Regulatory Compliance and the Mainframe

Reg Harbeck
Disclaimer

>This presentation is based on current information and resource allocations as of August 17, 2007 and is subject to change or withdrawal by CA at any time without notice. Notwithstanding anything in this presentation to the contrary, this presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this presentation remain at CA’s sole discretion. Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA will make such release available (i) for sale to new licensees of such product; and (ii) to existing licensees of such product on a when and if-available basis as part of CA maintenance and support, and in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of such product who are current subscribers to CA maintenance and support on a when and if-available basis. In the event of a conflict between the terms of this paragraph and any other information contained in this presentation, the terms of this paragraph shall govern.

>CERTAIN INFORMATION IN THIS PRESENTATION MAY OUTLINE CA’S GENERAL PRODUCT DIRECTION. ALL INFORMATION IN THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY AND MAY NOT BE INCORPORATED INTO ANY CONTRACT. CA ASSUMES NO RESPONSIBILITY FOR THE ACCURACY OR COMPLETENESS OF THE INFORMATION. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT WILL CA BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
Agenda

> The Regulatory Compliance Context

> Enabling Compliance:
  - Identity and Access Management
  - Elimination of “Loose Ends”
  - Monitoring, Auditing & Reporting
  - Ease of Administration and Provisioning
  - Integrity and Privacy of Data

> Example solutions and how they fit

> Conclusion & Discussion
The Complexity of Regulatory Compliance

Business Issues
- Business Continuity
- Business Enablement
- Risk Management
- Operational Efficiency

Industry Regulations
- EU Data Protection
- Basel II
- ISO 27001, 27002
- Sarbanes – Oxley
- PCI DSS
- HIPAA
- GLBA

Risks
- Credit Risk
- Market Volatility
- Reputation
- Liability
- Competition
- Operational Risk

Continuous Compliance cuts across all areas
Putting it into Context

The most common element of all regulations is a **strong set of internal controls.**

> These controls must provide:

- **Accountability** – Who performed an action, who approved it, when was it done, and what was the result?

- **Transparency** – All business processes and controls must be fully understood, and clearly documented.

- **Measurability** – All internal processes must be able to be measured and evaluated as to success or failure. Measurement is done through auditing, logging, correlation and visualization.
Major Types of Regulations and Laws

source: IT Compliance Institute
Internal Control Frameworks

> Regulations don’t prescribe actual technologies to use for compliance. Instead, most companies adopt internal control frameworks as models of “best practice” for compliance.

> Some popular frameworks include:

- **COSO** – defines requirements for effective corporate governance
- **CobiT** – defines IT governance and control practices
- **ISO 27001, 27002** – define best practices in information security
- **ITIL** – defines the processes and activities to support IT services
The Importance of Security for Compliance

<table>
<thead>
<tr>
<th>Regulation Technology</th>
<th>SOX</th>
<th>HIPAA</th>
<th>Gramm-Leach-Bliley</th>
<th>Sec 17A-4</th>
<th>21 CFR Part 11</th>
<th>Basel II</th>
<th>USA Patriot Act</th>
<th>CA SB 1386</th>
<th>Canada PIPEDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Compliance</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Intelligence &amp; Data Warehousing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document / Content Management &amp; Access</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Records Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Archiving</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Storage</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Example: SOX Impact on IT

> SOX is not only for the financial accountants and auditors!

- Consider big picture:
  - If financial data resides on IT-maintained systems, those systems then are subject to SOX scrutiny
- Consider data maintained on IT systems, and consider significance of that data
  - Financial data
  - Sales forecasts
  - Confidential/”insider’’ information (email)
  - … and more
- Concern is not only with raw data itself, but also how it is processed, where it is kept, who can access/manipulate it, and more
Regulatory Compliance Factors
The Three “Horns” of Compliance

1. Efforts in trying to comply with the regulations

2. Penalties for failing to comply (plus bad publicity)

3. Regulations that require publicizing exposure incidents
Horn 1: Efforts to Comply

> Forces many companies to reflect on their current business practices

- Are current procedures optimal?
  - What are the strengths? Weaknesses? Where do deficiencies exist?
  - Which deficiencies violate rules? What are liabilities, material weaknesses?

- Are process/procedural changes warranted?
  - Can business benefit be had through change?
  - Can procedures be streamlined?
  - Can administrative overhead be simplified?

