we will need their help
  - Will be a much bigger project than anyone first anticipates
  - Will need owners identifying for all related assets, this is often the most difficult part of the project:
    - Users (Userids, Logonids or ACIDS)
    - Data & Security Profiles for the data

Regulatory Compliance

Typical RBAC project looks like:

- Project Definition Workshop
- Analysis
- Build
- Testing
- Implementation
- Support
- Final Cleanup

Regulatory Compliance

What we need to ensure is?

- Access
  - Are *access policies* and *data disclosure rules* implemented consistently across every application, data source and operating system?
  - Are the right people being authorised?
- Provisioning
  - Is every user account on every resource valid?
  - Is user access configured correctly to every resource?
  - And does it stay that way?
- Audit
  - Can I prove all of this to the auditor, for all users, systems and operational information?

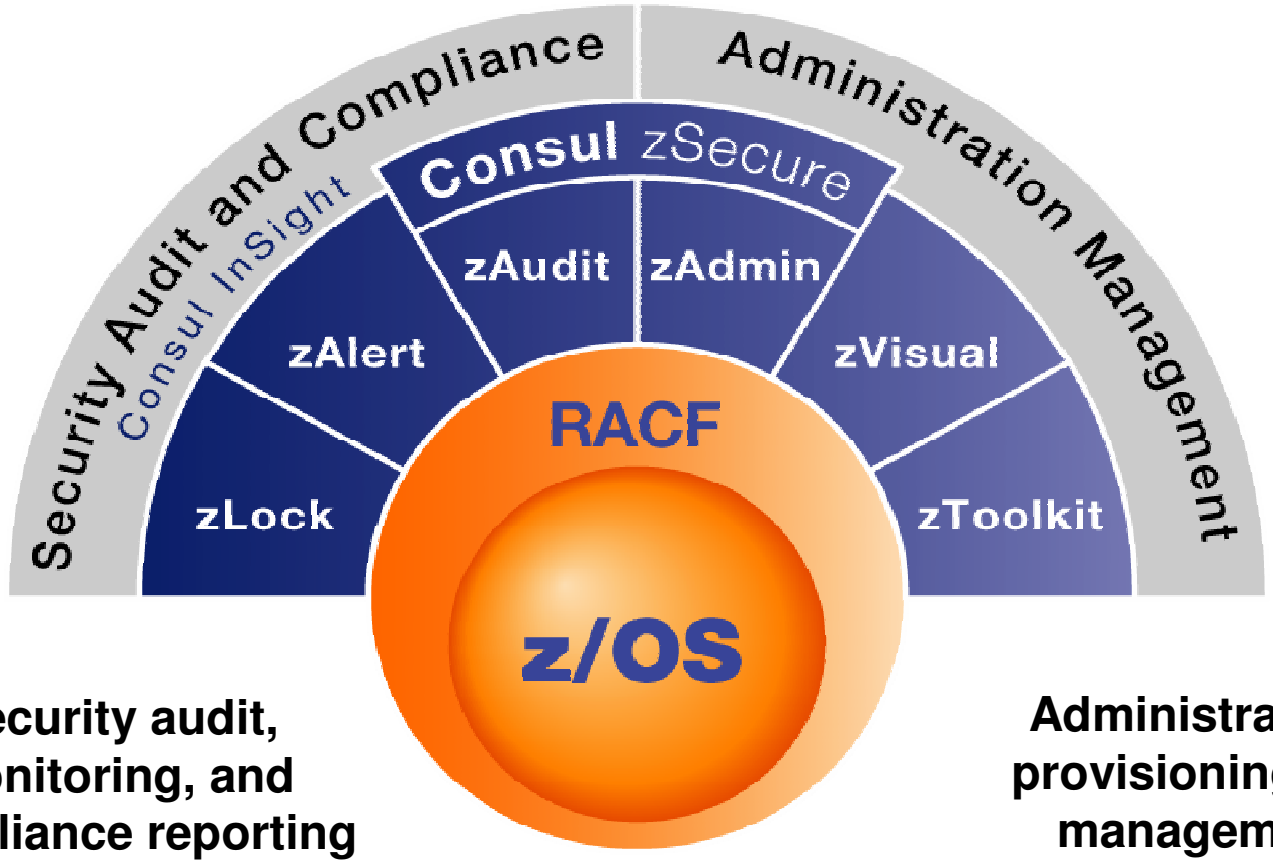
Regulatory Compliance

Validation of Users and their access

- User validation
  - Can I link to the HR system?
  - What is the leavers and joiners process?
  - What is the movers process?
  - What do I do about inactive users?
    - What do the standards say?
- Access Validation
  - Who has what role?
    - How do I validate this?
    - How often do I validate this?
  - What does the role have access to?
    - How do I validate this?
    - How often do I validate this?

