

---

# IS4231 T8

# SECURITY MANAGEMENT MODELS

---

GROUP 5: HE QI, VASHIQA AGRAWAL, EDWARD NG

---



# Part 1

**QUESTION 1: CONSIDERING WHY A CERTAIN INFORMATION SYSTEM/INFOSEC PROGRAM COULD BE PCI DSS COMPLIANT BUT NOT SECURED, WHICH OF THE FOLLOWING IS A POTENTIAL REASON? (PLS SELECT ALL THE OPTIONS THAT APPLY)**

1. The effectiveness of Self-assessment compliant is with doubt.
2. Typically, QSAs may only review a sample of system components.
3. The system could be compliant at the examination point but failed to keep compliant along the way.
4. QSAs' professionalism may be with doubt.

**QUESTION 1: CONSIDERING WHY A CERTAIN INFORMATION SYSTEM/INFOSEC PROGRAM COULD BE PCI DSS COMPLIANT BUT NOT SECURED, WHICH OF THE FOLLOWING IS A POTENTIAL REASON? (PLS SELECT ALL THE OPTIONS THAT APPLY)**

- 1. The effectiveness of Self-assessment compliant is with doubt.
- 2. Typically, QSAs may only review a sample of system components.
- 3. The system could be compliant at the examination point but failed to keep compliant along the way.
- 4. QSAs' professionalism may be with doubt.

**QUESTION 1: CONSIDERING WHY A CERTAIN INFORMATION SYSTEM/INFOSEC PROGRAM COULD BE PCI DSS COMPLIANT BUT NOT SECURED, WHICH OF THE FOLLOWING IS A POTENTIAL REASON? (PLS SELECT ALL THE OPTIONS THAT APPLY)**

1. The Self-Assessment Questionnaire includes a series of yes-or-no questions for each applicable PCI Data Security Standard requirement. Thus the self assessor might not rigorously check their systems for non-compliance
2. Even properly scoped assessments are limited by time and resources, and as such, in most cases QSAs can only review a sample of systems components. Making it impossible for a QSA to uncover all gaps and vulnerabilities.
3. Some organizations falsely assume that PCI DSS compliance is merely passing their annual assessments and obtaining certifications. These organizations are employing compliance efforts into a singular event; however, failing to maintain compliance is part of the organization's continuous monitoring effort.

**QUESTION 2: THEORETICALLY, WHICH OF THE FOLLOWING MERCHANTS DOES *NOT* NEED TO COMPLY WITH PCI STANDARDS?**

1. Starbucks
2. Square POS
3. FavePay
4. None of the above

## QUESTION 2: THEORETICALLY, WHICH OF THE FOLLOWING MERCHANTS DOES *NOT* NEED TO COMPLY WITH PCI STANDARDS?

1. Starbucks
2. Square POS
3. FavePay
- 4. None of the above

The PCI DSS applies to **all entities that store, process, and/or transmit cardholder data**. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

# COMMON CRITERIA - EVALUATION ASSURANCE LEVEL

- **EAL1: Functionally Tested**

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious.

- **EAL2: Structurally Tested**

EAL2 requires the cooperation of the developer in terms of the delivery of design information and test results but should not demand more effort on the part of the developer than is consistent with good commercial practice.

- **EAL3: Methodically Tested and Checked**

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

- **EAL4: Methodically Designed, Tested and Reviewed**

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.



# COMMON CRITERIA - EVALUATION ASSURANCE LEVEL

- **EAL5: Semiformally Designed and Tested**

EAL5 permits a developer to **gain maximum assurance from security engineering** based upon rigorous commercial development practices **supported by moderate application of specialist security engineering techniques**.

- **EAL6: Semiformally Verified Design and Tested**

EAL6 permits developers to **gain high assurance from application of security engineering techniques** to a rigorous development environment in order to produce a **premium TOE** for protecting **high-value assets** against significant risks.

- **EAL7: Formally Verified Design and Tested**

EAL7 is applicable to the development of **security TOEs for application in extremely high risk situations** and/or where the high value of the assets justifies the higher costs.

**QUESTION 3: CONSIDERING THE SEVEN EALS, WHICH OF THE FOLLOWING PRODUCTS MAY BE MORE LIKELY TO GET ITSELF EXAMINED AGAINST EAL 7 (I.E., FORMALLY VERIFIED DESIGN AND TESTED) REQUIREMENTS?**

1. Commercial firewall
2. Chips for military usage
3. Digital signature solution
4. Key management system

QUESTION 3: CONSIDERING THE SEVEN EALS, WHICH OF THE FOLLOWING PRODUCTS MAY BE MORE LIKELY TO GET ITSELF EXAMINED AGAINST EAL 7 (I.E., FORMALLY VERIFIED DESIGN AND TESTED) REQUIREMENTS?

1. Commercial firewall
- 2. Chips for military usage
3. Digital signature solution
4. Key management system

EAL7 is applicable to the development of security TOEs for application in **extremely high risk situations and/or where the high value of the assets justifies the higher costs**

TOE: Target Of Evaluation

# Part 2

PCI DSS



# Part 2 Qn 1

Target Data Breach Case

---

# Summary of Lawsuits

WHO?



