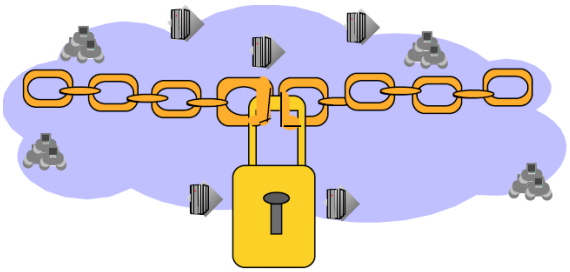
# Satisfying Selected PCI Requirements with z/OS Communications Server

# Baltimore Washington RACF Users' Group

**February 17, 2010**

**Speaker: Gwen Dente,**
**IBM Advanced Technical Skills,**
**Gaithersburg, MD**



**Consulting IT Specialist**
**z/OS Communications Server and Networking Security; Communication Controller for Linux on z; Communications Server for Linux on z**

## Abstract

- The requirements to implement the Payment Card Industry (PCI) standards in U.S. companies and institutions have reached a point at which talking about the theory and its meanings no longer suffices. It is time to take action!
- The PCI requirements need to be met ASAP by practical implementation measures. For example, how do you prove that you have met Requirement 8.1, or 8.2, or 8.3? How can you use z/OS Communications Server or other IBM products to comply with other PCI requirement mandates?
- This session reviews many of the most pressing requirements and offers the specific solution or solutions in z/OS Communications Server to satisfy each of those requirements.

## Agenda

- Why the Resurgence of Interest in Security
- What You May Already Know About Security
- What Is Payment Card Industry (PCI) Compliance About?
- Common Compliance Mistakes
- Selected Segmentation Techniques with System z
- PCI 1.2:  Step by Step with System z and System z Software
- PCI Documents
- Appendix:  References
- Appendix:  PCI Data Flow

## Security in the News and the Courts ...

**Cost of data breaches keeps rising**

**Data breaches are costing organizations an average of $197 per lost or stolen customer record, an annual study finds**

By Matt Hines
November 28, 2007

[redacted]

Attacks from Outside and Inside!

**Attacks Continue on Retail Stores, Restaurants**

**Criminals exploit wireless vulnerabilities, social engineering to collect large volumes of customer data**

Aug 18, 2008 | 09:55 AM

**Insider Tries to Steal $400 Million at DuPont**

**Unusual computer activity is tipoff in successful case against chemist who tried to steal intellectual property for his new employer**

Feb 16, 2007 | 02:10 AM

**IT Worker Indicted For Setting Malware Bomb At Fannie Mae**

**IT contractor deployed highly malicious script before his administrative rights were terminated**

Jan 29, 2009 | 05:42 PM



1. Connecticut sues Accenture over stolen backup tape
   1. Unencrypted tape contained personal information on 58 taxpayers and nearly 460 state bank accounts
   2. Illegal negligence, unauthorized use of state property, and breach of contract
   3. Seeking damages related to securing the stolen data and ordering Accenture return some of project money
2. TJ Maxx
   1. Over 45 million credit and debit card numbers stolen
   2. $8 million gift card scheme
   3. U.S. Secret Service agents found Eastern Europe thieves who created high-quality counterfeit credit cards
   4. Lawsuit filed by CT, MA, and ME banking associations
   5. Estimated costs ? $1bn over five years (not including lawsuits)
   6. $117m costs in 2Q ’07 alone
3. Sentry Insurance
   1. Employee Thomas Binyan, Software Development Consultant, needed to pay off Gambling debts. Decided to sell identity information pilfered from Sentry databases on 110,000 Sentry Customers
   2. 36,000 Names/Addresses/SS#s/birth dates for $25,000
   3. Flew to Nashville to make the deal with…..The United States Secret Service (Ooops)
   4. Sentenced to 5 Years in Jail; ordered to pay Sentry $520,000
4. Hannaford Bros. Co (Grocery Chain)
   1. Met PCI Compliance, but Dec. 2007 - March 2008 suffered breach of 4.2 million Credit Card numbers
   2. May lead to strengthening or clarification of PCI mandates or stringent controls on auditors performing the PCI assessments (QSAs - Qualified Security Assessors)
5. Regarding Hannaford: "The company said the thefts appear to have happened during the transaction-authorization stage, which occurs after a payment card has been swiped at a register. The stolen information includes card numbers and expiration dates." (Taken from an article by Jaikumar Vijayan in http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072678)
6. The fines and the reimbursement costs are not collected directly from the breached entity but through the "acquiring bank" that authorizes a company such as Hannaford to accept payment-card transactions. Under PCI rules, it is these acquiring banks that are directly responsible for ensuring that their merchants are PCI-compliant.

## Security in the News and the Courts ...

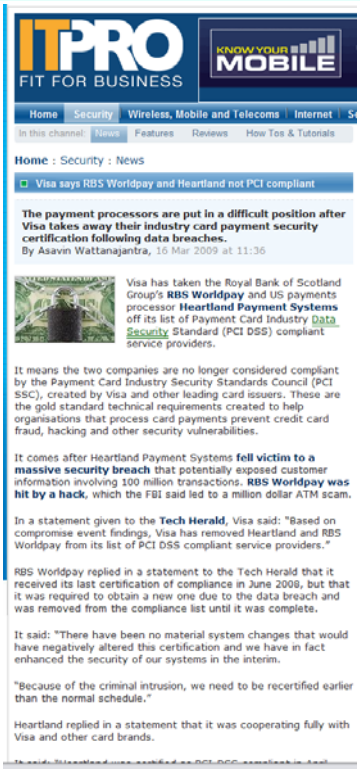
- **Connecticut sues Accenture over stolen backup tape**
  - Unencrypted tape contained personal information on 58 taxpayers and nearly 460 state bank accounts
  - Illegal negligence, unauthorized use of state property, and breach of contract
  - Seeking damages related to securing the stolen data and ordering Accenture return some of project money
- **TJ Maxx**
  - Over 45 million credit and debit card numbers stolen
    - $8 million gift card scheme
    - U.S. Secret Service agents found Eastern Europe thieves who created high-quality counterfeit credit cards
  - Lawsuit filed by CT, MA, and ME banking associations
  - Estimated costs ? $1bn over five years (not including lawsuits)
    - $117m costs in 2Q '07 alone
- **Sentry Insurance**
  - Employee Thomas Binyan, Software Development Consultant, needed to pay off Gambling debts. Decided to sell identity information pilfered from Sentry databases on 110,000 Sentry Customers
    - 36,000 Names/Addresses/SS#s/birth dates for $25,000
  - Flew to Nashville to make the deal with…..The United States Secret Service (Ooops)
  - Sentenced to 5 Years in Jail; ordered to pay Sentry $520,000
- **Hannaford Bros. Co (Grocery Chain)**
  - Met PCI Compliance, but Dec. 2007 - March 2008 suffered breach of 4.2 million Credit Card numbers
  - May lead to strengthening or clarification of PCI mandates or stringent controls on auditors performing the PCI assessments (QSAs - Qualified Security Assessors)



1. The fines and the reimbursement costs are not collected directly from the breached entity but through the "acquiring bank" that authorizes a company such as Hannaford to accept payment-card transactions. Under PCI rules, it is these acquiring banks that are directly responsible for ensuring that their merchants are PCI-compliant.
2. Regarding Hannaford: "The company said the thefts appear to have happened during the transaction-authorization stage, which occurs after a payment card has been swiped at a register. The stolen information includes card numbers and expiration dates." (Taken from an article by Jaikumar Vijayan in http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072678)

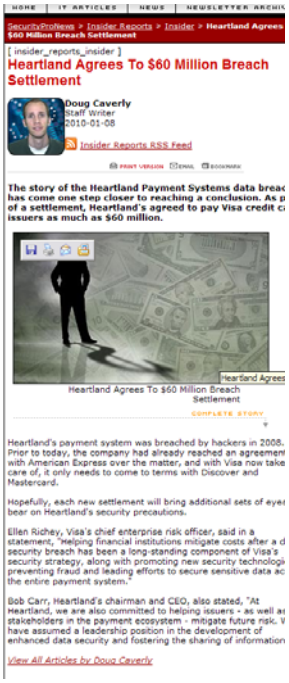
## Security in the News and the Courts ...

