PCI Compliance
for Large Computer Systems

Jeff Jilg, Ph.D.
atsec information security

August 3, 2010 – 3:00pm
Session 6990

About This Presentation

- About PCI assessment
- Structure and requirements of the program
- How to prepare
- Avoiding common pitfalls

PCI =
Payment Card
Industry

PCI Assessment

- What: Compliance with the PCI DSS
- Why: Mandated by the major credit card brands
- Who:
  - Any organization storing, processing or transmitting credit card data
- When: Annually
- How: Depending on the level determined by the card brand compliance is assessed by using a
  - SAQ
  - QSA accredited through the PCI SSC
- Goal: Report of Compliance (Passing!)

DSS= Data Security Standard

PCI SSC= PCI Security Standards Council

QSA= Qualified Security Assessor

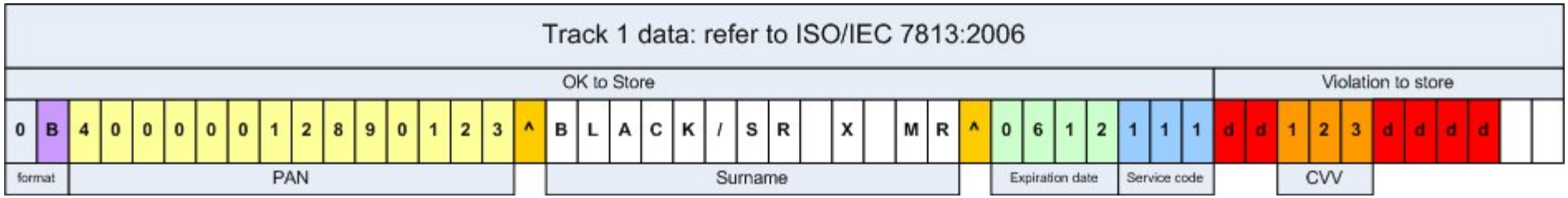
SAQ=Self Assessment Questionnaire

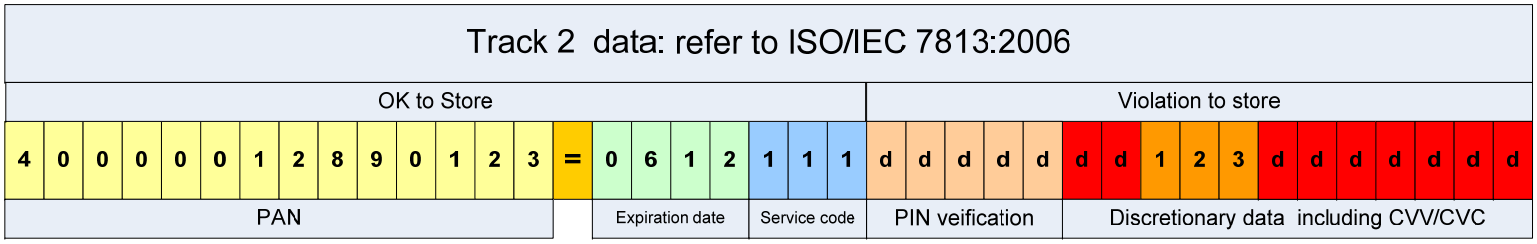
PCI DSS Structure and Requirements

- The PCI SSC was founded by five international payment card brands in 2004.
  - American Express
  - Discover Financial Services
  - JCB International
  - MasterCard Worldwide
  - Visa, Inc.
- The PCI SSC mission includes developing and maintaining common security standards across the brands
- Mandated via each brands contractual agreements, and card brand security programs

PCI DSS Structure and Requirements

- Intended to protect card holder data.