- Consider cost:
  - Can a cost savings be realized through change?
  - Can compliance costs be minimized and/or more effectively managed?
Dear Ms. SarBox:

The SEC estimates that it will cost $91,000 annually in order to be in compliance with just Sec. 404. Is it really worth it?

*Cheap in Charleston*

Dear Cheap,

Try looking at it from another angle.

Cost of compliance: $91,000.

Not being a convicted felon: Priceless.

Source:  [http://www.sox-online.com/ms_sarbox.html](http://www.sox-online.com/ms_sarbox.html)
> There are many laws covering data privacy, such as:

- New Jersey requires businesses destroy un-needed customer data and notified customers if there is unauthorized access
- Louisiana requires notification of residents, plus the state government, if confidential data compromised
- Illinois law is similar but does not require notification of state officials
Business Value: a Strategic Approach

> “Think through the brick”

> Implicit in Regulations is Well-Run Business

> Unified & Simplified Management = Strength

> Anticipate Opportunities & Challenges
Compliance is *not* the final goal!

> Most companies have focused here:

- Document & Evaluate Controls
- Test Operating Effectiveness
- Prepare Report on Internal Controls
- Attest & Report

Fix Weak Controls

- Management Task
- Auditor Task

Business efficiency and effectiveness

Lower costs
Easier compliance

Attest
& Report

Automate Sustain

Improve Business Perf.

Most companies have focused here:
Enabling Compliance

> Identity & Access Management
> Elimination of “Loose Ends”
> Monitoring, Auditing & Reporting
> Ease of Administration
> Integrity and Privacy of Data
Identity & Access Management

> Focus on business value
  - Policy-based security, not technical constraints

> Strategic design
  - Enterprise-wide, synchronization, integration
  - Comprehensive coverage

> Preempt your vulnerabilities
  - Default “Deny”
  - Separation/segregation of duties
  - One user per account
    - Including Super User
Access Management: Key Compliance Capabilities

> All regulations require effective controls on all user access to all sensitive IT resources, including:

- Web-based applications
- Critical system services
- System files, databases, and repositories
- Host-based (non-web) applications and files
- Mainframe applications and data
- Super User privileges
- Separation of duties
Elimination of “Loose Ends”

> People don’t like to “give back” access
  - Creates “back doors”

> It’s common not to know all of a person’s accounts
  - When they leave, they leave a door open

> Tracking down extraneous accesses & IDs is not easy
  - Security product stats insufficient
  - Heavy-handed deletions backfire

> Failing to do so can lead to exposure...
  - Major NA retailer credit card info
  - Major financial institution in France: insider exposures
Cleaning Up Loose Ends: Key Compliance Capabilities

> SOX compliance generally requires proper internal controls to ensure:
  - User definitions/directories are properly maintained
  - Security entitlements are properly maintained

> PCI compliance requires the revocation of users every 90 days
  - Cleaning up covers entitlements as well

> ISO 27001 cites management review of access rights using a formal process
Monitoring, Auditing & Reporting

> Who
  - Which IDs are defined and in use

> What
  - Resource entitlement reporting
  - Administrative capabilities
  - OS configuration

> When
  - Logging of security and administrative actions
  - Visibility of changes to key parameters, datasets

> Why
  - Business impact, exposures
  - Compliance relevance
Monitoring, Auditing & Reporting: Key Compliance Capabilities

> Ease of querying and reporting on system configuration
  ▪ Ensure OS configuration and environment are solid
  ▪ Real-time on-line and batch reporting and alerting

> Ability to relate security configuration to regulatory requirements
  ▪ Simple preconfigured reports on security files
  ▪ Flexible customization for unique environmental factors
  ▪ Minimal resource usage or performance impact

> Regular monitoring and tracking of security activities
  ▪ Logging of violations and sensitive resource usage
  ▪ Tracking of security administration
Ease of Administration

> **Enable Security Administrators**
  - Experienced personnel are buried in demands
  - “New Generation” is unused to mainframe interface
  - Complicated interfaces lead to mistakes

> **Keep It Straightforward, Simple**
  - Single point of graphical administration
  - Ease of querying accesses and configuration
  - At-a-glance awareness
Ease of Administration: Key Compliance Capabilities