- **Heartland and Royal Bank of Scotland not PCI-compliant**
  - reported March 16, 2009




- **At risk:**
  - Fines
  - Reputation
  - Financial Loss (theft) from breach itself

- **Heartland settles for $60M**
  - reported Jan. 8, 2010






1. The fines and the reimbursement costs are not collected directly from the breached entity but through the "acquiring bank" that authorizes a company such as Heartland to accept payment-card transactions. Under PCI rules, it is these acquiring banks that are directly responsible for ensuring that their merchants are PCI-compliant.
2. Heartland articles from:
3. http://www.itpro.co.uk/609192/pcis-bob-russo-data-loss-hurts-brand-more-than-a-fine
4. http://www.securitypronews.com/insiderreports/insider/spn-49-20100108HeartlandAgreesTo60MillionBreachSettlement.html
5. http://www.itpro.co.uk/610190/visa-says-rbs-worldpay-and-heartland-not-pci-compliant

## Security in the News and the Courts ...




1. Connecticut sues Accenture over stolen backup tape
   1. Unencrypted tape contained personal information on 58 taxpayers and nearly 460 state bank accounts
   2. Illegal negligence, unauthorized use of state property, and breach of contract
   3. Seeking damages related to securing the stolen data and ordering Accenture return some of project money
2. TJ Maxx
   1. Over 45 million credit and debit card numbers stolen
   2. $8 million gift card scheme
   3. U.S. Secret Service agents found Eastern Europe thieves who created high-quality counterfeit credit cards
   4. Lawsuit filed by CT, MA, and ME banking associations
   5. Estimated costs ? $1bn over five years (not including lawsuits)
   6. $117m costs in 2Q '07 alone
3. Sentry Insurance
   1. Employee Thomas Binyan, Software Development Consultant, needed to pay off Gambling debts. Decided to sell identity information pilfered from Sentry databases on 110,000 Sentry Customers
   2. 36,000 Names/Addresses/SS#s/birth dates for $25,000
   3. Flew to Nashville to make the deal with…..The United States Secret Service (Ooops)
   4. Sentenced to 5 Years in Jail; ordered to pay Sentry $520,000
4. Hannaford Bros. Co (Grocery Chain)
   1. Met PCI Compliance, but Dec. 2007 - March 2008 suffered breach of 4.2 million Credit Card numbers
   2. May lead to strengthening or clarification of PCI mandates or stringent controls on auditors performing the PCI assessments (QSAs - Qualified Security Assessors)
5. Regarding Hannaford: "The company said the thefts appear to have happened during the transaction-authorization stage, which occurs after a payment card has been swiped at a register. The stolen information includes card numbers and expiration dates." (Taken from an article by Jaikumar Vijayan in http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072678)
6. The fines and the reimbursement costs are not collected directly from the breached entity but through the "acquiring bank" that authorizes a company such as Hannaford to accept payment-card transactions. Under PCI rules, it is these acquiring banks that are directly responsible for ensuring that their merchants are PCI-compliant.

## The Rush to Secure Data: The Nature of Risk

- **Data is valuable**
  - Data at Rest
  - Data in Transit, in Flight
  - Data in Use
- **Intellectual Property Theft**
  - Confidential Manufacturing Processes
  - Financial Information
  - Customer Lists
  - Digital Source Code
  - Marketing Strategies
  - Research Data
- **Economic Espionage**
  - Trade Secrets
- **Regulatory Compliance**
  - Consumer Privacy
  - Financial Integrity
- **Security costs growing 3x faster than IT budgets**

## Impact of Security Breaches

- **At Risk:**
  - Reputation
  - Economic Viability
- **Impact**
  - Economic
    - Fines
    - Lawsuits
  - Consumer confidence
    - ** 77% of 2,750 consumers polled said they would stop shopping at stores that suffer data breaches
  - Competitive advantage
    - Investors' confidence
- **Loss of business**
  - * 1/3 of companies could go out of business with a major security breach

* McAfee Survey
**Javelin Strategy & Research



1. The items listed are mentioned in the surveys indicated.
2. However, security also impacts the availability of operations and data, thus leading to the impacts listed here.

# Operational Issues Pushing IT to the Breaking Point

***Costs and Service Delivery***

- Explosion in volume of data and information
- Rising operational costs of systems and networking
- Difficulty in deploying new applications and services

***Business Resiliency and Security***

- Security of your assets and your clients' information
- Compliance requirements and government mandates
- Systems and applications need to be available

***Energy Efficiency***

- Rising energy costs and rising energy demand
- Power and thermal issues inhibit operations
- Environmental compliance and social responsibility

***Changing application models***

- Unpredictable workload characteristics
- Manage fast growth of "smart" objects and data volumes
- Need maximum flexibility for real time interaction

## Security as a Component of High Availability

1. Redundancy

2. Performance & Tuning

3. Security

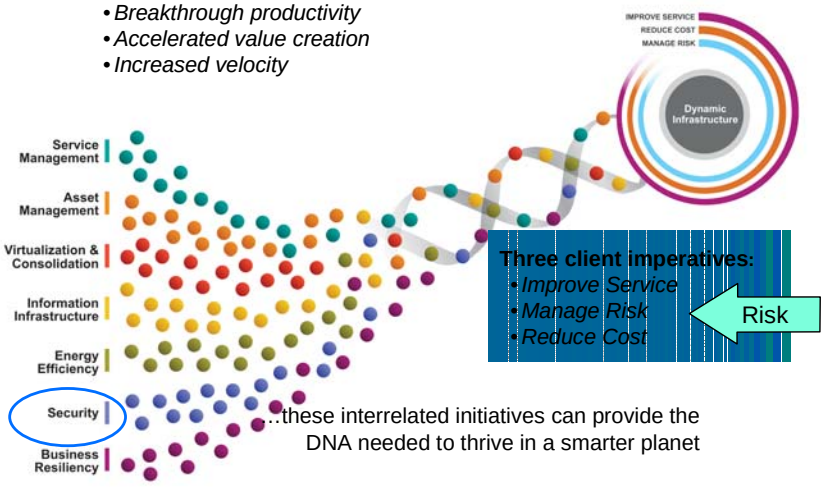


1. When organizations first started thinking about security, they often equated it to the prevention of Denial of Service attacks or to anything that would impact high availability and thus violate their Service Level Agreements (SLAs).
2. A  High Availability strategy should address at least all three of these areas:
   1. Redundancy in its many forms  (Many of these were detailed on the previous visual.)
   2. Performance and Tuning of the network and its components.
   3. Providing security to prevent violations that could restrict access to business applications and the network they reside on.

# Smarter Planet, Dynamic Infrastructure to Manage Risk

**New possibilities:**

- *Breakthrough productivity*
- *Accelerated value creation*
- *Increased velocity*




…these interrelated initiatives can provide the DNA needed to thrive in a smarter planet

# What You May Already Know About Security

## The IBM Security Framework

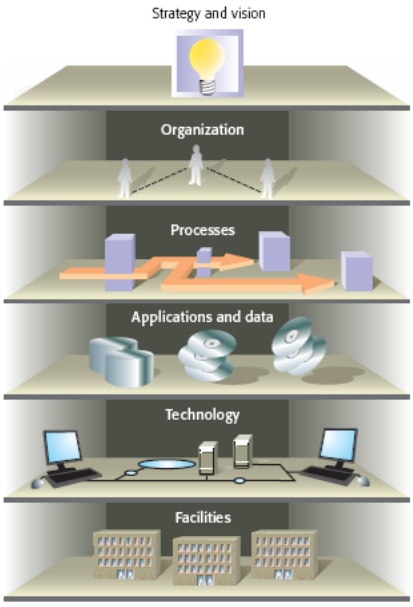

**IBM Solutions:**

- **Security Compliance**
  - Demonstrate policy enforcement aligned to regulations
- **Identity and Access**
  - Controlled and secure access to information, applications, and assets
- **Data Security**
  - Protect and secure data and assets
- **Application Security**
  - Manage, monitor, audit
- **Infrastructure Security**
  - Threat management across networks, servers, end-points



1. The IBM Security Framework provides a model for selecting, designing, and monitoring technologies to protect all aspects of an IT organization.
2. IBM provides the professional services to assess an organization's needs for security with regard to compliance mandates and general security requirements. These services can design, implement, and manage security technologies and can recommend hardware and software solutions for an organizaiton.

## IBM Business Resilience Framework and Security




### Strategy and Vision:
- Day to day activities for continuous operation.

### Organization
- Communication channels, skills of people, training

### Processes
- Accounts receivable and payable, Change management, incident management

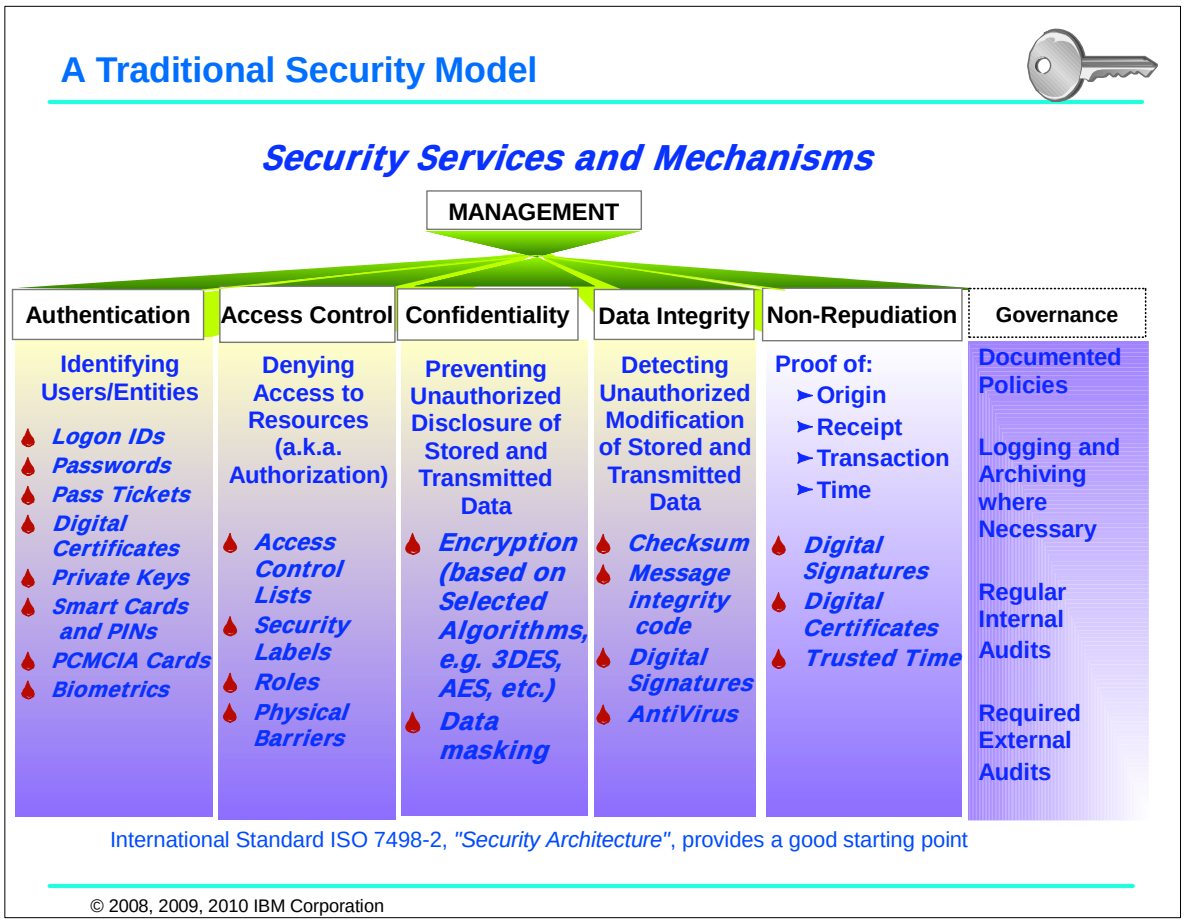
### Applications and data
- Customer relationship management, enterprise resource management, database and transaction processing applications