The Card Brand Security Programs

Security Program	URL
The MasterCard Site Data Protection Program (SDP)	http://www.mastercard.com/us/sdp/index.html
Visa Cardholder Information Security Program (CISP)	http://usa.visa.com/merchants/risk_management/cisp_overview.html
American Express Data Security Operating Policy Compliance Program (DSOP)	https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=spinfo&ln=en&frm=US&tabbed=complienceRequirement
Discover Information Security & Compliance (DISC)	http://www.discovernetwork.com/fraudsecurity/disc.html
JCB	http://www.jcb-global.com/english/pci/

All use the current version of the PCI DSS (currently 1.2.1)
- available from https://www.pcisecuritystandards.org/index.shtml

PCI DSS Structure and Requirements

The Twelve Key Requirements of PCI DSS	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.

PCI DSS Structure and Requirements

The Twelve Key Requirements of PCI DSS	
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

PCI DSS Structure and Requirements

- Card brand program requirements
  - Annual assessment of compliance with PCI DSS
  - Quarterly Requirement for external network vulnerability scanning by an ASV
  - COTS Payment Applications must be from the approved list
  - Certified Payment Transaction Security Devices

ASV = Approved Scanning Vendor

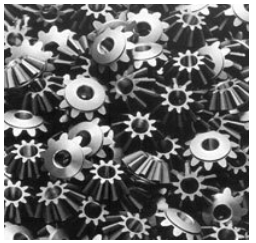
COTS= Commercial Off The Shelf

PCI DSS Structure and Requirements

- PCI DSS detailed requirements **summary**
  - Full mapping from high level security policy through configuration standards to implementation
  - Penetration testing and internal network vulnerability scanning on major network changes
  - Secure programming standards
  - Organizational, process, and HR policies

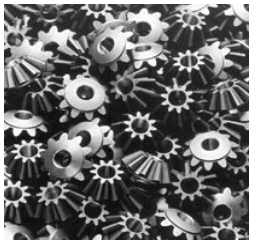
HR= Human Resource

An Approach for Compliance



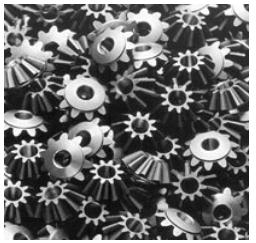
- The first time is always the hardest
- Build security measurement, and assess-ability into the business processes
- Always be ready for an assessment
  - A properly prepared organization shouldn't need to do much preparation. They should be ready at ANY time.
  - Be aware of changes in the standards.
    - Keep up to date with them.
    - Reviewing for changes once a year - one month before the assessment leads to problems.

An Approach for Compliance



- Understand the assessment requirements and how z/Series supports you in meeting them.
- There may be differences in how controls can be met or interpretations needed for your environment. e.g.:
  - Malware requirements in PCI DSS
  - File Integrity Checking for PCI
- Have a GOOD and effective risk management process.
  - That matches YOUR organization
- Specify compensating controls wisely
  - Too many are a red flag: but they are probably necessary!

An Approach for Compliance



Reuse other assessment results

- PCI DSS, FISMA, ISO/IEC 27001, SAS/70, SOX, EuroSOX etc.
- Use assurance given by product certifications:
  - Common Criteria, FIPS 140-2 etc.
  - Vendors spend a lot of resource and money giving you this assurance.
- Integrate security management systems:
  - BUT each assessor needs to make his or her own determination
- Awareness training, HR processes, internal audit of organizational processes and others are common