Why?

- Loss of money in alerting customers to the breach
- Loss of money in reimbursing fraudulent charges and reissuing cards
- Possible increase in losses if criminals use the cards
- Target knew its systems were vulnerable but wanted to keep costs down.

# Quiz!

When did the target data breach occur?

Hint: It's a day equivalent to the  
*Great Singapore Sale!*

---

# Quiz!

When did the target data breach occur?

A black square with the words "BLACK FRIDAY" in white, bold, sans-serif capital letters.

**BLACK  
FRIDAY**

**Nov 27 - Dec 15 2013**

---



## 1) WHAT ARE THE REQUIREMENTS IN PCI DSS V3.2.1 THAT TARGET MIGHT HAVE FAILED TO COMPLY WITH BEFORE THE BREACH?

### How did the breach occur?

- Gary Warner, founder of Malcovery Security, feels servers fell to **SQL-injection attacks**. He bases that on the many similarities between the Target breach and those perpetrated by the Drinkman and Gonzalez data-breach gang which also used SQL injection.
- Hackers broke into the retailer's network using **login credentials stolen** from a heating, ventilation and air conditioning company that does work for Target at a number of locations.
- Fazio apparently had access rights to Target's network for carrying out tasks like remotely monitoring energy consumption and temperatures at various stores.
- The attackers leveraged the access provided by the Fazio credentials to move about undetected on Target's network and upload malware programs on the company's Point of Sale (POS) systems.
- Target says the attackers gained access to customer names, credit card or debit card numbers, card expiration dates and CVV security codes. Krebs on Security and the *Wall Street Journal* report that the thieves accessed data from the magnetic stripes stored on the back of credit and debit cards.



# Your Turn!

## Which requirements did Target fail to comply with?

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

**1.1** Establish and implement firewall and router configuration standards that include the following:

- 1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations
- 1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
- 1.1.3** Current diagram that shows all cardholder data flows across systems and networks
- 1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- 1.1.5** Description of groups, roles, and responsibilities for management of network components
- 1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
- 1.1.7** Requirement to review firewall and router rule sets at least every six months

**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

*Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.*

- 1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
- 1.2.2** Secure and synchronize router configuration files.
- 1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.

**1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.

**1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

(For example, block traffic originating from the Internet with an internal source address.)

**1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

**1.3.5** Permit only “established” connections into the network.

**1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

**1.3.7** Do not disclose private IP addresses and routing information to unauthorized parties.

*Note: Methods to obscure IP addressing may include, but are not limited to:*

- *Network Address Translation (NAT)*
- *Placing servers containing cardholder data behind proxy servers/firewalls,*
- *Removal or filtering of route advertisements for private networks that employ registered addressing,*
- *Internal use of RFC1918 address space instead of registered addresses.*

# Which requirements did Target fail to comply with?

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

**1.1** Establish and implement firewall and router configuration standards that include the following:

**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations

**1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

**1.1.3** Current diagram that shows all cardholder data flows across systems and networks

**1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

**1.1.5** Description of groups, roles, and responsibilities for management of network components

**1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

**1.1.7** Requirement to review firewall and router rule sets at least every six months

**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

*Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*

**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

**1.2.2** Secure and synchronize router configuration files.

**1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.

**1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.

**1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

(For example, block traffic originating from the Internet with an internal source address.)

**1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

**1.3.5** Permit only "established" connections into the network.

**1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

**1.3.7** Do not disclose private IP addresses and routing information to unauthorized parties.

*Note: Methods to obscure IP addressing may include, but are not limited to:*

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls,
- Removal or filtering of route advertisements for private networks that employ registered addressing,
- Internal use of RFC1918 address space instead of registered addresses.

# Your Turn!

## Which requirements did Target fail to comply with?

### Requirement 3: Protect stored cardholder data

**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

**3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:

- There is a business justification and
- The data is stored securely.

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:

**3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- The cardholder's name
- Primary account number (PAN)
- Expiration date
- Service code

To minimize risk, store only these data elements as needed for business.

**3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

**3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

*Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*

**3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography, (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

*Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*

**3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

*Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*

**3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:

*Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*



# Which requirements did Target fail to comply with?

## Requirement 3: Protect stored cardholder data

**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

**3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:

- There is a business justification and
- The data is stored securely.

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:

**3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- The cardholder's name
- Primary account number (PAN)
- Expiration date
- Service code

To minimize risk, store only these data elements as needed for business.

**3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

**3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

*Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*

**3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography, (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

*Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*

**3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

*Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*

**3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:

*Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*

# Your Turn!

## Which requirements did Target fail to comply with?

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

**6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as high, medium, or low) to newly discovered security vulnerabilities.

*Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.*

*Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organizations environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a high risk to the environment. In addition to the risk ranking, vulnerabilities may be considered critical if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*

**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

*Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*

**6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

- In accordance with PCI DSS (for example, secure authentication and logging)
- Based on industry standards and/or best practices.
- Incorporating information security throughout the software-development life cycle

*Note: This applies to all software developed internally as well as bespoke or custom software developed by a third party.*

**6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.

**6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

- Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines
- Appropriate corrections are implemented prior to release.
- Code-review results are reviewed and approved by management prior to release.

*Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*

**6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following:

**6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

**6.5.2** Buffer overflows

**6.5.3** Insecure cryptographic storage

**6.5.4** Insecure communications

**6.5.5** Improper error handling

**6.5.6** All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).



# Which requirements did Target fail to comply with?

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

**6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as high, medium, or low) to newly discovered security vulnerabilities.

*Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.*

*Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organizations environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a high risk to the environment. In addition to the risk ranking, vulnerabilities may be considered critical if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*

**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

*Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*

**6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

- In accordance with PCI DSS (for example, secure authentication and logging)
- Based on industry standards and/or best practices.
- Incorporating information security throughout the software-development life cycle

*Note: This applies to all software developed internally as well as bespoke or custom software developed by a third party.*

**6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.

**6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

- Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines
- Appropriate corrections are implemented prior to release.
- Code-review results are reviewed and approved by management prior to release.

*Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*

**6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following:

**6.5** Address common coding vulnerabilities in software-development processes as follows:

**6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

**6.5.2** Buffer overflows

**6.5.3** Insecure cryptographic storage

**6.5.4** Insecure communications

**6.5.5** Improper error handling

**6.5.6** All "high risk" vulnerabilities identified in the vulnerability identification process

# Your Turn!

Which requirements did Target fail to comply with?

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

**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.

**7.1.1** Define access needs for each role, including:

- System components and data resources that each role needs to access for their job function
- Level of privilege required (for example, user, administrator, etc.) for accessing resources.

**7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

**7.1.3** Assign access based on individual personnel's job classification and function.

**7.1.4** Require documented approval by authorized parties specifying required privileges.

**7.2** Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

This access control system(s) must include the following:

**7.2.1** Coverage of all system components

**7.2.2** Assignment of privileges to individuals based on job classification and function.

**7.2.3** Default "deny-all" setting.

**7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.



# Which requirements did Target fail to comply with?

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

**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.

**7.1.1** Define access needs for each role, including:

- System components and data resources that each role needs to access for their job function
- Level of privilege required (for example, user, administrator, etc.) for accessing resources.

**7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

**7.1.3** Assign access based on individual personnel's job classification and function.

**7.1.4** Require documented approval by authorized parties specifying required privileges.

**7.2** Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

This access control system(s) must include the following:

**7.2.1** Coverage of all system components

**7.2.2** Assignment of privileges to individuals based on job classification and function.

**7.2.3** Default "deny-all" setting.

**7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

# Your Turn!

## Which requirements did Target fail to comply with?

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

**8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.

**8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

**8.1.3** Immediately revoke access for any terminated users.

**8.1.4** Remove/disable inactive user accounts within 90 days.

**8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

- Enabled only during the time period needed and disabled when not in use.
- Monitored when in use.

**8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts.

**8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

**8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

**8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric.

**8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

**8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

**8.4** Document and communicate authentication policies and procedures to all users including:

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

**8.5.1 Additional requirement for service providers only:** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

*Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*

**8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

**8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

# Which requirements did Target fail to comply with?

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

**8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.

**8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

**8.1.3** Immediately revoke access for any terminated users.

**8.1.4** Remove/disable inactive user accounts within 90 days.

**8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

- Enabled only during the time period needed and disabled when not in use.
- Monitored when in use.

**8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts.

**8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

**8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

**8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric.

**8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

**8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

**8.4** Document and communicate authentication policies and procedures to all users including:

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

**8.5.1 Additional requirement for service providers only:** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

*Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*

**8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

**8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).



# Your Turn!

## Which requirements did Target fail to comply with?

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

**11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

*Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*

**11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification.

**11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected.

**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

*Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.*

*For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*

**11.3** Implement a methodology for penetration testing that includes the following:

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

**11.4** Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

**11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

*Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*

# Which requirements did Target fail to comply with?

## Requirement 11: Regularly test security systems and processes

**11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

*Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*

**11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification.

**11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected.

**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

*Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.*

*For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*

**11.3** Implement a methodology for penetration testing that includes the following:

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

**11.4** Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

**11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

*Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*

# Your Turn!

Which requirements did Target fail to comply with?

## Requirement 12: Maintain a policy that addresses information security for all personnel

**12.1** Establish, publish, maintain, and disseminate a security policy.

**12.1.1** Review the security policy at least annually and update the policy when the environment changes.

**12.2** Implement a risk-assessment process that:

- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
- Identifies critical assets, threats, and vulnerabilities, and
- Results in a formal, documented analysis of risk.

Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

**12.3** Develop usage policies for critical technologies and define proper use of these technologies.

*Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*

Ensure these usage policies require the following:

**12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

# Which requirements did Target fail to comply with?

## Requirement 12: Maintain a policy that addresses information security for all personnel

**12.1** Establish, publish, maintain, and disseminate a security policy.

**12.1.1** Review the security policy at least annually and update the policy when the environment changes.

**12.2** Implement a risk-assessment process that:

- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
- Identifies critical assets, threats, and vulnerabilities, and
- Results in a formal, documented analysis of risk.

Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

**12.3** Develop usage policies for critical technologies and define proper use of these technologies.

*Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*

Ensure these usage policies require the following:

**12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

# 29%

According to Verizon, only 29% of companies are compliant a year after validation!



2) CONSIDERING THE BUSINESS MODEL OF TARGET, IF TARGET PLANNED TO CONDUCT SELF-ASSESSMENT FOR COMPLIANCE PURPOSE, WHICH SELF-ASSESSMENT QUESTIONNAIRE (SAQ) TARGET SHOULD USE TO DO SELF-ASSESSMENT (E.G., A, A-EP)?

Which is Target? Circle the answer.

**Merchant**

OR

**Service  
Provider**

2). CONSIDERING THE BUSINESS MODEL OF TARGET, IF TARGET PLANNED TO CONDUCT SELF-ASSESSMENT FOR COMPLIANCE PURPOSE, WHICH SELF-ASSESSMENT QUESTIONNAIRE (SAQ) TARGET SHOULD USE TO DO SELF-ASSESSMENT (E.G., A, A-EP)?

Which is Target? Circle the answer.

**Merchant**

OR

**Service  
Provider**

2). CONSIDERING THE BUSINESS MODEL OF TARGET, IF TARGET PLANNED TO CONDUCT SELF-ASSESSMENT FOR COMPLIANCE PURPOSE, WHICH SELF-ASSESSMENT QUESTIONNAIRE (SAQ) TARGET SHOULD USE TO DO SELF-ASSESSMENT (E.G., A, A-EP)?

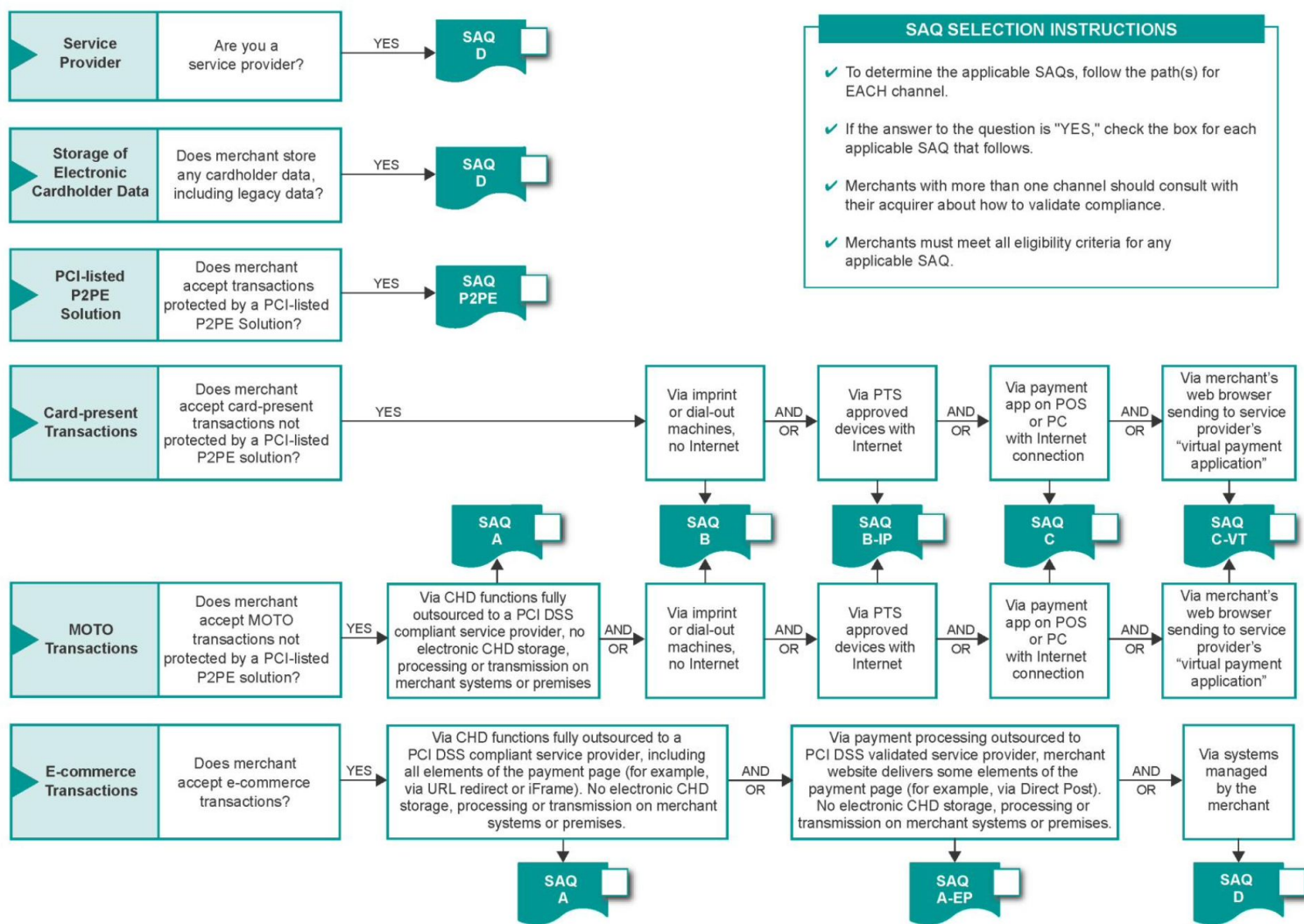
Merchant:

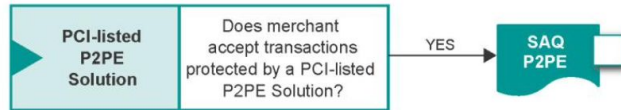
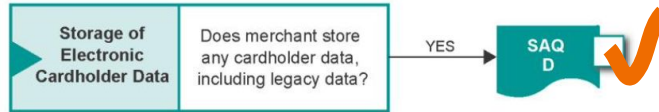
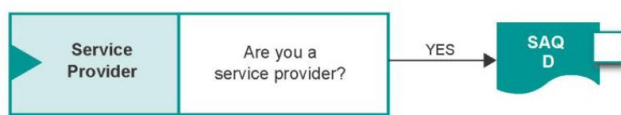
*“For the purposes of the PCI DSS, a merchant is defined as any entity that **accepts payment cards** bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.”*

Service Provider:

*“Business entity that is **not a payment brand**, directly involved in the processing, storage, or transmission of **cardholder data**. This also includes companies that provide services that control or could impact the security of cardholder data.” ---> <https://www.visa.com/splisting/searchGrsp.do>*

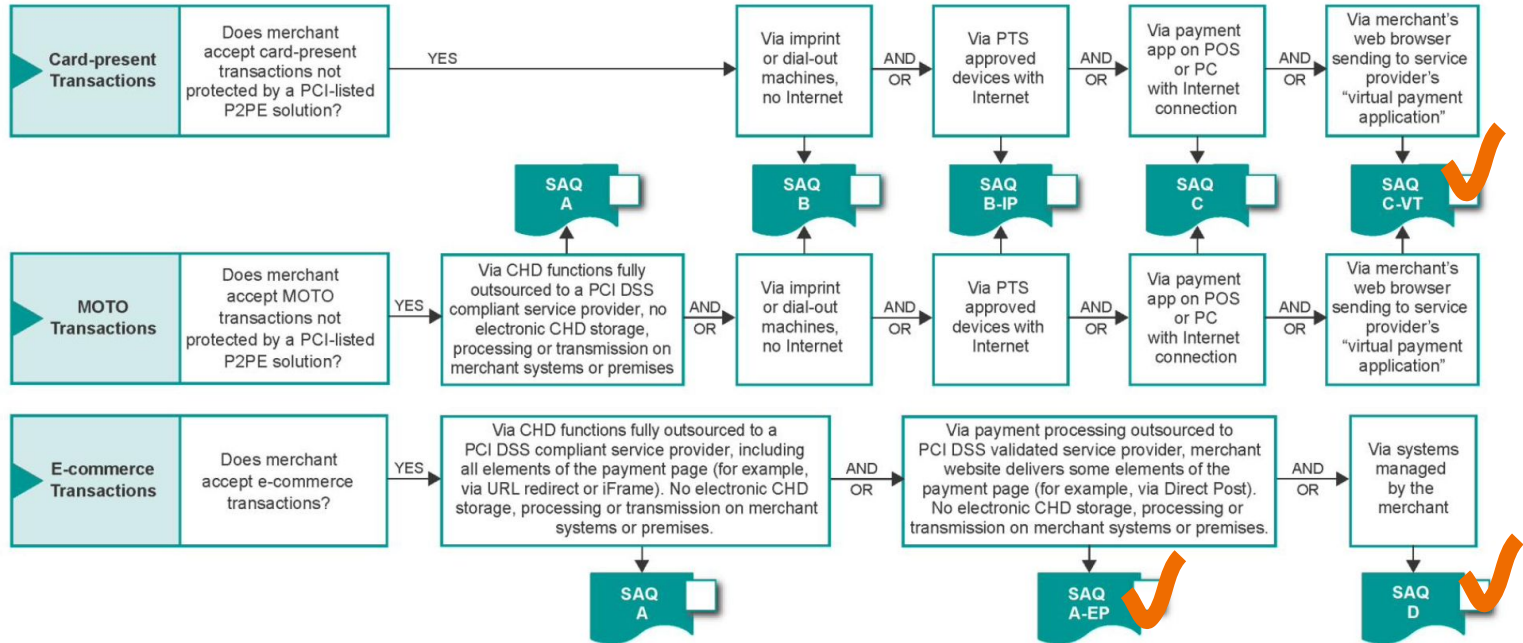
# Your Turn!





### SAQ SELECTION INSTRUCTIONS

- ✓ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✓ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✓ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✓ Merchants must meet all eligibility criteria for any applicable SAQ.