### Technology
- Hardware, software, networking protocols

### Facilities
- Physical plant



1. Compare this depiction of IBM's "business resilience strategy" with "IBM's Security Framework," which was described on the previous page.
2. Note how the five levels to deal with are the same in each strategy, thus once again pointing out the interrelationship between security and high availability.
3. Strategy and vision—relates to the strategies used by the business to complete day-to-day activities to achieve continuous operations. Examples include compliance, governance, availability, continuity, and security strategies.
4. Organization—relates to organizational structure, communication channels, and people skills and responsibilities. Examples include human resources, training, and internal and external communications.
5. Processes—relates to the critical business processes necessary to run the business, as well as the supporting IT processes. Examples include accounts receivable, accounts payable, incident management, and change management.
6. Applications and data—examples include customer relationship management (CRM) applications, enterprise resource planning (ERP) applications, and database and transaction-processing applications.
7. Technology—relates to the systems, network, and industry-specific technology necessary to enable the business applications and data. Examples include host systems, workstations, and Internet Protocol (IP) networks.
8. Facilities—relates to the buildings, factories, or offices necessary to house the business production or service infrastructure and the staff. Examples include data centers, office buildings, and physical security operations.

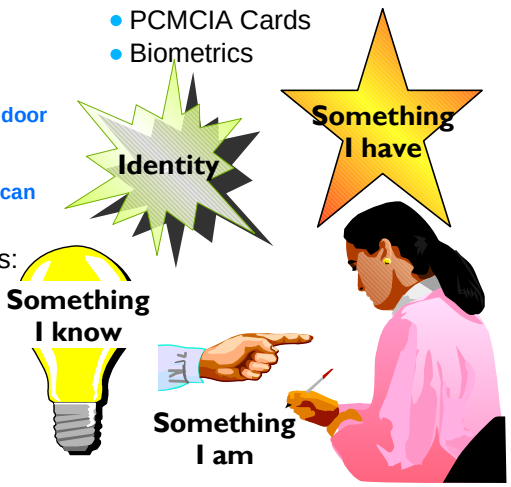



1. This is an older version of the ISO security model. Note the entry for "Governance" and "Logging." This is not part of the ISO model, but it is nevertheless integral for any security implementation. We have added it here to show its importance.

## What is Authentication?

- **Authentication**
  - Identifying Users/Entities
  - Who and What needs to be verified?
- **Policies for Authentication**
  - Who designs and administers them?
- **Two-factor Authentication**
  - Two validation methods from following three methods:
    - Something I know:
      - **Password, PIN, mother's maiden name, or birthdate, etc.**
    - Something I have
      - **Digital Certificate, eID Card, Identity Card, or door key, etc.**
    - Something I am
      - **Fingerprint, Facial Scan, Body Scan, or Iris Scan**
- **Two-level Authentication**
  - Two of the same type of validation methods:
    - Something I know:
      - **Password and PIN**
    - Something I have:
      - **Digital Certificate and e-ID Card**
    - Something I am:
      - **Thumbprint and Iris or Retina Scan**

- **Mechanisms to use**
  - Logon IDs
  - Passwords
  - Pass Tickets
  - Digital Certificates
  - Private Keys
  - Smart Cards and PINs
    - e-ID Cards in Europe
  - PCMCIA Cards
  - Biometrics



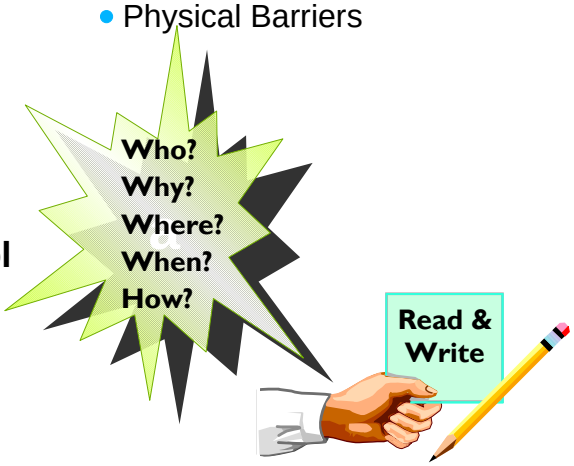



- Most points within data flow allow represented by standard or product function will allow some form of authentication.
- The authentication may be specific or generic.

## What is Access Control?

- **Access Control**
  - Permitting and Denying Access to Resources (a.k.a. Authorization)
    - Who can access
    - What form access (How?)
      - What function is allowed
    - From where can they access?
    - Under what conditions?
      - Time, manner, place
    - From which Hardware
    - From which Software
- **Policies for Access Control**
  - Who designs and administers the policies?

- **Mechanisms**
  - Access Control Lists
  - Security Labels
  - Roles
  - Biometrics
  - Physical Barriers






- Stretch your mind when looking for access control. Go beyond the traditional access control structure. What controls exist? Port, filters, etc.

## What is Confidentiality?

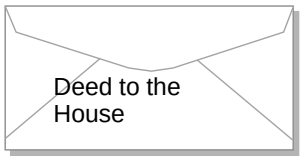
- **Confidentiality**
  - Preventing Unauthorized Disclosure of Stored and Transmitted Data
  - What needs to be concealed from whom?
- **Policies for Confidentiality**
  - What are the policies to protect Data at Rest and Data in Transit?
  - Who designs and administers the policies?
- **Mechanisms**
  - Cryptography on Hardware
  - Encryption (based on Selected Algorithms, e.g. 3DES, AES, etc.)
  - Data masking




- Confidentiality and data integrity are both included in many configurations for standards-based interfaces, such as, HTTP, FTP, Kerberos, LDAP. Additionally, user-written applications may also require or need to require privacy and integrity above what is provided by system components.

## What is Data Integrity?

- **Data Integrity**
  - Detecting Unauthorized Modification of Stored and Transmitted Data
- **Policies for Data Integrity**
  - What are the policies to protect Data at Rest and Data in Transit?
  - Who designs and administers the policies?
- **Mechanisms**
  - Cryptography
  - Checksum
  - Message integrity code
  - Digital Signatures
  - AntiVirus





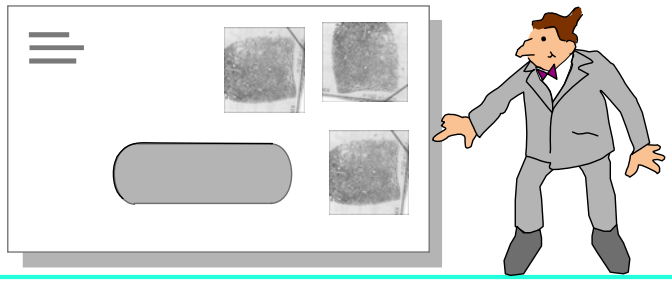


- Confidentiality and data integrity are both included in many configurations for standards-based interfaces, such as, HTTP, FTP, Kerberos, LDAP. Additionally, user-written applications may also require or need to require privacy and integrity above what is provided by system components.

## What is Non-Repudiation?

- **Non-Repudiation**
  - Proof of:
    - Origin
    - Receipt
    - Transaction
    - Time
- **Policies for Non-Repudiation**
  - Who determines the policies for non-repudiation?
- **Mechanisms**
  - Digital Signatures
    - Signature created using Private Key and verified with Public Key
  - Digital Certificates
    - Provides assurance that public key belongs to person or entity that is supposed to be the owner.
  - Trusted Time

I know that you have seen this envelope!
Your fingerprints are all over it!





1. For non-repudiation you must be careful to understand the intent of the security to be provided and that the function performed either by the application or product interface provides the security to the full extent required.

2. If something is crucial to be presented by a specific time, is the system time adjusted for different time zones or is a management/legal caveat required?
3. If something is only to be accepted from a specific origin, how do you know that the origin has not changed due to firewall setup, etc.?

