

Requirement 6: Change Control (6.4)



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com





Requirement 6.4

Have change control processes





Requirement 6.4

Follow change control processes and procedures for all changes to system components. The processes must include requirements 6.4.1 through 6.4.6.



Requirement Guidance

- Without **properly documented** and **implemented change controls**, **security** features could be inadvertently or deliberately **omitted** or **rendered inoperable**, **processing irregularities** could occur, or **malicious code** could be introduced.



Change is what turns a
PCI DSS compliant
environment into a
non-compliant environment



6.4 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Policies and procedures
Examine records	-	
Interview people	-	





Requirement 6.4.1

Keep test/development environments
separate from production





Requirement 6.4.1

Separate development/test environments from production environments, and enforce the separation with access controls.



Requirement Guidance

- Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less- stringent security configurations and possible vulnerabilities in a test or development environment.

6.4.1 Testing Procedures

Observe/examine systems and settings	Y	Network device configurations, access controls
Examine documentation	Y	Network documentation
Examine records	-	
Interview people	-	





Requirement 6.4.2

Have separation of duties between test/development environments and production



Requirement 6.4.2

Separation of duties
between development/test
and production
environments



Requirement Guidance

- Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know.
- The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.

One user, two accounts



Meghan_dev



Meghan_prod



6.4.2 Testing Procedures

Observe/examine systems and settings	Y	Processes
Examine documentation	-	
Examine records	-	
Interview people	Y	Responsible people in dev/test Responsible people in prod





Requirement 6.4.3

Real card numbers (PANs) must not be used for testing or development



Requirement 6.4.3

Production data (live PANs) are not used for testing or development



Requirement Guidance

- Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).



Test cards come pre-configured:

4242 1234 4568 9101

- Always accept

4242 1234 4568 9110

- Always decline

4242 1234 4568 9119

- Accept if < \$50, otherwise decline

6.4.3 Testing Procedures

Observe/examine systems and settings	Y	Test data, processes
Examine documentation	-	Testing processes
Examine records	-	
Interview people	Y	Responsible people



Don't use your own
personal card
numbers in
development and test
environments.





Requirement 6.4.4

Test data and accounts must be removed before release





Requirement 6.4.4

Removal of **test data and accounts** from system components **before** the system becomes **active** / goes into **production**.



Requirement Guidance

- Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.

6.4.4 Testing Procedures

Observe/examine systems and settings	Y	Testing processes, production data and accounts
Examine documentation	-	
Examine records	-	
Interview people	Y	Responsible people





Requirement 6.4.5

Change control procedures must include 6.4.5.1 through 6.4.5.4





Requirement 6.4.5

Change control procedures must include the following:

6.4.5.1

Impact documentation

6.4.5.2

Formal approval

6.4.5.3

Functionality testing

6.4.5.4

Back-out procedures



Requirement Guidance

- If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches—might not be fully realized and could have unintended consequences.



Requirement 6.4.5.1

(Change control procedures must include)

Documentation of impact.



Requirement Guidance

- The impact of the change should be documented so that all affected parties can plan appropriately for any processing changes.



Requirement 6.4.5.2

(Change control procedures must include)

Documented change approval by authorized parties.



Requirement Guidance

- Approval by authorized parties indicates that the change is a legitimate and approved change sanctioned by the organization.



Requirement 6.4.5.3

(Change control procedures must include)

Functionality testing to verify that the change does not adversely impact the security of the system.



Requirement Guidance

- Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change. Testing should validate that all existing security controls remain in place, are replaced with equally strong controls, or are strengthened after any change to the environment.



Requirement 6.4.5.4

(Change control procedures must include)

Back-out procedures.



Requirement Guidance

- For each change, there should be documented back-out procedures in case the change fails or adversely affects the security of an application or system, to allow the system to be restored back to its previous state.

6.4.5 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Change control procedures
Examine records	Y	Change control records
Interview people	Y	Responsible people





Requirement 6.4.6

After significant change, re-assess all relevant PCI DSS requirements



Requirement 6.4.6

(Change control procedures must include)

Upon completion of a **significant change**, all **relevant** PCI DSS requirements must be implemented on all new or changed systems and networks, and **documentation updated** as applicable.



Requirement Guidance

- Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment.
- Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed.
- A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process.

What's Typically Significant?

New additions

**Upgrades
(hardware & software)**

**Cardholder
data flows**

**Boundary
of the CDE**

**Supporting
infrastructure**

**Third party
service providers**



What's Typically Relevant?



Documentation: Network, data flows, inventory

Secure builds and defaults

Storage of cardholder data

Logging and monitoring

Vulnerability scanning

Is a penetration test needed?

6.4.6 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Change control records System configuration (network diagrams, asset registers etc.)
Interview people	Y	Responsible people



That's Fine in Theory