### Target.com and Target app

- Target RedCard™ (Target Debit Card, Target Credit Card, Target™ Mastercard®)
- Third-party credit cards: American Express®, Discover®/Novus®, Mastercard®, Visa®, Target PCard (corporate purchasing card), credit cards from foreign banks
- Third-party debit cards: must be connected with Visa or Mastercard and processed as a credit card
- Target GiftCards, Target eGiftCards and mobile Target GiftCards
- Third-party gift cards from American Express, Discover, Visa and Mastercard.
- [Affirm](#)
- PayPal® on Target.com and the Target app
  - PayPal® is not an accepted payment method for items sold by Target Plus™ Partners.

### Target stores

- Cash: Target doesn't accept currency or coin from foreign countries. However, depending on where the Target store is located, stores may be able to accept Canadian dollars or Mexican pesos. Target stores update exchange rates weekly.
- Target RedCard™ (Target Debit Card, Target Credit Card, Target Mastercard™)
- Target Application on Mobile Device (Target Debit Card, Target Credit Card, Target Mastercard™)
- Target Temporary Slips (Target Debit Card, Target Credit Card)
- Third-party Credit Cards: Visa®, Mastercard®, Discover®/Novus®, American Express®, credit cards from foreign banks (JCB Japanese Credit Bureau), Diner's Club International, and FSA/HSA cards are redeemable for FSA/HSA eligible items.
- Debit/ATM and EBT Cards: U.S.-issued debit/ATM cards. Stores will accept Canadian debit/ATM cards with a NYCE® or an Interac® logo paired with Visa® logo. Some stores have the ability to perform SNAP transactions.
- Contactless pay using the Target Mastercard® or any other approved third-party credit card designed for contactless pay.
- Gift Cards: Target GiftCards, Merchandise Return Cards and Prepaid Gift Cards with a Visa®, Mastercard®, Discover®, or American Express® logo. Starbucks gift cards can be used at the in-store Starbucks registers. Target GiftCards can't be used to apply a payment towards a RedCard or to purchase Target GiftCards, specialty gift cards, American Express, Visa or Mastercard gift cards, iTunes gift cards, or services at Minute Clinics within Target stores.
- Gift Certificates: A Target Corporation gift certificate is good in the issuing country only.
- Merchandise Voucher: Target merchandise vouchers don't expire.
- Multiple Payment Methods Sales: Store team members can accept both a credit and debit card or EBT card per sale. Our checkout registers can process multiple credit cards in one transaction.
- Personal Checks
- Rebate Checks: Generally only pay for part of the cost of an item. Rebate checks are not allowed to purchase any Target GiftCard, specialty gift card or any third-party gift cards from American Express, Discover, Visa and Mastercard. FSA /HSA checks are redeemable at pharmacy and optical lanes.
- WIC (Women, Infants and Children) Program (approved in authorized stores only)
- Mobile Payments such as Apple Pay®, Google Pay™, Samsung Pay, or any contactless digital wallet.
- Alipay is approved in authorized stores only.
- Campus Cash is approved in authorized stores only.

# Part 2



COMMON CRITERIA

# IDPS SYSTEMS WITH DIFFERENT EALS ACHIEVED

## **Trend Micro Deep Security 11.0 (EAL2+)**

- Software intrusion detection and prevention software system
- Certifier: DXC Security Testing/Certification Laboratories

## **LogPoint 5.2.5 (EAL3+)**

- Security Information and Event Management (SIEM) system. It is part of an enterprise network and collects and analyses log information from devices on this network.
- Certifier: atsec information security AB



# IS PRODUCT B MORE SECURED THAN PRODUCT A?

- If both products have the exact same TOE then yes
- Otherwise it would not be an accurate comment since the products would be tested specifically to the target scope
- Moreover the concept of Augmenting Security Assurance Components (EAL X+). also makes a bigger difference
- An eal4+ might be more secure than eal 5 depending on the AVA\_VAN - vulnerability assessment



## Part 2: Qn 2

New Compliance Level:  
Protection Profile (PP)  
Compliant

---

# PROTECTION PROFILE (PP) COMPLIANT INTRODUCTION

- A document part of Common Criteria.
- A **combination** of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.
- A PP specifies **generic security evaluation criteria**.
- Specifies **the EAL1-7**
- A PP **states a security problem rigorously** and to **specify security requirements**
- Define a **Security Target (ST)**

# NIAP'S TRANSITION TO PROTECTION PROFILES

- In October of 2009, the National Information Assurance Partnership (NIAP), transitioned away from Evaluation Assurance Levels (EAL) and moved to Protection Profiles (PP).