## What is Governance?

- **Governance**
  - Governance relates to decisions that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes.
  - For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data.
- **Mechanisms**
  - Written Policies
  - Auditing of Policy Compliance
  - Logging
  - Reporting
    - Security
    - Performance
    - etc.
  - Monitoring
  - Assessing

# What Is Payment Card Industry (PCI) Compliance About?

## What is the Payment Card Industry?

Payment Card Industry (PCI) Security Standards Council (SSC)
Founders and Members of the Executive Committee:

- *PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.*
- *The standards globally govern all merchants and organizations that store, process or transmit this data – with new requirements for software developers and manufacturers of applications and devices used in those transactions.*
- *Compliance with the PCI set of standards is mandatory for their respective stakeholders, and is enforced by the major payment card brands who established the Council:*
  - *American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.*
- *Participating Organizations: Merchants, banks, processors, developers and point of sale vendors*

## Applicability of PCI DSS Requirements: Environment

- **PCI DSS requirements apply to all system components that are included in or connected to the ***cardholder data environment*.**
  - The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including network components, servers and applications.
    - Network components may include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
    - Server types may include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
    - Applications may include but not limited to all purchased and custom applications, including internal and external (Internet) applications.
- ***Adequate network segmentation*, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.**
  - A Qualified Security Assessor (QSA) can assist in determining scope within an entity's cardholder data environment along with providing guidance about how to *narrow the scope of a PCI DSS assessment* by implementing proper network segmentation.

**Reference PCI DSS V1.2:**
https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-2.pdf

## Applicability of PCI DSS: "cardholder data"Yes

| | Data Element | Storage Permitted | Protection Required | PCI DSS Req. 3.4 |
|---|---|---|---|---|
| Cardholder Data | Primary Account Number (PAN) | Yes | Yes | Yes |
| | Cardholder Name[1] | Yes | Yes[1] | No |
| | Service Code[1] | Yes | Yes[1] | No |
| | Expiration Date[1] | Yes | Yes[1] | No |
| Sensitive Authentication Data[2] | Full Magnetic Stripe Data[3] | No | N/A | N/A |
| | CAV2/CVC2/CVV2/CID | No | N/A | N/A |
| | PIN/PIN Block | No | N/A | N/A |

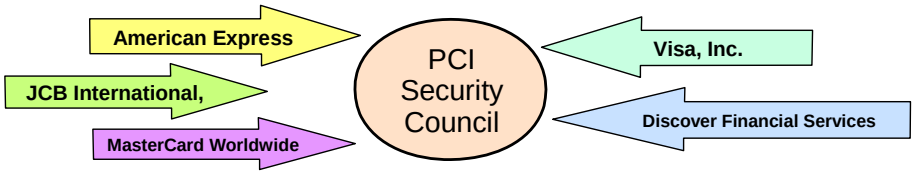
- **Cardholder data is defined as the primary account number ("PAN,"¨ or credit card number) and other data obtained as part of a payment transaction, including the following data elements (see more detail below in the table):**
  - PAN
  - Cardholder Name
  - Expiration Date
  - Service Code
  - Sensitive Authentication Data: (1) full magnetic stripe data, (2) CAV2/CVC2/CVV2/CID, and (3) PINs/PIN blocks)
- **The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply.**

**Reference PCI DSS V1.2:**
https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-2.pdf



1. *These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.
2. ** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

## Payment Card Industry (PCI) Data Security Standard 1.2 ("Just another security model")




**Build and maintain a secure network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

**Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure applications and systems.

**Implement strong access control measures**

Requirement 7: Restrict access to cardholder data by business need-to-know.

*Requirement 8:* Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

**Regularly Monitor and Test Network**

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

**Maintain an Information Security Policy**

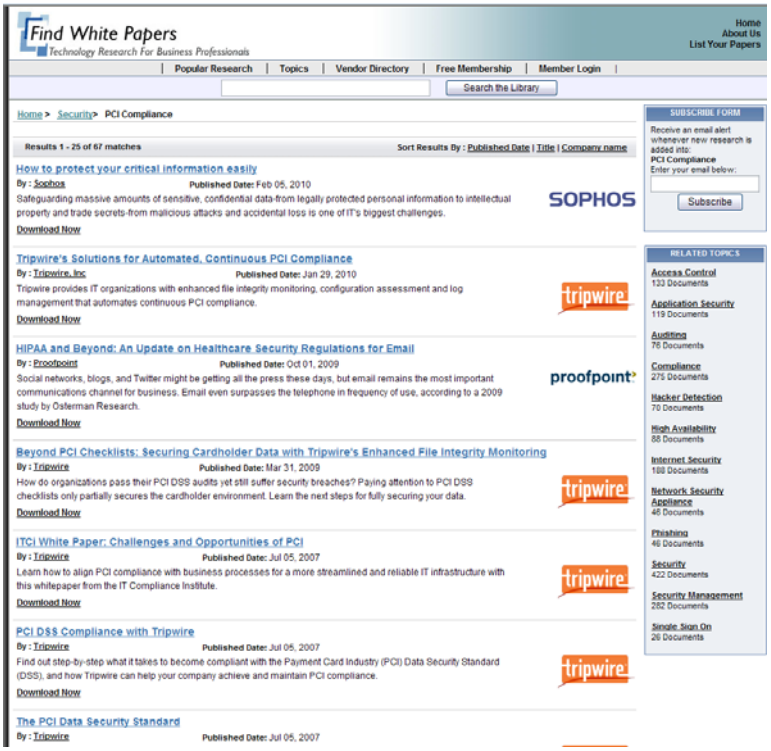
Requirement 12: Maintain a policy that addresses information security.



- The PCI council has its own version of a security model, which you see here.
- As of January 1, 2009, PCI Standard 1.2 is in effect. Any new assessments started as of this date must comply with the forms and regulations provided with 1.2. Any assessments begun before January 1, 2009 may continue to use the older 1.1 forms unless the card brand decides otherwise. V1.2 is a further clarification of 1.1.
- The following description of the Council that was formed to create these standards is taken from URL: https://www.pcisecuritystandards.org/
  1. "The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection."
  2. "The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc."
- The Payment Card Industry standards provide a structure for assessing security in an IT installation. Most of the bullets in the PCI-DSS reflect line items in any of the other security architectures with which you are familiar.
- Although the structure provided by PCI DSS was built to secure credit card data, in fact, the same structure can apply to many other standards, like those demanded by NIST, for example.
- The following paragraphs are quoted from the PCI Standards Council web page at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
  1. "The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.
  2. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
  3. The PCI DSS January 2005 version has been enhanced in the PCI DSS Version 1.1. The PCI DSS January 2005 version may no longer be used for PCI DSS compliance validation after December 31, 2006.
  4. The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.
  5. Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.
  6. The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized: ...."
- These are six principles and 12 requirements (called "the dirty dozen" or "the digital dozen" ) in the PCI DSS 1.1 standards, as you see on this page above.
- You may find many articles on the PCI standards by performing a search on the web.

# Common Compliance Mistakes

## Search the Web for White Papers and PCI Experiences






1. This page is at: http://www.findwhitepapers.com/index.php?option=com_categoryreport&task=viewlist&id=17&cat=310&srcid=2008&gclid=CPTI_vzw5Z8CFZhb2godElnVGQ
2. A general search of the web provices a list of valuable information, including a pointer to a book on "PCI for Dummies," and many news articles.

## Top 10 Audit Failures by Rank*

| Rank | PCI Requirement* | Audit Failure Percentage |
|---|---|---|
| 1 | **Requirement 11:** Regular testing | 48% |
| 2 | **Requirement 6:** Secure applications | 45% |
| 3 | **Requirement 3:** Protect data | 45% |
| 4 | **Requirement 8:** Unique user ID | 42% |
| 5 | **Requirement 10:** Track access | 40% |
| 6 | **Requirement 12:** Security policy | 38% |
| 7 | **Requirement 1:** Maintain firewall | 37% |
| 8 | **Requirement 2:** Avoid program defaults | 37% |
| 9 | **Requirement 9:** Restrict physical access | 37% |
| 10 | **Requirement 4:** Encrypt transmitted data | 27% |

**For more detail on the requirements, please see www.pcisecuritystandards.org.

* From the Verisign White Paper "More Lessons Learned -- Practical Tips for Avoiding Payment Card Industry (PCI) Audit Failure" available at www.verisign.com.

## Prerequisite: Understand the Flow of PCI Data

**BIggest Obstacles to Successfully Completing a PCI Assessment:**

- **Lack of knowledge where all the data is at rest**
- **Lack of knowledge of all processes that touch PCI data**

1. ***What is the normal data flow?***
2. ***What is the data flow when something goes wrong (typically lack of connectivity)?***
3. ***How many log files are there?***
4. ***What is stored in the log files?***
5. ***Where are the log files stored?***
6. ***How often are they backed-up?***
7. ***Where are the back-ups located?***
8. ***Is the 3rd party location secured to PCI standards?***
9. ***Are there printouts that need securing (e.g. payment receipt)?***

See Appendix with PCI Data Flow Diagrams.

## PCI and Network Segmentation (PCI DSS 1.2)

### *Network Segmentation*

- Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement.
- However, it is recommended as a method that may reduce:
  - The scope of the PCI DSS assessment
  - The cost of the PCI DSS assessment
  - The cost and difficulty of implementing and maintaining PCI DSS controls
  - The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)
- ***Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.***
- Network segmentation can be achieved through
  - internal network firewalls,
  - routers with strong access control lists or
  - other technology that restricts access to a particular segment of a network.