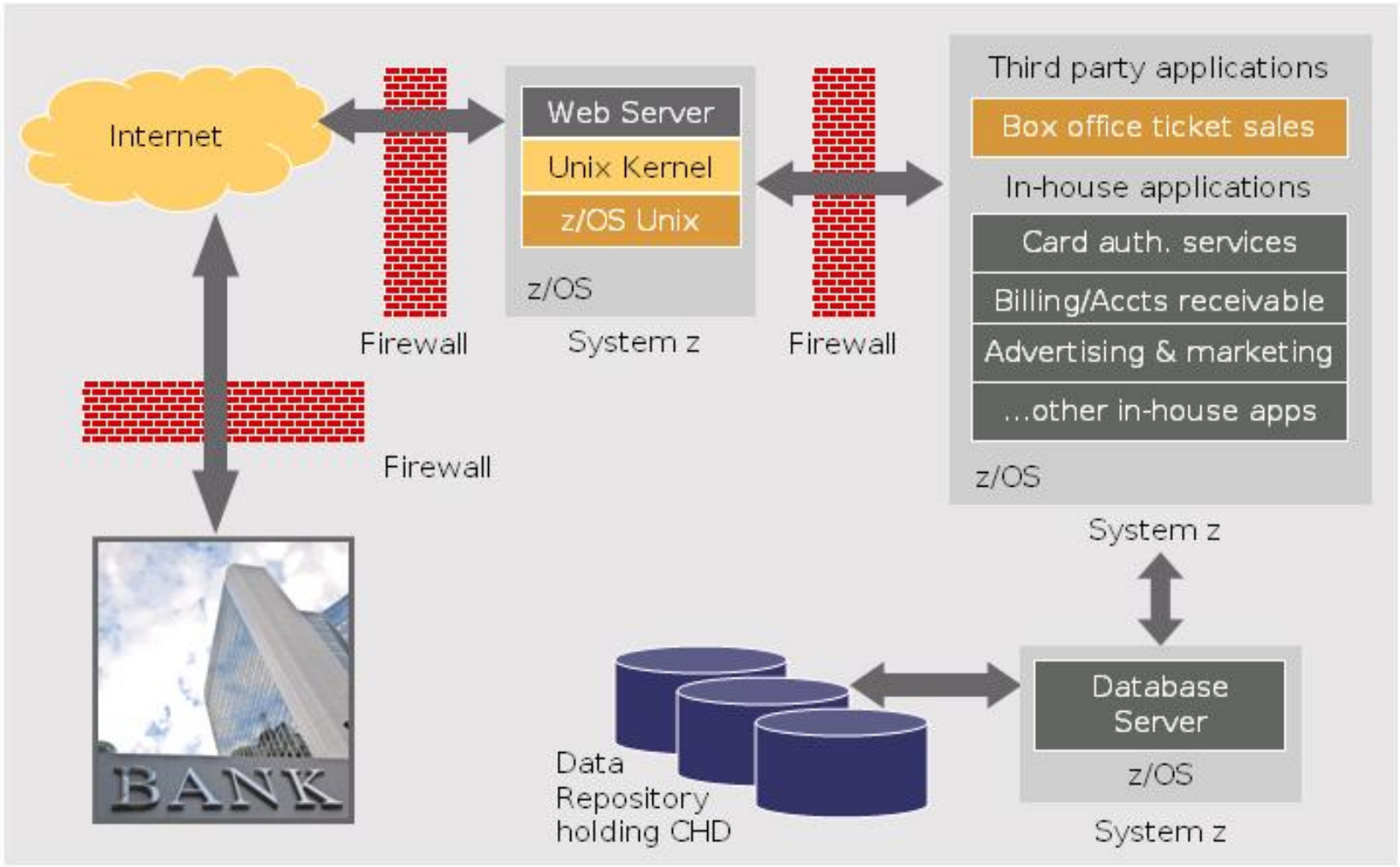
Do not reinvent the wheel!

Use it!

