Purpose: this document defines the procedure to follow in case of an actual or suspected cyber-attack or breach of information held or controlled by Accor SA or another entity of the Accor Group, including when such cyber-attack or breach originates in an entity operated under an Accor brand through a franchise or a management agreement.

SUMMARY

Revision	Date	Redacted by	Verified by	Approved by
0.1	Dec 2019	Data Team (based on previous PCI DSS Incident Response Plan)	MC Vittet	Data Team
1.0	30/03/2020	Thomas Elm	MC Vittet	Thomas Elm
1.7	31/3/2021	Marie-Christine Vittet		

1. INTRODUCTION

1.1. Context

Although Accor is taking the necessary steps to ensure protection of personal data (including cardholder data), the risk of a cyber-attack or a data breach still exists. Thus, Accor will strive to bring the best response should an incident occur.

Having a formalized procedure is also required by several personal data protection regulations in the world including by the European General Data Protection Regulation (GDPR) and worldwide by the Payment Card Industry Data Security Standards (PCI DSS) for cardholders' data - see **Appendix 9**. Under many regulations around the world it is mandatory to notify data breaches to data protection authorities, mainly when it implies personal data. It is also often mandatory to notify the concerned natural persons of such breach. For example:

- the GDPR requires such notification to be sent to the competent authority (no later than 72 hours after becoming aware of a breach) and to the natural persons, where the personal data breach is likely to result in a high risk to such natural persons;
- PCI DSS requires notifications to be sent to the schemes according to specific deadlines defined for each scheme.

Accor is committed to comply with these regulations and standards whether it concerns its clients, prospects, employees, or partners' data.

This Cyber-Attack/Data Breach Response Plan describes in detail the procedures that the various stakeholders within the organization must follow in case of a cyber-attack or a data breach.

If the criteria defined to qualify an event as a Country/Region or a Worldwide Crisis are met, this Cyber-Attack/Data Breach Response Plan may be accompanied by the Group's crisis management manual ("ALERT")[1].

1.2. Goals

The present document aims at defining the procedures that the various stakeholders within the organization must follow in case of a cyber-attack or a data breach. It provides the appropriate tools to identify and report alerts, qualify alerts as incidents and provide appropriate response (responsibilities, identification, incident plan, test and response steps).

This document must be known by all members of an Incident Response Team and by:

- All Business Owners (the person in charge of a given business activity) to ensure sufficient measures are taken in the event of an incident concerning their perimeter

[1] Accor guideLines & Emergency Response Tools: https://accor.sharepoint.com/Security

- Project Managers (PCI and GDPR)
- All support teams: Operations, Legal, Digital, Treasury, Risks & Insurances, Communication, etc.

1.3. Glossary of terms used

alert	Following items are considered as security alerts: - IT Security Alerts: ○ Intrusion Detection System (IDS) or File Integrity Monitoring (FIM) alert; ○ Unauthorized activity (invalid login attempt, unauthorized log deletion, etc.); ○ Unexpected network traffic; ○ Security and antivirus product malfunction; - Suspicious activities or actions of suspicious persons in connection with IT systems or any type of media containing information; - Guest complaints, regardless of the channel (customer care, social networks, hotels…). After investigation, an alert can turn either into a false positive or an incident.
application-specific procedure	The procedure presented in **Appendix 1** that Business Owners must use to document how they prepare for an incident in the context of a specific tool or activity under their responsibility.
Data Protection Officer or **DPO**	The position created by the GDPR and which primary role is to ensure that the organization processes the personal data of its staff, customers, providers or any other natural person in compliance with the applicable data protection rules and which acts as a point of contact with the data protection authorities.
GDPR	The regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Incident	A personal data breach, meaning a breach of security leading to either: - the accidental or unlawful destruction of… - the accidental or unlawful loss of… - the accidental or unlawful alteration of… - unauthorized disclosure of… - unauthorized access to… personal data transmitted, stored or otherwise processed. Examples: - Personal data (such as usernames, passwords or purchases history) are published online by an attacker; - Personal data have been stolen or lost on a physical media (paper, IT device, backup material, etc.); - Personal data have been stolen using social engineering or tampered device (tampered payment terminal for example); - An alert is raised by a third party (data protection authority, service provider, bank, etc.); - An email is sent to several recipients in "to:" or "cc:" field, thereby all recipient can see the email address of other recipient.