## PCI and Network Segmentation (PCI DSS 1.2)

- **Prerequisite to reduce the scope of the cardholder data environment:**
  - understanding of business needs and processes related to the
    - storage,
    - processing or
    - transmission of cardholder data.
- **Restrict cardholder data to as few locations as possible**
  - eliminate unnecessary data, and
  - consolidate necessary data,
- **Worst Case: reengineer business practices**
- **Aid to Understanding Scope:**
  - Documenting cardholder data flows via a dataflow diagram
- **Have you correctly isolated the data environment?**
  - The QSA (or internal auditor) decides
- **However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as**
  - a given network's configuration,
  - the technologies deployed, and
  - other controls that may be implemented.
- **Appendix F: PCI DSS Reviews - Scoping and Selecting Samples provides more information on the effect of scoping during a PCI DSS assessment.**

## Verisign Hints and Tips

- **Store less data**
  - Justify the storage of credit card data

http://www.verisign.com/static/PCI_REASONS.pdf

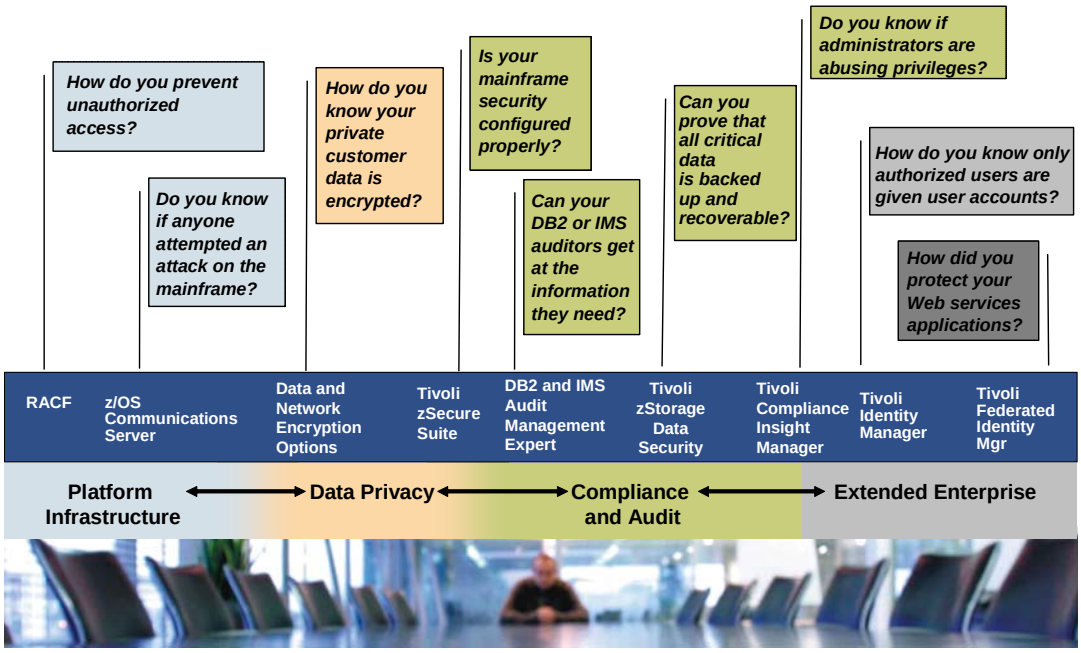
- **Understand the flow of data**
  - Document the flow of credit card data throughout your organization
- **Encrypt Data**
  - Incorporate encryption at the development phase
  - Have an overall encryption strategy
- **Address Applications and Network Vulnerabilities**
  - Update POS Systems
  - Update your software with patches as they are released
  - Identify Poorly Coded Web Applications
  - Have a third party conduct an application test and code review
  - Scan Quarterly for application and systems vulnerabilities
  - Perform quarterly scans
  - Implement strict Software / System Development Life Cycle (SDLC) Processes
  - Avoid ad hoc development, implement replicable processes, and document everything
- **Improve Security Awareness and Training**
  - Continually educate and train internal staff'; develop processes that ensure adherence to security procedures and policies
- **Monitor Systems for Intrusions and Anomalies**
  - Allow IDS Devices to Accumulate Sufficient Intelligence
  - Place IDS devices near the assets you want to protect
  - Establish a centralized server
  - Improve Log Monitoring and Retention
  - Centralize Logs and use active correlation
  - Hold people accountable for monitoring logs
  - Watch the applications
- **Segment Credit Card Networks and Control access to them**



1. From VeriSign: Whitepaper; Lessons Learned: top Reasons for PCI Audit Failures and how to avoid them
2. http://www.verisign.com/static/PCI_REASONS.pdf
3. From Wikipedia, the meaning of "SDLC":
4. "SDLC, the Software Development Life Cycle relates to models or methodologies that people use to develop systems, generally computer systems. Note: the acronym is sometimes thought of to represent Software Development Life Cycle and sometimes the process/model is simply referred to as the SLC. Computer systems have become more complex and usually (especially with the advent of Service-Oriented Architecture) link multiple traditional systems often supplied by different software vendors.
5. To manage this, a number of system development life cycle (SDLC) models have been created: waterfall, fountain, spiral, build and fix, rapid prototyping, incremental, and synchronize and stabilize.
6. SDLC adheres to important phases that are essential for developers, such as planning, analysis, design, and implementation, and are better explain in the section below. The oldest model, that was originally regarded as "the SDLC" is the waterfall model: a sequence of stages in which the output of each stage becomes the input for the next. These stages generally follow the same basic steps but many different waterfall methodologies give the steps different names and the number of steps seems to vary between 4 and 7.

# The PCI Audit: IBM Tivoli Perspective

## Questions auditors might ask:




*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

# Selected PCI Segmentation Techniques with System z

## PCI and Network Segmentation (PCI DSS 1.2)

### *Network Segmentation*

- Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement.
- However, it is recommended as a method that may reduce:
  - The scope of the PCI DSS assessment
  - The cost of the PCI DSS assessment
  - The cost and difficulty of implementing and maintaining PCI DSS controls
  - The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)
- ***Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.***
- Network segmentation can be achieved through
  - internal network firewalls,
  - routers with strong access control lists or
  - other technology that restricts access to a particular segment of a network.

## Lists of System z and z/OS Segmentation Techniques

- **Separate Physical IP (Sub)nets**
- **Concealing Networks**
  - OSPF: concealing a range behind an Area Border router
  - OSPF: "Ignore undefined interfaces" in order to restrict link state / route advertisements
  - EIGRP: selective redistribution of network addresses
- **Separate Network Adapters (OSA Ports) -- i.e., no Sharing**
- **"Isolate" path through a shared OSA port**
- **Separate MACs on OSA Ports for routers to direct traffic to**
- **Separate Virtual LANs (VLANs)**
- **OSA Express Connection Isolation (z/OS V1R11)**
- **Separate TCP/IP stacks**
- **Separate IP Addresses (incl. VIPA)**
  - Bound to Server or to Client (Investigate Source IP Address Options)
- **Separate IP Ports (Can even combine with PORTACCESS)**
  - RESTRICTLOWPORTS
  - RESERVED PORTS
    - PORT RESERVED [DENY]
    - PORT UNRSV
- **Separate LPARs (Common Criteria Evaluation Assurance Level 5 (EAL5))**
- **Stack-Affinity Servers -- i.e., Servers are reached through 1 TCP/IP stack**
- **Bind-Specific Servers -- i.e., Servers are reached through 1 IP address**



1. Please reference other presentations at SHARE on:
   1. OSA implementation
   2. Routing Protocols
   3. z/OS CS Security Features
   4. Application Security Features

## Lists of System z and z/OS Segmentation Techniques ...

- NETACCESS (Secure Zones) -- Internal z/OS IP Controls to limit external networks that are allowed to access the TCP/IP stack
- PORTACCESS -- Internal z/OS IP Controls to limit address space, application (server), and userid access to certain application ports
- Subplexes within the SYSPLEX -- i.e., which VTAMs and TCP/IP stacks can access parts of the XCF Connections in a Sysplex
- IP Filtering -- Permit or Deny access to TCP/IP ports and addresses
- IPSec -- Establish a Virtual Private Network (VPN) to provide authentication, data integrity checking, and encryption between security endpoints of a network
- SSL/TLS -- -- Establish a secured TCP connectioin to provide authentication, data integrity checking, and encryption between Clients and Servers in a network

## Lists of System z and z/OS Segmentation Techniques ...

- **Network Address Translation -- Conceal IP Addresses in the secure zone from users outside the secure zone of a network**
- **Application segmentation techniques**
  - Examples for TN3270
    - Mapping Controls; Allow/Restrictappl; LU naming exit; Separate Address Spaces
- **Application access:**
  - Session Monitor
  - Access Control List
  - FTP
    - APPL class with FTP
    - User Exits
- **SYSLOGD Isolation - Separate Logs per Server, not just for Type of Server**
- **Centralizing Security information in a Secure Zone**
- **DMZ (Demilitarized Zone)**
- **And Many More ...**

# PCI 1.2: Step by Step with System z and System z Software

## PCI DSS 1.2: Build and Maintain a Secure Network (1)

***Requirement 1: Install and maintain a firewall configuration to protect data***

- **1.1 Firewall – Protect from unauthorized access from the internet**
  - Hipersockets – No network connections between firewall and back-end processing
  - Intrusion Detection Services (z/OS Comm Server)
  - IP Filtering - (z/OS Comm Server)
  - IBM Proventia Intrusion Prevention System Appliance (IPS)
- **1.2 Build configuration that denies all traffic from "untrusted" networks and hosts**
  - z/OS Network Policy Agent – IP packet filtering (z/OS Comm Server)
    - Self-protects server by blocking unwanted traffic
  - z/OS NETACCESS using RACF SERVAUTH class (z/OS Comm Server)
    - Disallows traffic to "untrusted" networks/hosts based on defined "security zones"
- **1.3 Build configuration that restricts connections between publicly accessible servers and any system component storing cardholder data.**
  - Implement DMZ
  - Provide network segmentation with VMAC, VLAN, OSA Express Connection Isolation, or hidden OSPF network segments
  - z/OS Network Policy Agent – IP packet filtering - (z/OS Comm Server)
    - Self-protects server by blocking unwanted connections
  - z/OS NETACCESS using RACF SERVAUTH class (z/OS CommServer)
    - Disallows traffic to "untrusted" networks/hosts based on defined "security zones"