> Graphical, and auditable, management of all user profiles and access rights
> Enable role-based definition of accounts, accesses
> Common graphical interface for multiple tasks
Integrity and Privacy of Data

> **Critical, sensitive production data**
  - Strategic corporate information
  - Customer data
  - Employee and partner information

> **Danger of loss and exposure**
  - Offsite tape backups
  - Data sent to partners on tape

> **Undesirable consequences**
  - Have to notify public of customer data exposure
  - Impact on corporate reputation
  - Possible law suits, charges
Integrity and Privacy of Data: Key Compliance Capabilities

> Encryption of all sensitive tape data sent offsite
> Easy, transparent implementation
> Comprehensive, simple key management
> Free, secure decryption for authorized third parties
Example Solutions
Example Solutions

> Identity & Access Management
> Elimination of “Loose Ends”
> Monitoring, Auditing & Reporting
> Ease of Administration
> Integrity and Privacy of Data
Identity & Access Management

CA provides a comprehensive access management suite to protect critical resources, including:

- CA SiteMinder: Web-based applications
- CA TransactionMinder: Web Services
- CA Access Control: Host-based resources
- CA ACF2 and CA Top Secret Security: Mainframe
  - Plus DB2 Options
Elimination of “Loose Ends” – CA Cleanup

- Identifies unused IDs and accesses
- Reports on activity at any time
- Can automatically generate commands for removal
- Creates recovery file for deleted logon ids and accesses
- Supports multiple security databases in synchronized environments
Monitoring, Auditing & Reporting

> CA ACF2 and CA Top Secret have long provided for basic needs

- Flexible/powerful logging capability
- Powerful out-of-box reports using security logs for:
  - Administrative changes
  - Event reporting
  - Operational reporting
- Powerful out-of-box capability using actual security data basis for:
  - “Who has...” user entitlement reporting
  - “Who can...” resource control entitlement reporting
CA Responds with CIA

> You told us your needs, we listened

> We’ve responded with Compliance Information Analysis (CIA) in CA ACF2 and CA Top Secret r12

> CIA Features:

  - Aids assessment of security policy
  - Flexible foundation for compliance reporting
    - Facilitates ad-hoc queries
  - Minimizes performance constraints
  - Integrates multiple security data bases
    - Provides mainframe enterprise-wide capability
CIA Overview

- Uses data model optimized for compliancy requirements
- Data model defined in RDB (DDL’s)
- Data downloaded from security database(s)
- Data loaded into DB2
  - Other RDBs to follow
- CA ACF2 and CA Top Secret distribute ready-to-use compliance reports
CA Auditor for z/OS

- Integrity auditing tool - Helps achieve compliance
  - Non-systems people can see potential exposures
  - Facilitates the review of OS resources
  - Assurance that OS integrity meets corporate standards
  - Establishes baselines for internal and external audits
  - Validates the integrity of systems
  - Quickly identifies changes and potential exposures to OS programs, files and libraries
  - Not dependent on a particular ESP or OS version
Ease of Administration: CA Web Administrator for ACF2 and Top Secret

- Seamless Administration of CA ACF2 and CA Top Security environments
- Enables Remote administration
- Reduces the learning curve for new generation of users
- Helps towards centralizing Security Management efforts
## Integrity and Privacy of Data: A Tape Data Loss Epidemic?