Leverage systems

SHARE

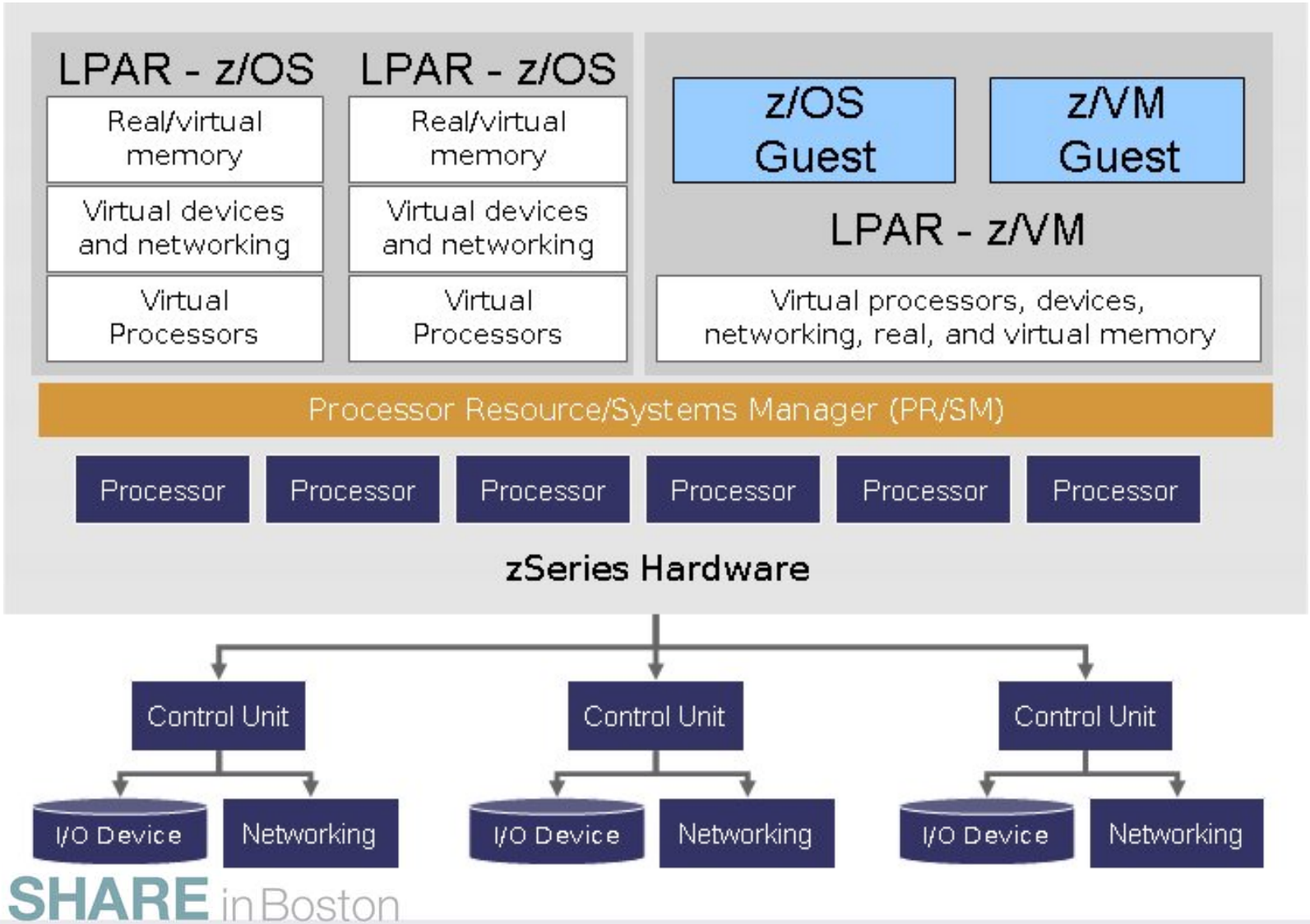
A Typical PCI DSS Configuration



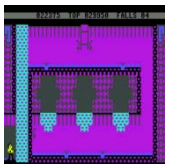
System z Virtualization

- Multiple mechanisms to virtualize computing resources
- Every computing resource (CPU, Memory, Devices) can be virtualized on a System z
- Hypervisors' environments (PR/SM and z/VM) are completely separated from other computing environments provided by that hypervisor.
- The hypervisor is in complete control of the actual computing resources and only allows access to assigned resources.
- The separation capabilities of the hypervisors have been subject to thorough security evaluations
  - PR/SM – Common Criteria EAL5
  - z/VM – Common Criteria EAL4