## PCI DSS 1.2: Build and Maintain a Secure Network (2)

***Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters***

- **2.2 Develop configuration standards for all system components.**
  - z/OS Network Policy Agent (z/OS Comm Server)
  - Consistent system-wide policy for network security functions
  - System HealthChecker built in z/OS to check system configurations for best practices in security
  - Implement RACF zSecure functions
- **2.2.1 Implement only one primary function per server**
  - System z design points for multiprocessing and system integrity
  - LPARs at EAL5
  - Address Space isolation
  - Storage Protect Keys
  - Hardware Cryptography
  - Integrity Statement
  - RACF and Application Access control and auditing features
  - Segment traffic with IPSec, bind-specific VIPAs
  - IBM Tivoli Access Manager
  - IBM Proventia Network Multi-Function Security
- **2.3 Encrypt all non-console administrative access**
  - System z network encryption options
    - SSL-TLS, OpenSSH, IPSec (z/OS, Linux on z, z/VM, ISVs)

## PCI DSS 1.2: Protect Cardholder Data (3, 4)

***Requirement 3: Protect Stored Cardholder Data***

- **3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs)**
  - IBM z/OS Encryption Facility (Disk and Tape)
  - IBM Encrypting Tape Drives
  - IMS and DB2 Encryption Tool
  - OPTIM Data Privacy Masking
- **3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:**
  - IBM RACF
  - IBM System z Crypto Cards

***Requirement 4: Encrypt transmission of cardholder data across open, public networks***

- **4.1 Use strong cryptography and security protocols such as SSL, TLS and IPSEC**
  - System z network encryption options
    - SSL, TLS, OpenSSH, IPSec (z/OS, Linux, z/VM, ISVs)
  - System z features:
    - Specialty engine (zIIP) support for IPsec
    - SSL handshake acceleration with Crypto Express2
    - Encryption acceleration in general purpose processors
    - Encryption Facility (controlled decryption for file transfers)
  - DataPower XML Security Gateway
  - Proventia Network Intrusion Prevention System (outboard and on System z Linux)

## PCI DSS 1.2: Vulnerability Management (5, 6)

***Requirement 5: Use and regularly update anti-virus software or programs***

- **5.2 Ensure that all anti-virus mechanisms are current ... And capable of generating audit logs**
  - z/OS Intrusion Detection Services
    - Self-protects z/OS; Complementary to network based IDSs (not stateful)
  - IBM Proventia Desktop Endpoint Security
  - IBM Proventia Network Enterprise Scanner
  - IBM SMP/E maintenance on z

***Requirement 6: Develop and maintain secure systems and applications***

- **6.1 Ensure that all system components ... have the latest vendor-supplied security patches installed.**
  - Install/maintenance procedures for Microcode Levels of OSA Network Adapters
- **6.2 Establish a process to identify newly discovered security vulnerabilities ...**
  - Reviewing PSP Buckets for z/OS and its Components; install, maintain with SMP/E
  - IBM Rational AppScan to discover code vulnerabilities
- **6.3.2 Separate development/test & production environments**
  - RACF Access controls
  - Network Segmentation: VLANs, VMACs, etc.
- **6.3.4 Production data not used in testing or development**
  - OPTIM Test Data Creation

## PCI DSS 1.2: Strong Access Control (7)

***Requirement 7: Restrict access to cardholder data by business need-to-know***

- **7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.**
- **7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.**
  - IBM z/OS RACF or other Security Access Facility (SAF) product
  - IBM Tivoli Access Manager
  - IBM Tivoli zSecure Admin
  - IBM Tivoli Compliance Insight Manager
  - MultiLevel Security (MLS) for more advanced "compartmentalized" requirements
  - Deploy z/OS Communications Server NETACCESS, PORTACCESS, STACKACCESS to protect network security zones
  - Control access to z/OS CS commands with SERVAUTH mechanisms
  - IPSec Implementations to deny all unless specifically permitted
  - IDS with Traffic Regulation rules to limit access to specific percentages
  - Application security controls, including Access Control Lists
  - Use of Client Security Certificates to authorize specific clients

## PCI DSS 1.2: Strong Access Control (8, 9)

***Requirement 8: Assign a unique ID to each person with computer access.***

- **8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties.**
  - x.509 Digital certificate with Client Authentication, plus
  - Application with Userid and Password
- **8.4 Encrypt all passwords during transmission ....**
  - Use SSL/TLS (AT-TLS), IPSec, and/or OpenSSH to encrypt userid and pasword
- **8.5 Ensure proper user authentication and password management**
  - IBM z/OS RACF or other SAF product
  - IBM Tivoli Identity Manager
  - IBM Tivoli Federated Identity Manager
  - Digital Certificate services (PKI Services producing x.509 Security Certificates)
  - Use Policy Agent with AT-TLS that interfaces with a Certificate Revocation List application.

***Requirement 9: Restrict physical access to cardholder data***

- **9.1 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.**
  - Encrypt data end-to-end to remote printers (IPSec connections)
  - IBM Digital Video Surveillance
  - IBM Biometric Access Control

## PCI DSS 1.2: Monitor and Test Networks (10)

***Requirement 10: Track and monitor all access to network resources and cardholder data***

- **Audit records that are centralized, protected, isolated with audit trail with highly detailed information**
  - Implement RACF zSecure functions
  - z/OS CS TN3270 (SMF records)
  - z/OS CS FTP (SMF records)
  - Other z/OS CS Applications
  - SAF log audits; SYSLOGD audits; Policy Agent TRMD Reporting for IDS and IPSec
  - z/OS Communications Server SYSLOGD isolation
  - IBM OPTIM DataBase Archiving
  - IBM Tivoli Compliance Insight Manager
  - IBM Tivoli Security Operations Manager
  - IBM Proventia Server IPS

# PCI DSS 1.2: Monitor and Test Networks (11)

***Requirement 11: Regularly test security systems and processes***

- **Scans and Penetration Testing**
  - IBM Integrated Internet Security Services (ISS) (Approved Scanning Vendor - ASV)
  - z/OS Communications Server IDS reporting and notification
  - Tivoli Security Compliance Manager
  - IBM Proventia Network Anomaly Detection System (ADS)
  - IBM Global Services
  - IBM Rational AppScan
  - IBM OPTIM Test Data Creation

## PCI DSS 1.2: Information Security Policy

*Requirement 12: Maintain a policy that addresses information security for employees and contractors*

- **Implement RACF zSecure functions**
- **z/OS Network Policy Agent (z/OS Communications Server)**
  - Provides consistent system-wide policy for network security functions
- **IBM Global Services**
- **Tivoli Console Insight Manager**
- **IBM Lab Services**

# PCI Documentation

## The Main PCI Standards Document


In V1.2 this document includes what were separate documents in V1.1: the Audit guide and the PCI Standard itself.

## The PCI Self-Assessment Questionnaire


- "Please consult your acquirer or payment brand for details regarding PCI DSS validation requirements."



1. Quoted from the "Instructions and Guidelines" for completing the PCI DSS Self-Assessment Questionnaire (SAQ):
2. "The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are multiple versions of the PCI DSS SAQ to meet various scenarios. This document has been developed to help organizations determine which SAQ best applies to them.
3. The PCI DSS SAQ is a validation tool for merchants and service providers not required to undergo an onsite data security assessment per the PCI DSS Security Assessment Procedures, and may be required by your acquirer or payment brand.
4. Please consult your acquirer or payment brand for details regarding PCI DSS validation requirements.
5. The PCI DSS SAQ consists of the following components:
    1. 1. Questions correlating to the PCI DSS requirements, appropriate for service providers and merchants: See “Selecting the SAQ and Attestation that Best Apply to Your Organization” in this document.
    2. 2. Attestation of Compliance: The Attestation is your certification that you are eligible to perform and have performed the appropriate Self-Assessment."

