

## 10: Track and Monitor all Access to Network Resources and Cardholder Data

---



# Requirement 10



Audit trails (logging)

Log specific events

Make sure the logs contain the right data

Time synchronization

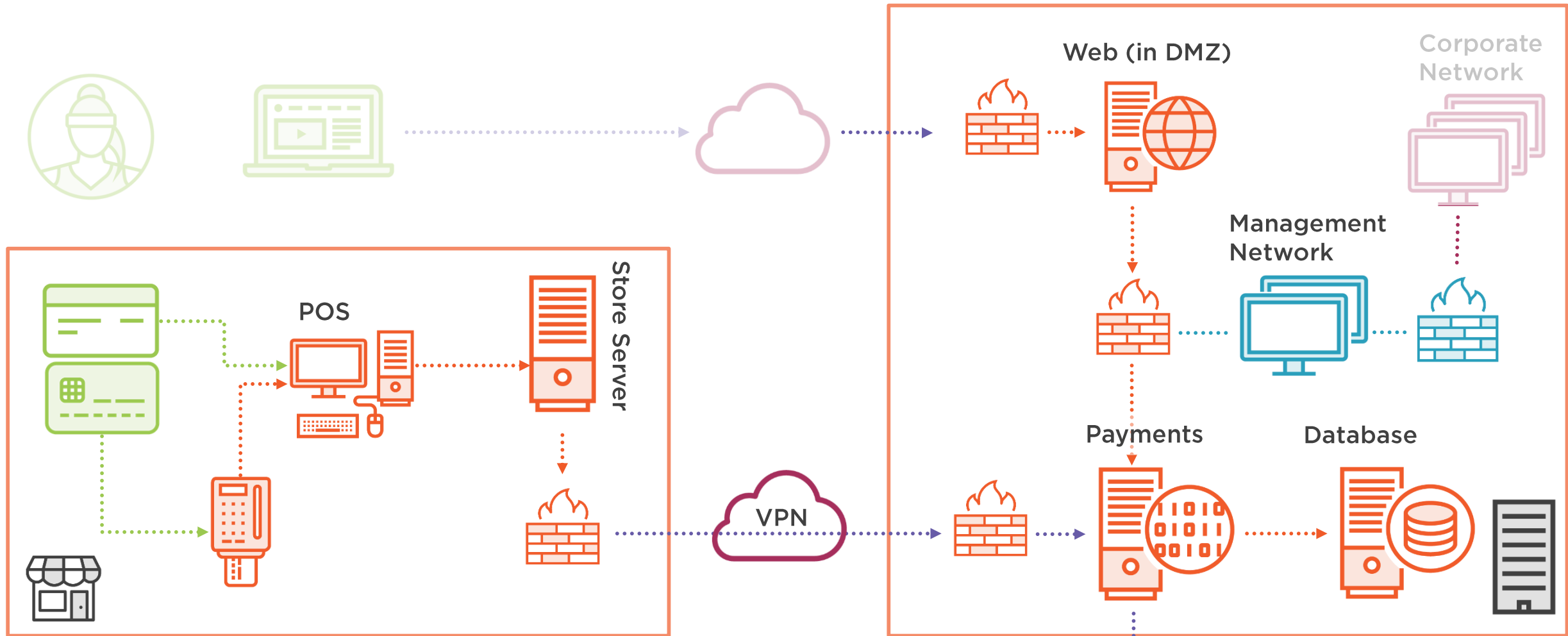
Secure and archive audit trails

Review logs and events and respond accordingly

Policies and procedures

\* Monitor the availability of critical security functions and respond to failures







# Requirement 10.1

Track user access to systems





## Requirement 10.1

Implement audit trails to **link** all **access** to system components to each **individual user**.



## Requirement Guidance

- It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

# 10.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe audit trails for system components</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>System administrators</b>





## Requirement 10.2

Implement automated audit trails  
to be able to reconstruct specific events.





## Requirement 10.2

Implement automated audit trails for **all system components to reconstruct** the following events:

See 10.2.1 through 10.2.7



## Requirement Guidance

- Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities



## 10.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe of audit logs, examine audit log settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 10.2.1

All individual user accesses to cardholder data



## Requirement Guidance

- Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.