System z Virtualization Architecture



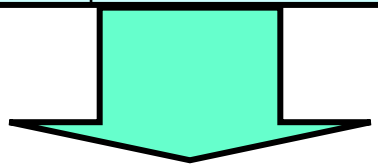
Pitfalls of Large Computing Systems



- Large, complex environment
- Tons of security critical configuration options
- Requires careful use and assignment of access rights and privileges
- High reliability implies high redundancy – also of critical data
- Customer developed system exits, services, and authorized programs can introduce critical vulnerabilities
  - Developers often not aware of the precautions needed
  - Often also true for third-party software

LCS PCI Challenges (2.2.1)

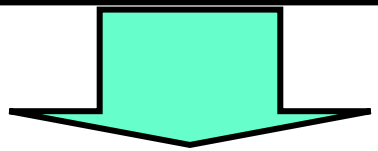
PCI DSS Rqmt	Testing Procedure
2.2.1 Implement only one primary function per server	**2.2.1** …verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.



- PCI SSC “This reduces possibility of access to Cardholder Data (CHD) through misconfigured applications on one server.
- LCS with proper segregation methods can ensure separation and reduce risks.
- Refer to PCI SSC “Navigating the PCI DSS” 2.2.1 where they point out this is primarily for non mainframe systems.

LCS PCI Challenges (6.1)

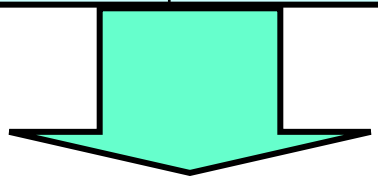
PCI DSS Rqmt	Testing Procedure
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed.	**6.1.a/b** …compare the list of security patches installed on each system to the most recent vendor security patch list to verify that current vendor patches are installed. ….must be installed within one month



- PCI SSC: objective is to reduce vulnerability exposure
- Installing untested PTFs (Program Temporary Fixes, aka patches) within a month may be cost ineffective with given resources
- QSA assessment of the patching process should include IBM testing and subject organization testing procedures
- Assessment of the associated patch criticality should be included

