

Requirement 12 Continued: Incident Response (12.10) BAU (12.11)



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com





Requirement 12.10

Have an incident response plan



Requirement 12.10

Implement **an incident** response plan.

Be prepared to respond immediately to a **system breach**.



Requirement Guidance

- Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities.

12.10 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Incident response plan Related procedures
Examine records	-	
Interview people	-	





Requirement 12.10.1

Create the **incident response plan** to be implemented in the event of system breach.

Ensure the plan addresses the following at a minimum:



Requirement Guidance

- The incident response plan should be thorough and contain all the key elements to allow your company to respond effectively in the event of a breach that could impact cardholder data.



What Goes in the Incident Response Plan?



Roles and responsibilities

How to inform the payment brands

Step-by-step procedures

Business recovery and continuity

Backup (and restore) processes

Other legal compliance requirements

- California Bill 1386, GDPR

Coverage of all critical components

12.10.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Incident response plan Incident reports
Examine records	Y	Historical incident
Interview people	Y	Responsible people





Requirement 12.10.2

Review and **test** the **plan**, including all elements listed in Requirement 12.10.1, at least **annually**.



Requirement Guidance

- Without proper testing, key steps may be missed, which could result in increased exposure during an incident.

12.10.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Testing documentation
Examine records	-	
Interview people	Y	Responsible people





Requirement 12.10.3

Designate specific personnel to be available on a 24/7 basis to respond to alerts.



Requirement Guidance

- Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become “polluted” by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.



Requirement 12.10.4

Provide **appropriate training to staff** with security **breach** response **responsibilities**.



Requirement Guidance

- Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become “polluted” by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.

12.10.3 & 12.10.4 Testing Procedures

Observe/examine systems and settings	Y	Incident response settings
Examine documentation	Y	Policies
Examine records	Y	Incident response records
Interview people	Y	Responsible people





Requirement 12.10.5

Include **alerts** from **security monitoring systems**,

including but not limited to

intrusion-detection,
intrusion-prevention,
firewalls, and file-integrity
monitoring systems.



Requirement Guidance

- These monitoring systems are designed to focus on potential risk to data, are critical in taking quick action to prevent a breach, and must be included in the incident-response processes.

12.10.5 Testing Procedures

Observe/examine systems and settings	Y	Processes
Examine documentation	Y	Processes Incident response plan
Examine records	-	
Interview people	-	





Requirement 12.10.6

Develop a **process** to **modify** and **evolve** the **incident response plan** according to **lessons learned** and to incorporate **industry developments**.



Requirement Guidance

- Incorporating “lessons learned” into the incident response plan after an incident helps keep the plan current and able to react to emerging threats and security trends.



12.10.6 Testing Procedures

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





PLURALSIGHT

Products ▾

Courses ▾

View plans

Resources ▾

Call us +441173741780



Sign in ▾

TRY FOR
FREE

PCI DSS: The State of Cardholder Data Attacks

By John Elliott and Aaron Willis

In this course, you'll learn about the criminals' ways of working from an experienced (PFI) Forensic Investigator and discover what actually happens in the course of a PCI forensic investigation.

START A FREE 10-DAY TRIAL

▶ PLAY COURSE OVERVIEW

Course Overview ^

Course Overview 2m

Understanding the Forensic Collection Process ^

🔒 Introducing the Authors and Their Backgrounds 2m

🔒 How Do You Know You've Been Breached? 1m

🔒 How Should a Breach Victim (Merchant) React? 3m

🔒 What Does the PFI Professional do First? 5m



Incident Response





Requirement 12.11

For Service Providers Only

Validate business-as-usual activities



Requirement 12.11

Additional requirement for service providers only:

Perform **reviews at least quarterly** to confirm personnel are **following security policies and operational procedures**.

- Daily log reviews
- Firewall rule-set reviews
- Applying configuration standards to new systems
- Responding to alerts
- Change management processes



Requirement Guidance

- *Note: This requirement applies only when the entity being assessed is a service provider.*
- Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.



12.11 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Policies and procedures
Examine records	Y	Records of reviews
Interview people	Y	Responsible people





Requirement 12.11

Additional requirement for service providers only:

Maintain **documentation** of quarterly review process to include:

1. **Documenting results of the reviews**
2. **Review** and **sign-off** of results by **personnel assigned responsibility for th PCI DSS compliance program**



Requirement Guidance

- ***Note:** This requirement applies only when the entity being assessed is a service provider.*
- The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity’s preparation for its next PCI DSS assessment.

12.11 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Quarterly review documentation
Examine records	-	
Interview people	!	The person signing it off



PCI in BAU