	For PCI DSS specifically, incident means a system or data breach such as: - Printed cardholder data stolen (merchant tickets, fax); - Cardholder data stolen using social engineering (scam); - Physical attacks using skimmers or tampered payment terminal; - Server or computer intrusion inside PCI DSS perimeter, stolen server; - Any alert raised by a card scheme or acquiring bank; - Any alert qualified by IT Security as security incident; - Any incident raised by third party (Call Centers, PMS Providers); - Unauthorized wireless device (wifi, 3G/4G, etc.) in the PCI environment.
Incident Report Sheet or IRS	The document presented in **Appendix 3** centralizing all information on an incident and serving as a basis for communication between stakeholders.
Incident Response Team	The team as described in **Appendix 4** in charge of handling incidents and coordinating all actions in order to bring appropriate response to an incident.
PCI DSS	The current version in force of the Payment Card Industry Data Security Standard (V3.2.1 as of June 2018).
PCI Project Manager	The position which primary role is to lead and coordinate the PCI DSS compliance program. This position works closely to support other departments to manage PCI, to coordinate the annual assessment process and also with the worldwide community to follow local Headquarters and Hotels compliance.

1.4. Roles and responsibilities

To prevent incidents and to address them as they occur, the following responsibilities have been identified:

ROLES	RESPONSIBILITIES
Business Owner (the person in charge of a given business activity) **Operations** (countries/hotels)	Specify measures to take to prevent and react to incidents (log requirements, impact on individuals in case of data breach, business specific containment measures and communication channels), by using the application-specific procedure where the case may be. Regularly test measures taken to prevent and react to incidents. Report any alert and keep track of reported alerts. Collect information on all alerts and incidents. Prepare corrective actions to take. Participate to the Incident Response Team.
IT Leader	Implements log requirements and specific response mechanisms (password reset, etc.). Provides assistance to IT Security team (diagnostic, data gathering, containment, etc.). Applies recommendations (containment, eradication & recovery). Communicates and inform IT Security team. Collects information on all alerts and incidents. Prepares corrective actions to take. Participates to the Incident Response Team.

IT Security team	Monitors IT security alerts on a 24/7 basis. Runs diagnostic: removes false positives, determines the nature and scope of the incident. Recommends containment measures. Prepares written summary of the incident and correctives actions taken. Gathers evidence of the data breach. Recommends eradication & recovery steps. Participates to the Incident Response Team.
DPO	Assists in the qualification of an alert and the assessment of the severity of an incident. Notifies the data protection authority(ies) (ex. CNIL in France) when needed or liaises with local relays for such notifications. Assists in the notification of the incident to the concerned natural persons if the case may be. Participates to the Incident Response Team.
Legal	Provides assistance in measuring legal risks associated with the incident. Provides assistance for the exercise or defense of legal claims. Participates to the Incident Response Team.
Communication team	Monitors relations with Press / Media (Q&A, talking point, press communication, financial communication, internal communication). Assists in the elaboration of communication to the relevant audience (ex. internal or external). Communicates to data subjects when needed. Prepares and validates reporting to schemes with treasury. Participates to the Incident Response Team.
Risk and Insurance team	Assists in the risk assessment and the response plan. Triggers insurance policies when appropriate. Participates to the Incident Response Team.
Audit team	Ensures the existence of the incident procedure and its application.
Incident Response Team	Provides advice in the event of an alert. Gathers when an incident is confirmed. Takes decisions on the course of actions based on the incident.
Safety	Monitors security alerts on a 24/7 basis. If incident is related to a physical security issue, gathers evidences (access control logs and camera recordings), recommends containment measures, eradication & recovery steps, and prepares written summary of the incident and correctives actions taken. Contacts law enforcement when appropriate.

Roles and responsibilities for PCI DSS specifically:

ROLES	RESPONSIBILITIES

Payment & Fraud	Communicates central messages with hotels and 3rd parties.
Call Centers (third parties)	Exchange information with Accor and implement their own Cyber-Attack/Data Breach Response Plan.
Treasury	Communicates with Acquirers and Card Schemes in case of data breach involving payment card numbers. Participates to the Incident Response Team when payment card numbers are involved.

N.B.: the application-specific procedure can be used to add roles and responsibilities if needed.

2. INCIDENT RESPONSE Framework – NIST 800-61 Based

2.1. Preparation

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, we also try to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert stakeholders whenever incidents occur.