## Requirement 10.2.2

All actions taken by any individual with **root or administrative privileges**



## Requirement Guidance

- Accounts with increased privileges, such as the “administrator” or “root” account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.



### Requirement 10.2.3

#### Access to all audit trails



### Requirement Guidance

- Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel.



## Requirement 10.2.4

Invalid logical access attempts



## Requirement Guidance

- Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to “brute force” or guess a password.





## Requirement 10.2.5

**Use of** and changes to **identification and authentication mechanisms**—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges



## Requirement Guidance

- Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.



## Requirement 10.2.5

Use of and **changes to identification and authentication mechanisms**—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges



## Requirement Guidance

- Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.



## Requirement 10.2.5

Use of and **changes to identification and authentication mechanisms—including** but not limited to **creation of new accounts and elevation of privileges—** and all changes, additions, or deletions to accounts with root or administrative privileges



## Requirement Guidance

- Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.





### Requirement 10.2.5

Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and **all changes, additions, or deletions** to **accounts** with **root** or **administrative** privileges



### Requirement Guidance

- Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.



## Requirement 10.2.6

Initialization, stopping, or pausing of the audit logs



## Requirement Guidance

- Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.



## Requirement 10.2.7

Creation and deletion of system-level objects



## Requirement Guidance

- Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system. By logging when system-level objects, such as database tables or stored procedures, are created or deleted, it will be easier to determine whether such modifications were authorized.

# System-level Object

Anything on a system component that is required for its operation, including but not limited to **database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.**





## Requirement 10.3

What each log entry should contain





### Requirement 10.3

Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

Who

What

When

How

Where

Where



### Requirement Guidance

- By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.



## 10.3 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	-	
<b>Examine records</b>	Y	Audit logs
<b>Interview people</b>	-	





## Requirement 10.4

Synchronize all critical  
system clocks and times.







#### Requirement 10.4

Using time-synchronization technology, **synchronize** all critical system **clocks** and **times** and ensure that the following is implemented for acquiring, distributing, and storing time.



#### Requirement Guidance

- Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

## 10.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Configuration standards and processes</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 10.4.1

The time on systems is correct





#### Requirement 10.4.1

Critical systems have the correct and consistent time.



#### Requirement Guidance

- Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

# Testing Procedure 10.4.1

10.4.1a  
Examine process to  
verify that:

**Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC**

10.4.1b  
Examine systems to  
verify that:

**Where there is more than one designated time server, the time servers peer with one another to keep accurate time,**

**Systems receive time information only from designated central time server(s)**





## Requirement 10.4.2

### **Time data is protected.**

10.4.2.a Examine *things* to verify that **access to time data is restricted to only personnel with a business need to access time data.**

10.4.2.b Examine *things* to verify that any **changes to time settings on critical systems are logged, monitored, and reviewed.**



## Requirement Guidance

- Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

## 10.4.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configurations, time-synchronization settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Time-synchronization logs</b>
<b>Interview people</b>	<b>-</b>	





## Requirement 10.4.3

Time comes from trusted sources.





### Requirement 10.4.3

Time settings are received from **industry-accepted time sources**.



### Requirement Guidance

- Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

## 10.4.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Systems configurations</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 10.5

Make sure audit trails can not be tampered with.



## Requirement 10.5

**Secure audit trails** so they cannot be altered.



## Requirement Guidance

- Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.

## 10.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configurations and permissions</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>System administrators</b>





### Requirement 10.5.1

**Limit viewing** of **audit** trails to those with a **job-related need**.



### Requirement Guidance

- Adequate protection of the audit logs includes strong access control (limit access to logs based on “need to know” only), and use of physical or network segregation to make the logs harder to find and modify.
- Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.



## Requirement 10.5.2

**Protect** audit trail **files** from unauthorized modifications.

Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.



## Requirement Guidance

- Adequate protection of the audit logs includes strong access control (limit access to logs based on “need to know” only), and use of physical or network segregation to make the logs harder to find and modify.
- Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.



### Requirement 10.5.3

Promptly **back up** audit trail files to a centralized log server or media that is **difficult to alter**.