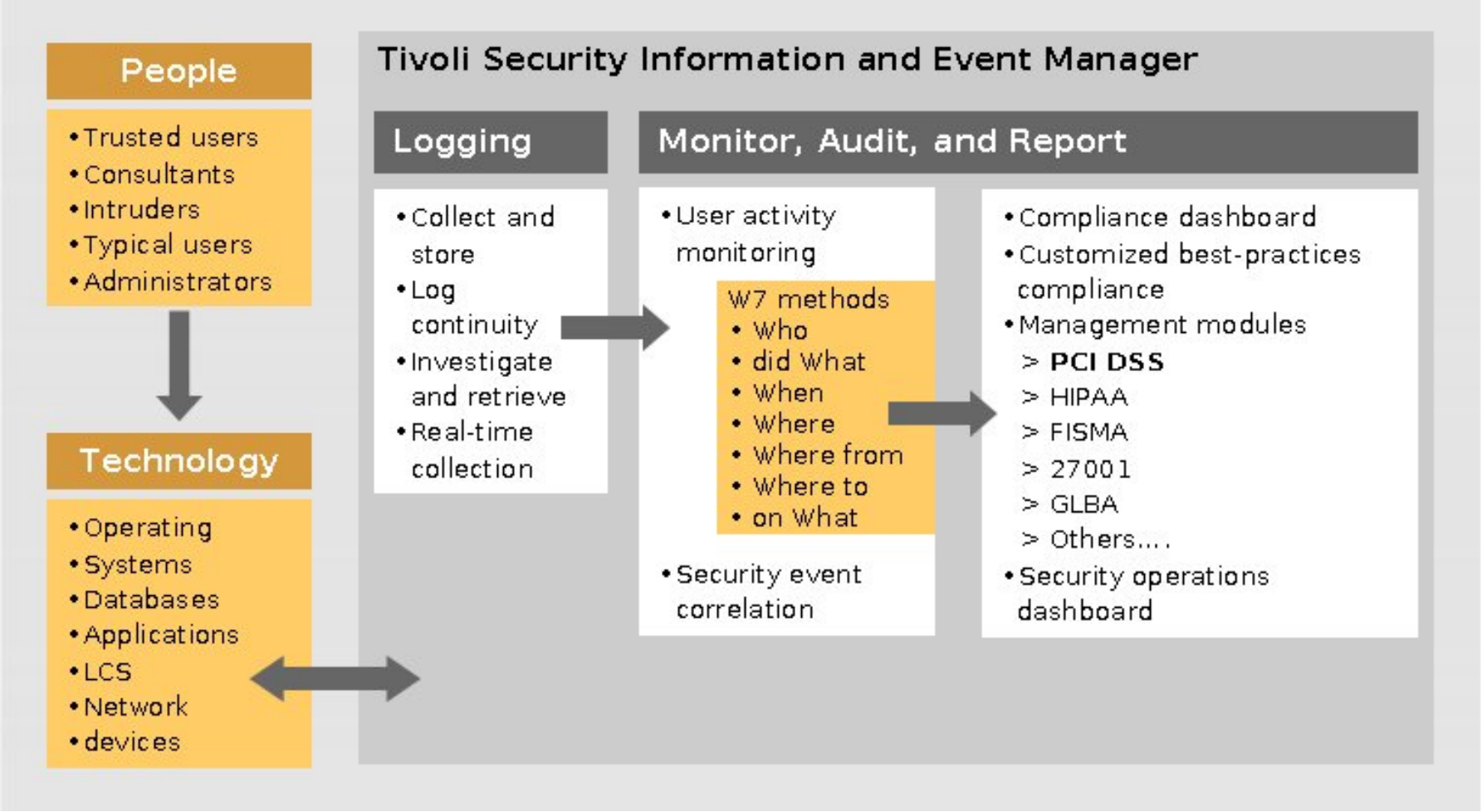
LCS PCI Challenges (11.5)

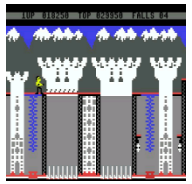
PCI DSS Rqmt	Testing Procedure
11.5 Deploy file-integrity monitoring (FIM) software to alert personnel to unauthorized modification of critical system files….	**11.5** Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files…



- PCI SSC: objective is to detect modifications to critical system files
- On LCS applies to system data sets, libraries, load modules, parmlibs (config data), and UNIX system service files (in zFS or HFS)
- Traditional FIM tools such as Tripwire or Aide do not exist on LCS.
- Audit function on z/OS can monitor all writes
- Audit system can monitor critical files during patch cycle/config chgs

System auditing, logging, events





Pitfalls: Choosing Your Assessor

- Choosing you assessor (skills and competency)
  - Do they have experience with mainframes?
  - Do they understand the additional security built in to such systems, or do they try and map it to more common paradigms?
- Conflict of Interest
  - Don’t choose assessor that tries to sell you their product, a partner’s product, or consultancy
- Transfer of Risk!
  - Your assessor assumes risk when they make statements about your systems. Are they mature enough to realize this?

Pitfalls: Snake Oil & Silver Bullets

- Unfortunately there are no
  - Silver bullets
  - Magic tools
  - Wondrous applications

Bibliography

- **PCI Security Standards Council**
  - https://www.pcisecuritystandards.org/index.shtml
- **PCI compliance for Large Computer Systems**
  - http://www.atsec.com/us/pci-lcs.html

Thank You

Thanks for your time and interest

Jeff Jilg
jeff@atsec.com
atsec information security
http://www.atsec.com
With QSA offices in Austin, TX, Germany, and China