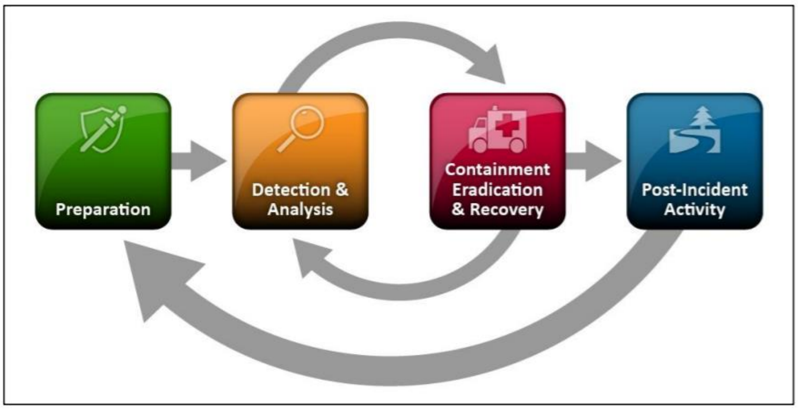


Figure 3-1. Incident Response Life Cycle

2.1.1. Preparing to handle incidents

The lists below provide examples of tools and resources available that may be of value during incident handling. These lists are intended to be a starting point:

- **Contact information for team members and others within and outside the organization** (primary and backup contacts), such as law enforcement and other incident response teams;

- **Incident reporting mechanisms**, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents;

- **Issue tracking system** for tracking incident information, status, etc. aside from emails and messaging solutions;

- **Traceability and logs**, Logs are used to explain anomalies, identify suspicious behaviors, understand the processes of an application. When an event is detected, the IT Security team must be able to use logs to track and identify the root cause. Logs also help to know the persons exposed to the data breach, and thus who will need to be contacted as part of the incident communication process.

- ***"DS-EA - RECO - Log Management Principles"****: description and specification of log requirements, with recommendation on log management solutions;*
- ***"Security in Project", paragraph 9 "Logs"****: specification on connection logs.*

*2.1.2.*Training the incident response team

All employees in contact with personal data must be trained appropriately and on a yearly basis to ensure proper handling of data and reduce the likelihood of accidental deletion, modification or transmission of data. Individuals must take reasonable precautions to protect personal data from deletion, modification, loss, or any kind of unauthorized action.

Employees in contact with personal data and Incident Response Team must be aware of security measures contained in this Cyber-Attack/Data Breach Response Plan, the APACHE procedure and the major steps to be taken in case of an incident. The application-specific procedure can be used to document the initial communication of the incident response plan, the last training date, etc.

2.2. Detection and analysis

2.2.1.Attack Vectors

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. We should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use **common attack vectors**. Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific procedures.

- **External/Removable Media**: An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.

- **Web**: An attack executed from a website or web-based application.

- **Email**: An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

- **Data exfiltration**: An attack executed with the objective to steal or take ownership over business or proprietary data – for example, clients' data or preferences.

- **Impersonation**: An attack involving replacement of something usual (common tool or software) with something malicious.

- **Third-Party Services**: An attack involving a third-party that provides services to the entity – for example, compromised software or tooling.

Other: An attack that does not fit into any of the other categories. This section focuses on recommended practices for handling any type of incident.

2.2.2. Signs of an Incident

The most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

Employees must be aware of their responsibilities in detecting security alerts to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their areas of responsibility. Some examples of security alerts that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from security guard, video evidence of a break-in or unscheduled/unauthorized physical entry);
- Fraud – Inaccurate information within databases, logs, files or paper records;
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals);
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, physical security alarms such as fire alarms, environmental alarms, natural disaster alerts).

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations ➔ **In all cases, every employee should report alerts to his management as soon as possible in order to launch immediate corrective actions or inquiries.**

An APACHE "Good practice sheet" has been set up for hotels to explain to hotel employees who to alert and how to manage the first moments when suspecting a cyber-attack or a data breach[2].

2.2.3. Incident Analysis

Incident detection and analysis would be easy if every indicator were guaranteed to be accurate; unfortunately, this is not the case. Performing the initial analysis and validation is challenging. In case of any alert it is imperative that all appropriate investigative or corrective action be taken by the manager receiving the alert notification to assure the integrity of the investigation and recovery process.

When faced with a potential situation the manager should do the following:

- Attempt to determine if the alert justifies a formal incident response:
  - **If so, or in case of any doubt about the qualification as incident, take a direct contact with a member of the appropriate Incident Response Team as identified in Appendix 4;**
  - If the alert does not require an incident response, the situation will be forwarded to the appropriate area to ensure that all support services required are rendered (helpdesk, operational management, etc.);
- If the alert involves a compromised computer system:

[2] Cyber-Attack / Data Breach: https://accor.sharepoint.com/Security/Lists/AccorDocument/CRISISMANAGEMENT/THEHOTELSCRISISMANAGEMENT/GOODPRACTICESHEETS/Cyber%20Attack%20EN%20VF.pdf