# Appendix: References

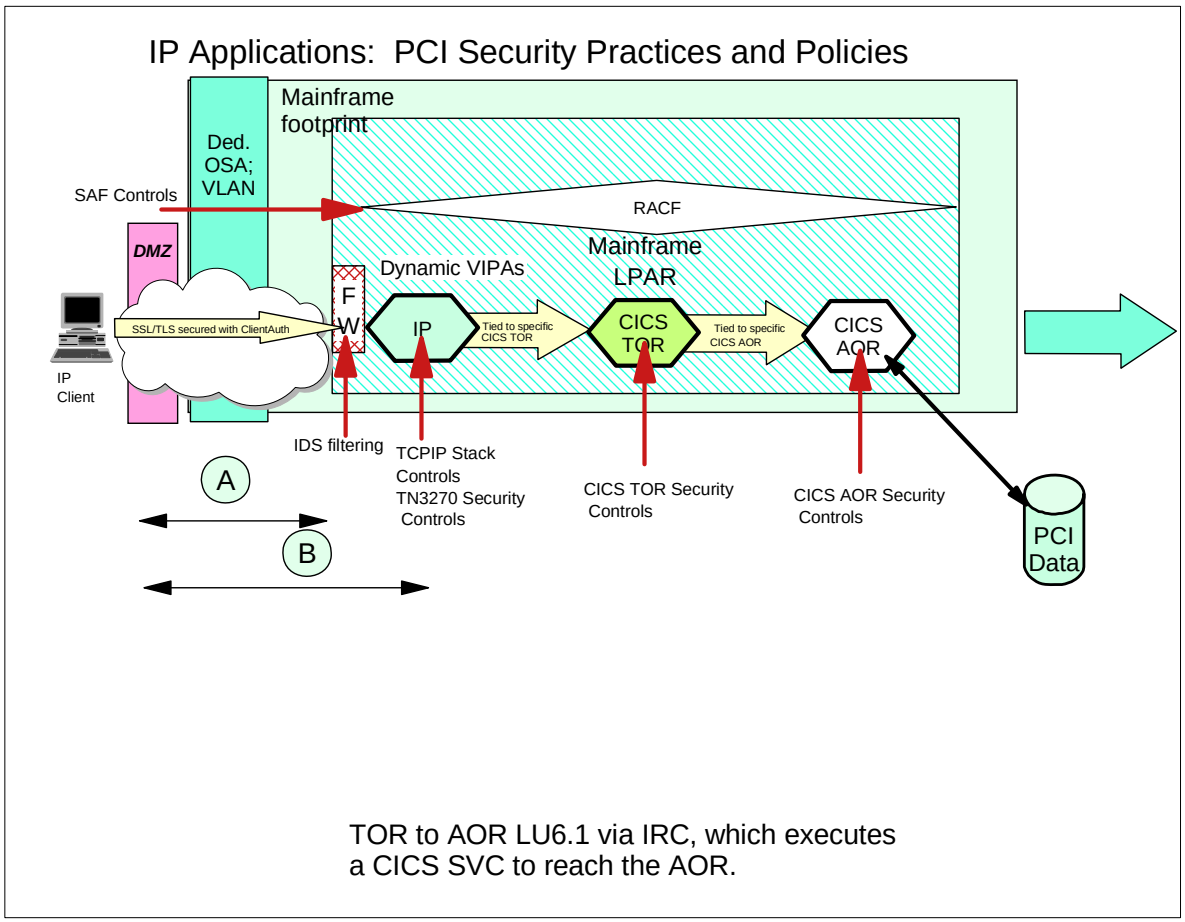
## Security References

- **https://www.pcisecuritystandards.org/**
  - PCI Documentation -- "how to"
- **http://www.iss.net/**
  - Security Consulting Services with IBM
  - Marketing of Proventia appliances for security outside the mainframe
- **http://www.ibm.com/software/network/commserver/zos/services/**
  - LAB Services out of Raleigh for Consulting and Implementation of z/OS Communications Server
- **http://www.ibm.com/servers/eserver/zseries/zos/security**
- **http://www.ibm.com/systems/z/security/**
- **http://www.ibm.com/software/network/commserver/zos/**

# Websites for IBM CS Publications, Whitepapers, etc.

| URL | Content |
|---|---|
| http://www.ibm.com/servers/eserver/zseries | IBM eServer zSeries Mainframe Servers |
| http://www.ibm.com/servers/eserver/zseries/networking | Networking: IBM zSeries Servers |
| http://www.ibm.com/servers/eserver/zseries/networking/technology.html | IBM Enterprise Servers: Networking Technologies |
| http://www.ibm.com/software/network/commserver | Communications Server product overview |
| http://www.ibm.com/software/network/commserver/zos/ | z/OS Communications Server |
| http://www.ibm.com/software/network/commserver/z_lin/ | Communications Server for Linux on zSeries |
| http://www.ibm.com/software/network/ccl | Communication Controller for Linux on zSeries |
| http://www.ibm.com/software/network/commserver/library | Communications Server products - white papers, product documentation, etc. |
| http://www.redbooks.ibm.com | ITSO redbooks |
| http://www.ibm.com/software/network/commserver/support | Communications Server technical Support |
| http://www.ibm.com/support/techdocs/ | Technical support documentation (techdocs, flashes, presentations, white papers, etc.) |
| http://www.rfc-editor.org/rfcsearch.html | Request For Comments (RFC) |

# Appendix:
# Sample PCI Flow Diagrams




**IN GENERAL FOR ENTIRE MAINFRAME FOOTPRINT**

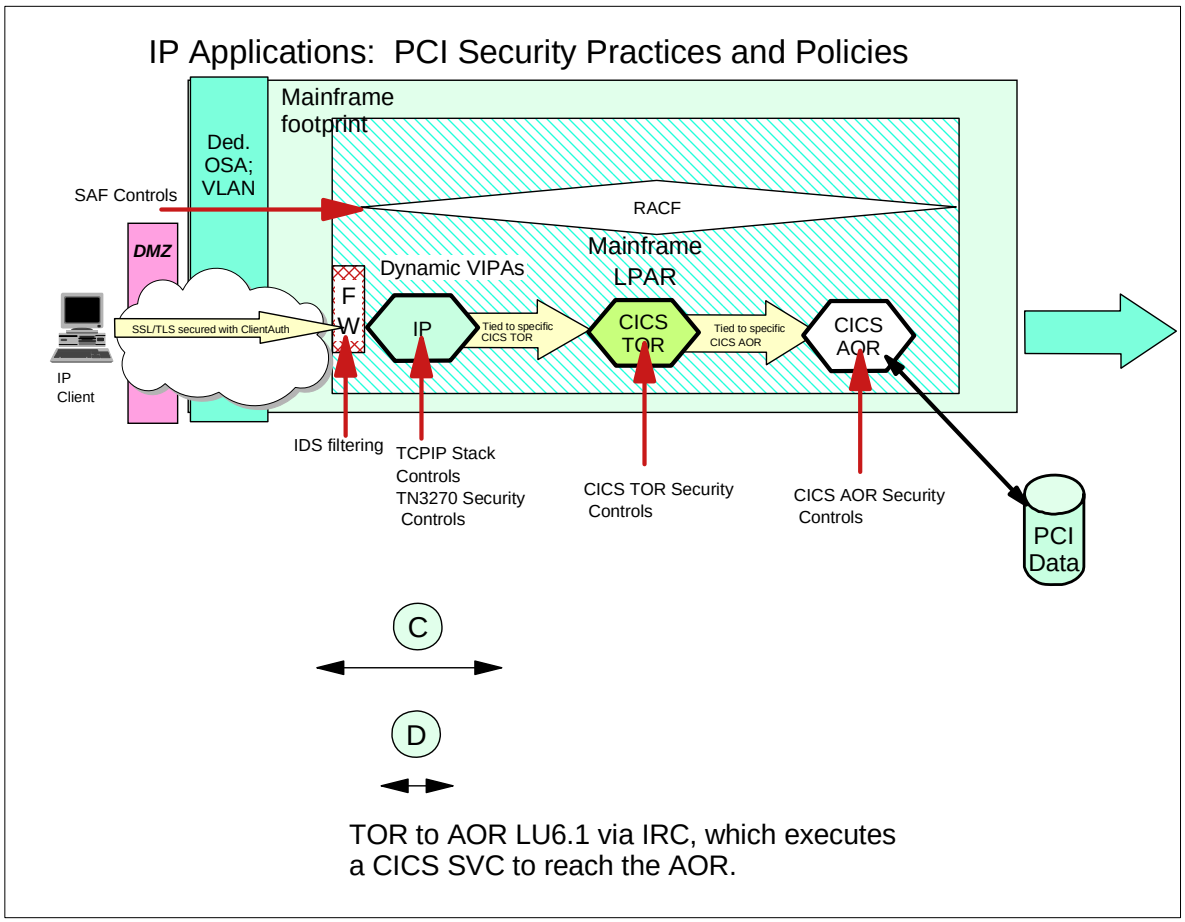
- Required: Procedures are documented and implemented to update hardware, systems software, and application software with latest security maintenance.
- Required: Personnel who develop code do not perform final production test of the code; different personnel perform final production test.
- Required: Use OPTIM or other software to create "look-alike" test data that is not the actual production data.
- Required: Document and Implement change control for all processes involving PCI data.
- Required: Implement IDS in network or on mainframe to thwart Denial of Service to TN3270 for PCI data and applications.
- Best Practice: Implement the IDS on the PCI LPAR using IBM Configuration Assistant.
- Required: Implement physical access control to PCI systems and data.

**PATH SECTION A:**

- Required: Access protected with SSL/TLS (Isolation through Authentication, Data Integrity and Privacy Controls)
- Required: Path into Intranet protected through DMZ configuration and multiple external firewalls filtering for IP addresses and NATing the addresses to conceal them.
- Best Practice: Network Adapter Access uses VLAN over dedicated Adapter (OSA) port, isolating this port from rest of peripheral network
- Best Practice: Network (outboard) firewall filters on source network and destination IP address for a specific TN3270 server endpoint (Unique Virtual IP Address - VIPA - per TN3270 PCI application)
- Desirable Granular Control: z/OS Policy Agent enforces IDS policy against remote TN3270 user network; IDS logs and reports reviewed daily

.**PATH SECTION B:**

- Required: Secured through SSL/TLS:
- Server and Client Authentication
- Data Integrity Checking
- Encryption with 3DES or AES