### Requirement Guidance

- Adequate protection of the audit logs includes strong access control (limit access to logs based on “need to know” only), and use of physical or network segregation to make the logs harder to find and modify.
- Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.





#### Requirement 10.5.4

Write logs for **external-facing technologies** onto a secure, centralized, **internal log server** or media device.



#### Requirement Guidance

- By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.
- Logs may be written directly, or offloaded or copied from external systems, to the secure internal system or media.



### Requirement 10.5.5

Use **file-integrity monitoring** or change-detection software **on logs** to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).



### Requirement Guidance

- File-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise.

## 10.5.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System settings, monitored files</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Results from monitoring activities</b>
<b>Interview people</b>	<b>-</b>	





## Requirement 10.6

Review logs and events.





## Requirement 10.6

Review logs and security events for all system components to identify anomalies or suspicious activity.

*Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*



## Requirement Guidance

- Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.
- The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

## 10.6 Testing Procedures

<b>Observe/examine systems and settings</b>	-	See 10.6.1 through 10.6.3
<b>Examine documentation</b>	-	
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 10.6.1

Review important events  
and incidents every day.





## Requirement 10.6.1

**Review** the following at least **daily**:

1. All security events
2. Logs of all system components that store, process, or transmit CHD and/or SAD
3. Logs of all critical system components
4. Logs of all servers and system components that perform security functions



## Requirement Guidance

- Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of “security event” will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of “normal” traffic to help identify anomalous behavior.



## 10.6.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Processes</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Security policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 10.6.2

Review less important events  
and incidents “periodically”



## Requirement 10.6.2

**Review** logs of all other system components **periodically** based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.



## Requirement Guidance

- Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment.

## 10.6.2 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Security policies and procedures, risk-assessment documentation
<b>Examine records</b>	-	
<b>Interview people</b>	Y	Responsible people





## Requirement 10.6.3

Investigate things learned from log reviews.



### Requirement 10.6.3

Follow up **exceptions** and **anomalies** identified during the review process.



### Requirement Guidance

- If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.

## 10.6.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Processes</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Security policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 10.7

Retain audit trail / log files for a year.





## Requirement 10.7

**Retain** audit trail **history** for at least **one year**, with a minimum of **three months immediately available** for analysis (for example, online, archived, or restorable from backup).



## Requirement Guidance

- Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.

## 10.7 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Processes</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Security policies and procedures</b>
<b>Examine records</b>	<b>Y</b>	<b>Audit logs</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 10.8

**For service providers only**

Respond to breaches of availability of critical security systems.



## Requirement 10.8

### ***Service providers only:***

Implement a process for the timely detection and reporting of failures of critical security control systems, including:

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls



## Requirement Guidance

- Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.
- The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

## 10.8 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Detection and alerting processes</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Policies and procedures</b>
<b>Examine records</b>	<b>!</b>	<b>Incident logs</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 10.8.1

**For service providers only**

Respond to breaches of availability of critical security systems.



## Requirement 10.8.1

*Service providers only:*  
**Respond to failures** of any critical security controls **in a timely manner**.

**Processes** for responding to failures in security controls **must include** ...



## Requirement Guidance

- If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment.
- Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.

Processes for responding to failures in security controls must include ...

1. Restoring security functions
2. Identifying and documenting the duration (date and time start to end) of the security failure
3. Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause





Processes for responding to failures in security controls must include ...

4. Implementing controls to prevent cause of failure from reoccurring
5. Identifying and addressing any security issues that arose during the failure
6. Performing a risk assessment to determine whether further actions are required as a result of the security failure
7. Resuming monitoring of security controls



## 10.8.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Policies and procedures</b>
<b>Examine records</b>	<b>Y</b>	<b>Security control records</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





# Requirement 10.9

Policies and procedures.





## Requirement 10.9

Ensure that security **policies and procedures** for monitoring all access to network resources and cardholder data are **documented, in use**, and **known** to all affected parties.



## Requirement Guidance

- Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.



## 10.9 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Security policies, Operational procedures
<b>Examine records</b>	-	
<b>Interview people</b>	Y	Responsible people and people who need to know



# That's Fine in Theory