Regulatory Compliance

IBM Tools



Security audit, monitoring, and compliance reporting

Administration, provisioning and management

LOGICALIS integration solutions

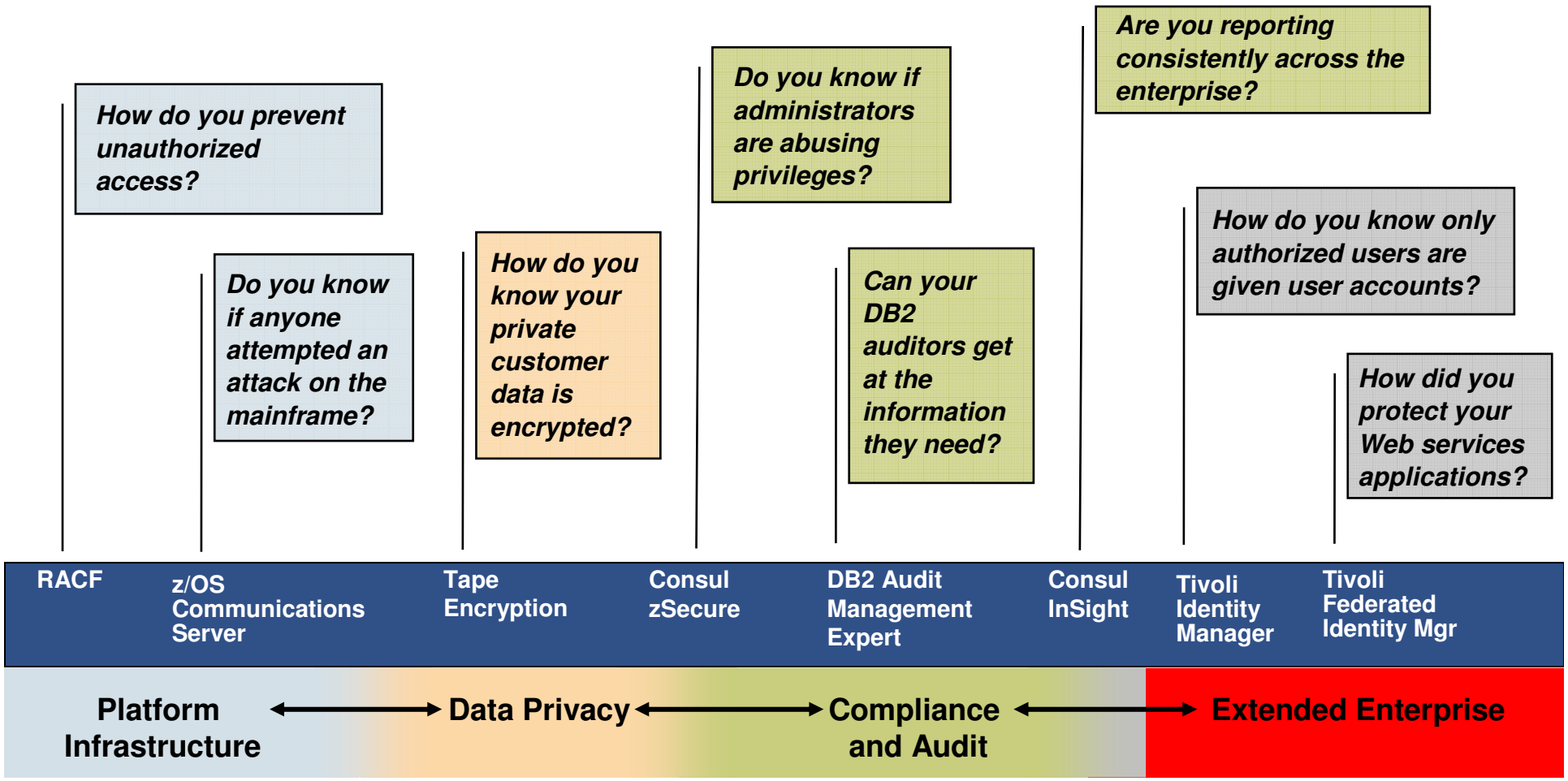
Regulatory Compliance

IBM Tools

zSecure Suite	Core Functions
zAdmin	**Efficient and Automated Security Administration**
zAudit	**Analysis , Reporting, Systems Integrity and Analysis, Event Detection**
zAlert	**Intrusion Detection and Alerting** **Compliance Monitoring of Privileged and Authorized Users**
zLock	**Compliance Enforcement of RACF Administrators** **Enforcement of RACF Naming Conventions and Security Standards**
zVisual	**Windows-based RACF Administration**
zToolkit	**CICS based RACF administration** **API toolkit between CICS applications with RACF, externalize security for CICS**
z/OS agent for InSight	**Integrate z/OS into Enterprise Compliance Dashboard** **Enable Business Auditors to Review z/OS Activities**

Regulatory Compliance

What Questions do the auditors ask?



Regulatory Compliance

3rd Party Tools

- Computer Associates
  - http://www.ca.com/gb/
- Vanguard Integrity Professionals
  - www.go2vanguard.com
  - Look at the conference well worth going for in-depth technical training
- Beta Systems
  - http://ww2.betasystems.com/en/products/dci/zsecurity/index.html
- Allen Systems Group
  - http://www.asg.com/products/productarea_list.asp?id=security
- ASPG
  - http://www.aspg.com/data-security.htm

Regulatory Compliance

- Shareware/Free Utilities
- Nigel Pentland
  - www.racf.co.uk - PC based reporting utilities

Regulatory Compliance

- IBM has recently launched a new website dedicated to Governance, which appears to have lots of useful information with sections on:
  - Business Resilience
  - Security
  - Service Management

www.ibm.com/software/tivoli/governance

Summary

- Compliance in one form or another affects us all
- Even as zSeries practitioners we need to understand how compliance will impact us
- We are going to be asked what controls are in place
- We will be expected to keep records that controls are checked
- You need to engage with your auditors, even if they know nothing about zSeries

Sales Pitch

- **GSE Annual Conference**
- **30th & 31st October 2007**
- **Chesford Grange Hotel, Kenilworth**
- 20+ Vendors
- 350+ Attendees
- Details can be found at:
  - www.gse.org.uk/tyc
  - Is being constantly updated
- Would be good to have you all there!

GSE
GUIDE SHARE EUROPE

LOGICALIS
integration solutions

Thanks

Mark Wilson

Logicalis

110 Buckingham Avenue
Slough, Berks, SL1 4PF

Mobile: +44 (0) 7768 617006

Email: mark.wilson@uk.logicalis.com

Chairman GSE Large Systems Working Group

LOGICALIS
integration solutions


thank you
LOGICALIS
integration solutions