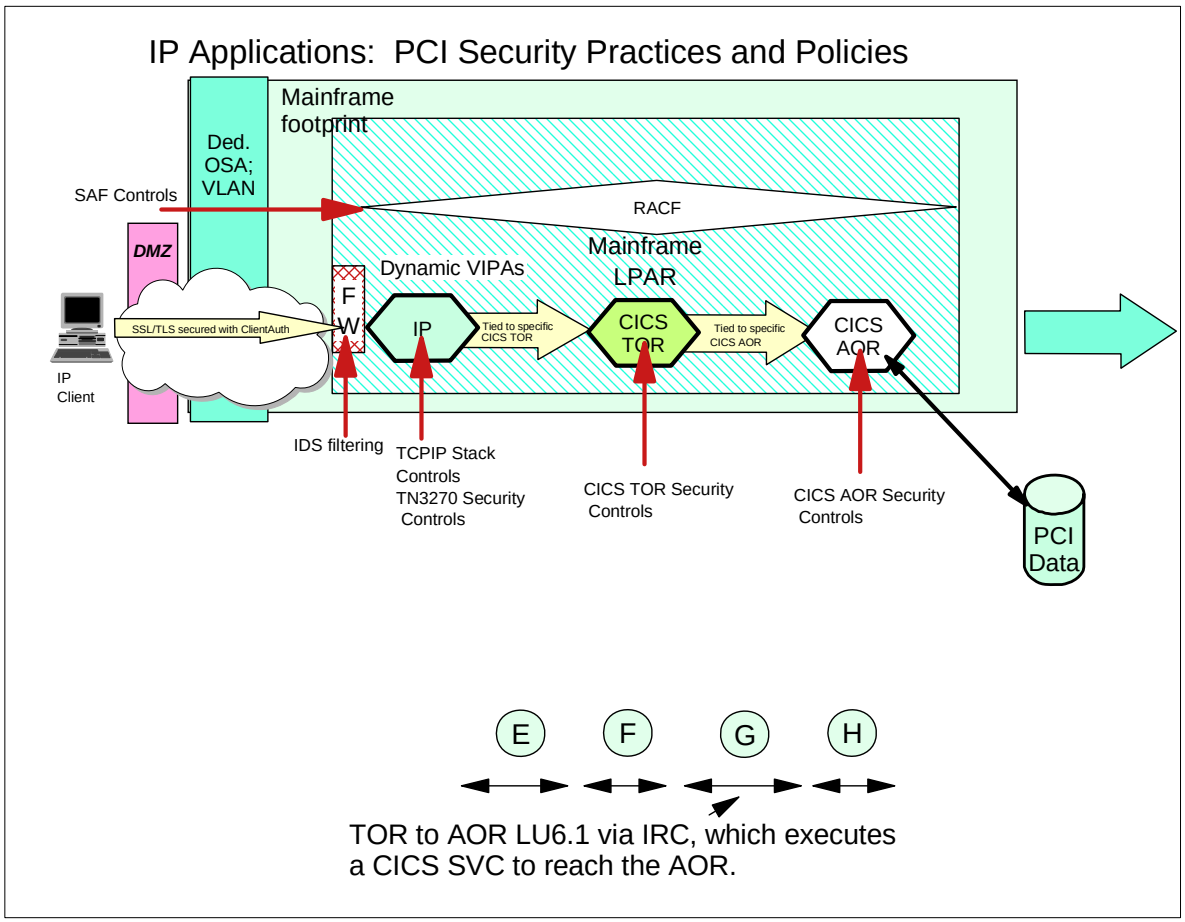



**PATH SECTION C:**

- Required: TN3270 is APF-authorized, allowing only certain users to run this server from certain controlled libraries on the system.
- Best Practice: TN3270 Server is isolated through IP addressing with bind-specific static VIPA address on Port reservations and separate port number that are reserved only for this address space.
- Required: z/OS separate address for each TN3270 address space delivers integrity through isolation techniques (storage protect keys, etc.)
- Required: TCP/IP Stack has opened only necessary ports and services
- Desirable Granular Control - Optional: Identify this instance of TN3270 port number with a Security Access Facility (SAF) RACF resource name.
- Desirable Granular Control - Optional: NETACCESS statement in TCP/IP stack permits traffic only between remote PCI network and this instance of TN3270 server address space

.**PATH SECTION D:**

- Required: SSL/TLS with Client Authentication and AES or 3DES required
- Required: This TN3270 address space is used only for access to PCI processes and data.
- Required: ALLOWAPPL, DEFAULTAPPL with LUSESSIONPEND to tie this user to specific PCI CICS Region, even at logoff.
- Required: LUname mapping to tie this TN3270 connection and remote IP address/roup of client to a specific CICS terminal in the CICS TOR region
- Required: ALLOWAPPL in TN3270 to restrict users to this instance of the CICS region; QUEUESESSION controls applied
- Required: Inactivity timeouts log user off after 15 minutes of inactivity.
- Desirable Granular Control - Optional: RESTRICTAPPL with CERTAUTH checking for CICS based upon CLIENT SSL/TLS Certificate; or RESTRICTAPPL with Client userid logon validation
- Required: SMF records (Type 119) for session initiation and termination audit records




**PATH SECTION E:**

- Required: Secured Internal Path within z/OS interconnects TN3270 server with CICS Terminal Owning Region.

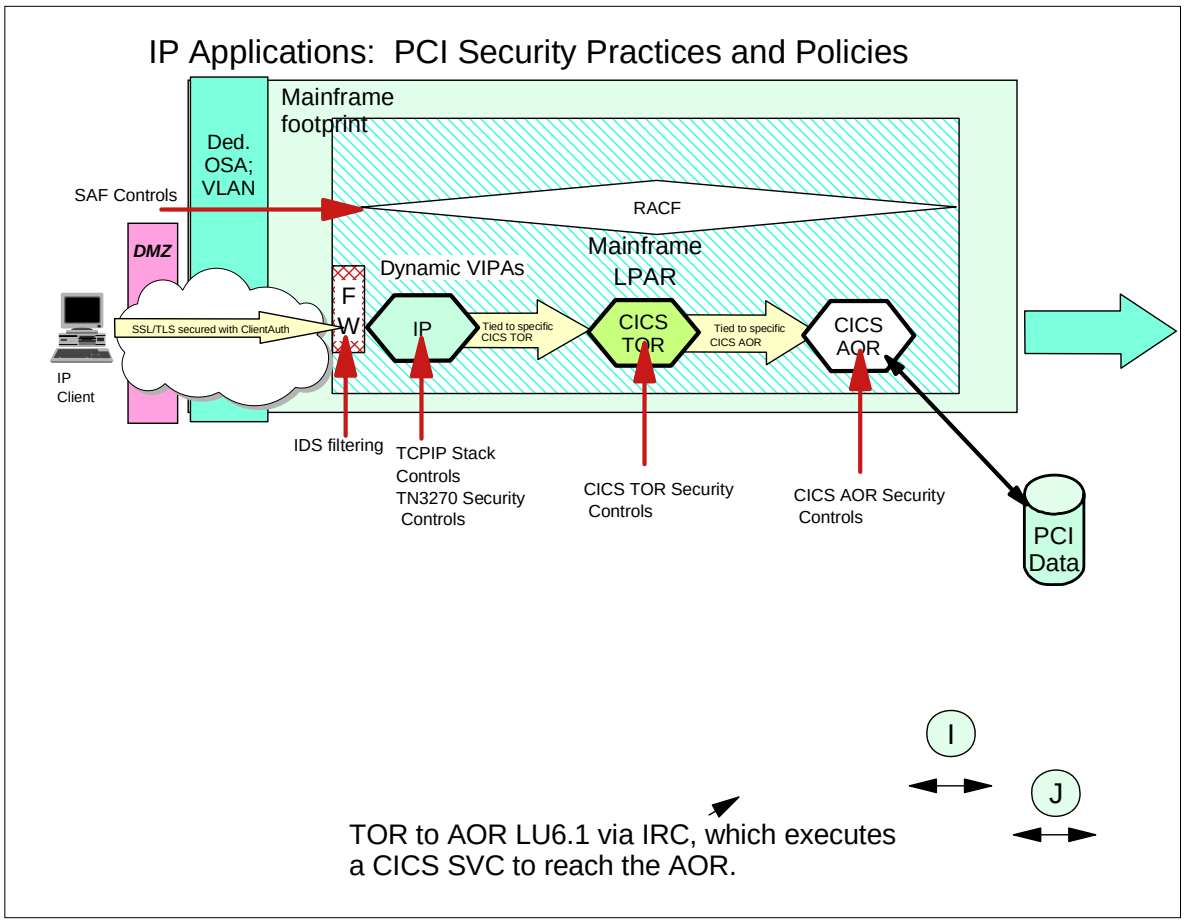
.**PATH SECTION F:**

- Required: TOR is protected in its own address space (subject to z/OS integrity controls)
- Required: TN3270 is APF-authorized, allowing only certain users to run this server from certain controlled libraries on the system.
- Required: Userid and Password of remote client are permitted by SAF (RACF) to this AOR.
- Required: Only this SNA LUname used by TN3270 may access this TOR
- Required: This TOR may access only a specific Application Owning region based on TRANID and AOR SSID.
- Required: Transactions are routed to AOR; no application code in TOR.
- Required: CICS Audit records maintained by XXXXXXXXXXXXX (Example: SMF110; User Journals)

**PATH SECTION G:**

**PATH SECTION H:**

- Required: AOR is protected in its own address space (subject to z/OS integrity controls)
- Required: This AOR region is APF-authorized, allowing only certain users to run this region from certain controlled libraries on the system.
- Required: This AOR can be reached only through the associated TOR
- Required: This AOR may execute Transaction IDs that are installed and related to PCI only.
- Resource level security isolates access to specific application modules involving PCI access.
- Required: CICS Audit records maintained by XXXXXXXXXXXXX (Example: SMF110; User Journals)




**PATH SECTION I:**

- Required: SAF controls determine by userid and password and group level who may access which data
- Required: SAF controls determine which applications may access the data
- Required: Audit records of access to data established with XXXXXXXXXXX (SMF records to record writes to DASD)

.**PATH SECTION J:**

- Required: Only encrypted data resides on PCI disk.
- Required: PCI data is isolated to a specific set of devices with no non-PCI data residing on the same device.
- Required: ICSF routines encrypt data using AES before the data is written to the disk.
- Required: ICSF routines decrypt the data after the data is read from disk.
- Required: ICSF key management routines are implemented and documented.

# End of Topic