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th># Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAN 07</td>
<td>IRS (26 tapes)</td>
<td>unknown!?</td>
</tr>
<tr>
<td>MAY 07</td>
<td>Large Mainframe Manufacturer</td>
<td>unknown!?</td>
</tr>
<tr>
<td>JUN 05</td>
<td>A Financial Company in the City</td>
<td>3,900,000</td>
</tr>
<tr>
<td>SEP 06</td>
<td>Credit Card Service / Retail</td>
<td>2,600,000</td>
</tr>
<tr>
<td>DEC 05</td>
<td>Large Midwestern Bank</td>
<td>2,000,000</td>
</tr>
<tr>
<td>FEB 05</td>
<td>A Large American Bank</td>
<td>1,200,000</td>
</tr>
<tr>
<td>MAY 05</td>
<td>Media and Entertainment Co.</td>
<td>600,000</td>
</tr>
<tr>
<td>JUN 07</td>
<td>Ohio State Workers</td>
<td>500,000</td>
</tr>
<tr>
<td>JAN 06</td>
<td>Home Services Co. in RI</td>
<td>365,000</td>
</tr>
<tr>
<td>DEC 05</td>
<td>Financial Service Co in Hartford</td>
<td>230,000</td>
</tr>
<tr>
<td>DEC 05</td>
<td>Large Hotel Chain</td>
<td>206,000</td>
</tr>
<tr>
<td>APR 05</td>
<td>Discount Brokerage Service</td>
<td>200,000</td>
</tr>
<tr>
<td>OCT 07</td>
<td>Virginia Public Ins. Agency</td>
<td>200,000</td>
</tr>
<tr>
<td>DEC 06</td>
<td>Medical Insurance Company.</td>
<td>200,000</td>
</tr>
<tr>
<td>JAN 08</td>
<td>Credit Company / Iron Vault Site</td>
<td>150,000</td>
</tr>
<tr>
<td></td>
<td>Others….</td>
<td>768,368</td>
</tr>
</tbody>
</table>

**Tape Records Compromised** > 13.1M

Source: Privacy Rights Clearinghouse, 2008
Key Management Best Practice

> Creation, tracking, auditing, backup, recovery and removal of expired keys integrated into CA 1, CA TLMS

> Keys always protected
Flexible Portability

Free B2B decryption software for your partners

B2B with Partners

Windows and Unix

Multi-Decryption Utility for Open Systems
Total Tape Compliance Strategy

Where:
> Tape Libraries, Archives, Vaults, Silos, DR sites, Outdated Media, Migrations, etc.

Opportunities:
> Secure Data Transfer, B2B Partner Security, Less Complexity and Costs, etc.
CA Tape Encryption

- Encrypt/decrypt physical tapes for any z/OS application
- Integrated System z HW compression
- Easy to use and implement
- Complete, automated encryption key life cycle management
- Lowest risk
- Use hardware and software you have invested in
- No changes to your infrastructure
- Greatest value – one integrated, complete solution
  - zIIP-enabled!
The Problem: Managing Encryption Keys Is Complex, Costly, and Error Prone

Administrative Overhead

Many Encryption Technologies, Vendors and Processes

Key Management Issues Are The Source Of Most Operational Problems, Increasing Costs*

- Complications with Key distribution: 57%
- Issues w/ Key backup & Recovery: 48%
- Complications with key rollover: 35%
- Difficulty in performing data recovery: 30%
- Problems with audit of Key life cycle: 27%
- Inflexibility to support minor configuration changes: 23%
- Lack ability to perform reconnaissance or eDiscovery: 22%

*Source: Forrester Research Survey
“The State of Data Security in North America”
August 2007
Automated, Full Lifecycle Key Management – CA Tape Encryption Key Manager

CA’s Efficient Key Management Solution Value To Customer:
- Consolidated Mgmt
- Automation
- Central Repository
- Cost Containment
- Cross Platform
- Security Compliance
CA KM Security and Tape Management

CA Tape Encryption Key Manager

Tape Management Systems

Security Systems

Supports All Major Mainframe Tape Management Systems Including:
- CA 1,
- CA TLMS,
- IBM DFSMSrmm,
- ASG ZARA,
- BMC Control/M,

Supports All Major Mainframe Security Systems Including:
- CA ACF2,
- CA Top Secret,
- IBM RACF

Tape Encryption System

CA Tape Encryption

IBM®

TS1120, 3592 E05
CA Tape Encryption Key Manager

> Enhances TS1120/3592E05 control
> Manages mainframe and distributed tape key environments
> Automates generating and maintaining digital certificates for use by the TS1120
> Manages the Full Life Cycle of the digital certificates
> Ensures keys never prematurely expire
> Automates manual processes Storage Administrator and Security Administrator
> Complies with NIST 800-57 standards
Summary

- **Focus on business value**
  - Look beyond compliance requirements
  - Embrace compliance….use it to grow your business!
  - “Virtuous cycle”

- **Strategic design**
  - Unify and Simplify with the right tools
  - Have a clear plan and approach
  - Key to compliance automation is a comprehensive, integrated identity and access management platform

- **Preempt your vulnerabilities**
  - To regulations, disasters and capricious malice
  - “Know thyself” – identify and preclude potential exposures