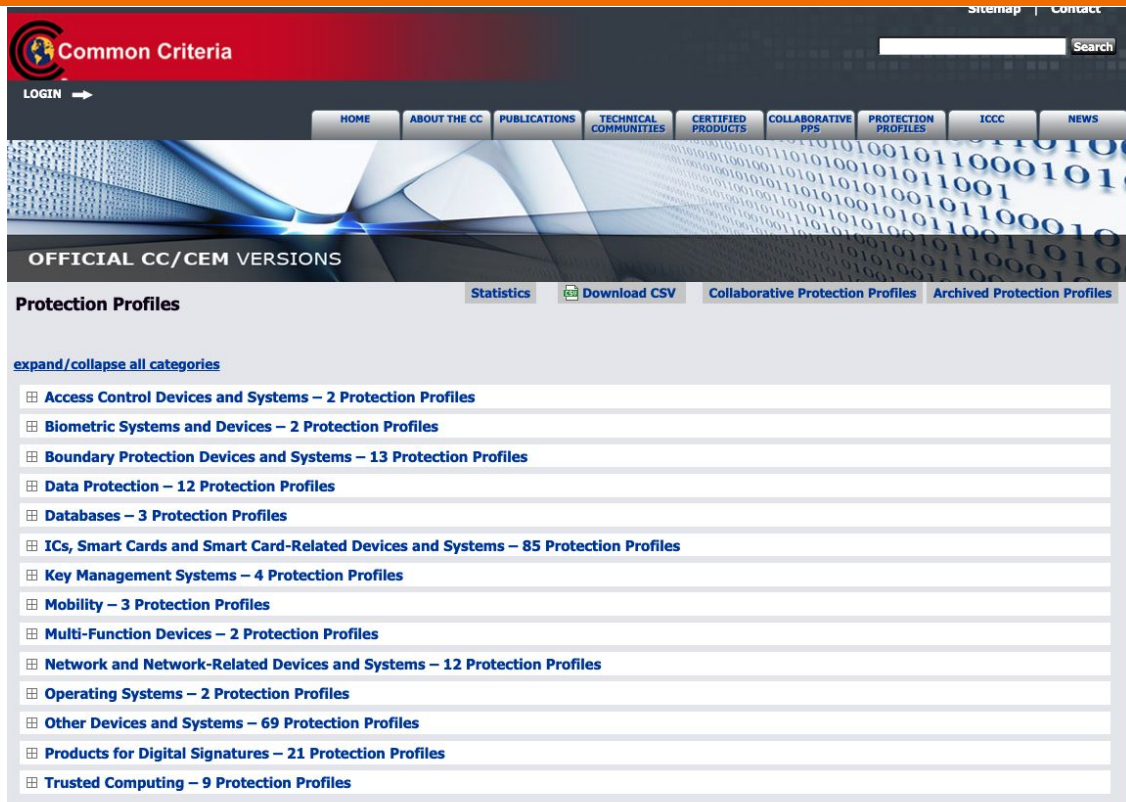
# APPROVED PROTECTION PROFILES

(CURRENTLY 56 VALIDATED NIAP-Approved PPs)

Tech Type	Profile Name	CC Ver.	Short Name	Sponsor	Approval Date	Sunset Date
Application Software	Protection Profile for Application Software Version 1.3	3.1	PP_APP_v1.3	NIAP	2019-03-01	
BIOS Update	Protection Profile for BIOS Update for PC Client Devices Version 1.0	3.1	PP_BIOS_v1.0	NIAP	2013-02-13	
Certificate Authority	Protection Profile for Certification Authorities Version 2.1	3.1	PP_CA_V2.1	NIAP	2017-12-01	
Email Client	Extended Package for Email Clients v2.0	3.1	PP_APP_EMAILCLIENT_EP_v2.0	NIAP	2015-06-18	
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201	3.1	CPP_FDE_AA_V2.0E		2019-02-01	
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201	3.1	CPP_FDE_EE_V2.0E		2019-02-01	
Encrypted Storage	PP-Module for File Encryption Enterprise Management Version 1.0	3.1	MOD_FEEM_V1.0	NIAP	2019-07-30	
Encrypted Storage	PP-Module for File Encryption Version 1.0	3.1	MOD_FE_V1.0	NIAP	2019-07-25	
Enterprise Security Management	PP-Module for Endpoint Detection and Response Version 1.0	3.1	MOD_EDR_V1.0	NIAP	2020-10-23	
Enterprise Security Management	PP-Module for Host Agent Version 1.0	3.1	MOD_HA_V1.0	NIAP	2020-10-23	
Enterprise Security Management	Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1	3.1	PP_ESM_ICM_V2.1	NIAP	2013-11-21	
Enterprise Security Management	Protection Profile for Enterprise Security Management - Policy Management Version 2.1	3.1	PP_ESM_PM_V2.1	NIAP	2013-11-21	
Enterprise Security Management	Protection Profile for Enterprise Security Management-Access Control Version 2.1	3.1	PP_ESM_AC_V2.1	NIAP	2013-11-12	
Firewall	collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625	3.1	MOD_CPP_FW_v1.4e		2020-07-01	

# APPROVED PROTECTION PROFILES

(CURRENTLY 239 VALIDATED International PPs)



The screenshot displays the Common Criteria website interface. At the top, there is a red header with the Common Criteria logo and the text "Common Criteria". Below the header, a navigation bar contains links: HOME, ABOUT THE CC, PUBLICATIONS, TECHNICAL COMMUNITIES, CERTIFIED PRODUCTS, COLLABORATIVE PPS, PROTECTION PROFILES, ICC, and NEWS. A search bar is located on the right side of the header. The main content area features a large banner with the text "OFFICIAL CC/CEM VERSIONS" and a background image of binary code. Below the banner, there is a section titled "Protection Profiles" with a sub-header "expand/collapse all categories". This section lists various categories of protection profiles, each with a corresponding number of profiles:

- Access Control Devices and Systems – 2 Protection Profiles
- Biometric Systems and Devices – 2 Protection Profiles
- Boundary Protection Devices and Systems – 13 Protection Profiles
- Data Protection – 12 Protection Profiles
- Databases – 3 Protection Profiles
- ICs, Smart Cards and Smart Card-Related Devices and Systems – 85 Protection Profiles
- Key Management Systems – 4 Protection Profiles
- Mobility – 3 Protection Profiles
- Multi-Function Devices – 2 Protection Profiles
- Network and Network-Related Devices and Systems – 12 Protection Profiles
- Operating Systems – 2 Protection Profiles
- Other Devices and Systems – 69 Protection Profiles
- Products for Digital Signatures – 21 Protection Profiles
- Trusted Computing – 9 Protection Profiles

# National Information Assurance Partnership (NIAP)

EAL	LEVEL 7
-----	---------

EAL	LEVEL 6
-----	---------

EAL	LEVEL 5
-----	---------

EAL	LEVEL 4
-----	---------

EAL	LEVEL 3
-----	---------

<b>EAL</b>	<b>LEVEL 2</b>
------------	----------------

EAL	LEVEL 1
-----	---------

NETWORK DEVICE

EAL	LEVEL 7
-----	---------

EAL	LEVEL 6
-----	---------

EAL	LEVEL 5
-----	---------

EAL	LEVEL 4
-----	---------

<b>EAL</b>	<b>LEVEL 3</b>
------------	----------------

EAL	LEVEL 2
-----	---------

EAL	LEVEL 1
-----	---------

VPN

EAL	LEVEL 7
-----	---------

EAL	LEVEL 6
-----	---------

EAL	LEVEL 5
-----	---------

<b>EAL</b>	<b>LEVEL 4</b>
------------	----------------

EAL	LEVEL 3
-----	---------

EAL	LEVEL 2
-----	---------

EAL	LEVEL 1
-----	---------

FIREWALL

# PROTECTION PROFILES

Product comparisons are  
**EASIER** and more **RELIABLE**



**PP COMPLIANT**

NETWORK DEVICE



**PP COMPLIANT**

VPN



**PP COMPLIANT**

FIREWALL



	PP	EAL
Security Requirements		
Recognition		
Objective / Subjective		

	PP	EAL
Security Requirements	<ul style="list-style-type: none"> <li>• All vendors within the same product type must adhere to the same security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Vendor individually chooses which security requirements to claim</li> </ul>
Recognition		
Objective / Subjective		

	PP	EAL
Security Requirements	<ul style="list-style-type: none"> <li>• All vendors within the same product type must adhere to the same security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Vendor individually chooses which security requirements to claim</li> </ul>
Recognition	<ul style="list-style-type: none"> <li>• Evaluation methods approved by the Common Criteria Recognition Arrangement</li> </ul>	<ul style="list-style-type: none"> <li>• Limited mutual recognition within the Common Criteria Recognition Arrangement, only up to EAL2</li> </ul>
Objective / Subjective		

	PP	EAL
Security Requirements	<ul style="list-style-type: none"> <li>• All vendors within the same product type must adhere to the same security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Vendor individually chooses which security requirements to claim</li> </ul>
Recognition	<ul style="list-style-type: none"> <li>• Evaluation methods approved by the Common Criteria Recognition Arrangement</li> </ul>	<ul style="list-style-type: none"> <li>• Limited mutual recognition within the Common Criteria Recognition Arrangement, only up to EAL2</li> </ul>
Objective / Subjective	<ul style="list-style-type: none"> <li>• objective</li> </ul>	<ul style="list-style-type: none"> <li>• subjective</li> </ul>

	PP	EAL
Result Repeatability		
Developed by		
How are threats identified?		

	PP	EAL
Result Repeatability	<ul style="list-style-type: none"> <li>Relevant, achievable, repeatable results</li> </ul>	<ul style="list-style-type: none"> <li>not repeatable across different products and vendors</li> </ul>
Developed by		
How are threats identified?		

	PP	EAL
Result Repeatability	<ul style="list-style-type: none"> <li>• Relevant, achievable, repeatable results</li> </ul>	<ul style="list-style-type: none"> <li>• not repeatable across different products and vendors</li> </ul>
Developed by	<ul style="list-style-type: none"> <li>• technical communities through the Common Criteria community</li> </ul>	<ul style="list-style-type: none"> <li>• individual vendors</li> </ul>
How are threats identified?		



	PP	EAL
Result Repeatability	<ul style="list-style-type: none"> <li>• Relevant, achievable, repeatable results</li> </ul>	<ul style="list-style-type: none"> <li>• not repeatable across different products and vendors</li> </ul>
Developed by	<ul style="list-style-type: none"> <li>• technical communities through the Common Criteria community</li> </ul>	<ul style="list-style-type: none"> <li>• individual vendors</li> </ul>
How are threats identified?	<ul style="list-style-type: none"> <li>• Threats identified and mandated by the NSA and other international security agencies</li> </ul>	<ul style="list-style-type: none"> <li>• Threats identified after vendor maps product functionality to Common Criteria</li> </ul>



THANK YOU!