- do not alter the state of the computer system; keep the computer system on and leave all currently running computer programs as is ➔ **do not shutdown the computer or restart the computer**;
- immediately alert IT department and follow their advices ➔ **do not take actions on your own**; in particular do not disconnect systems from network before being told to do so;

- Ensure that no one communicates with anyone outside of the Manager or the Incident Response Team about any details or generalities surrounding any suspected or actual incident. If the alert was qualified as actual incident, all communications with law enforcement or the public will be coordinated by the Incident Response Team;
- Document any information while waiting for the Incident Response Team to respond to the incident. This must include date, time, and the nature of the incident, if known. Any information the Manager can provide will help in responding in an appropriate manner ➔ **use the Report on Initial Observations Template in Appendix 2**;
- Remain available for any solicitation by the Incident Response Team.

2.2.4.Incident Qualification

Incident Response Team should first confirm the qualification of the alert as an incident. If it turns that the alert does not require an incident response, the situation will be forwarded to the appropriate area to ensure that all support services required are rendered (helpdesk, operational management, etc.). If the qualification as an incident is confirmed by the Incident Response Team, the latter measures the severity of the incident.

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- **Functional Impact:** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.

Category	Definition
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

- **Information Impact:** Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations.

Category	Definition
Low	
"Integrity Loss"	Unclassified information was changed or deleted on corporate non-critical systems or resources.
"Proprietary Breach"	Unclassified proprietary information were accessed. Examples: • Disclosure of non-sensitive guests preferences for a limited number of individuals.
Medium	
"Proprietary	Unclassified proprietary information were exfiltrated.

Breach”	Examples : • Successful attempt to obtain unauthorized information or access (e.g. attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, unauthorized wireless access point detected, etc.).
“Integrity Loss”	Sensitive or proprietary information was changed or deleted on corporate non-critical systems or resources.
High	
“Privacy Breach”	Sensitive personally identifiable information (PII – GDPR), credit card data (PCI DSS), employees, beneficiaries, etc. was accessed or exfiltrated. Examples: • Actual breach of security (e.g. multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.). • A third party having access to compromised data will be able to directly identify specific individuals.
“Proprietary Breach”	Classified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated.
“Integrity Loss”	Sensitive or proprietary information was changed or deleted on corporate critical systems or resources.

- **Recoverability Impact:** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

Category	Definition
Low	
“Regular”	Time to recovery is predictable with existing resources.
Medium	
“Supplemented”	Time to recovery is predictable with additional resources.
High	
“Extended”	Time to recovery is unpredictable; additional resources and outside help are needed
“Not Recoverable”	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly). A formal investigation need to be performed.

Important: in case of an incident impacting several factors, the maximum category level “Low, Medium or High” must be considered between all of these.

For the operational treatment, the « IT Security IRP » outlines the «Incident Prioritization » along with target recovery time in each case: https://confluence.accor.net/display/SECURITYPUB/Incident+Response+Management

2.2.5. Incident Notification

When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Please, review **Appendix 4** for more details.

2.2.5.1 Communication and press releases, legal actions or defenses, insurance claims and other actions

Within the Incident Response Team, the following stakeholders are involved and must take any appropriate action in accordance with their field of expertise:

- Communication Team
  - Manages external communication actions, including notification to concerned data subjects (see section **Error! Reference source not found.**)
  - Manages any media coverage by drafting press statement
- Legal Team
  - Assesses legal actions to be launched
  - Assists Business Owner in its relation with authorities (police department…)
- Insurance Team
  - Takes care of claim notifications to insurance companies
  - Manage relationships with insurance companies

2.2.5.2 Special notification: PCI DSS

For any data breach involving payment card information, according to PCI DSS, the **Incident Response Team** will use the following procedure:

- Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
  - Log all actions taken (e.g., written, video camera, etc.)
  - Utilize chain of custody techniques during all transfers of equipment and information related to the incident
  - Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT)
  - Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g. unplug the network cable, deactivate switch port, isolate to contained environment e.g. isolated VLAN). Utilize Disaster Recovery / Business continuity procedures to recover business processes
  - Preserve logs and electronic evidence
  - If using a wireless network, change SSID (Service Set Identifier or wireless network name) on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised)
  - Be on high alert and monitor all cardholder information systems
- Alert all necessary parties. Be sure to notify:
  - Internal or External Incident Response Team or Forensics Team, if they are not already involved
  - Merchant bank (hotel contacts its bank)
  - Law Enforcement
- Follow appropriate procedures for each card scheme: which Accor utilizes for credit card services (See **Appendix 7**)

About PFI – PCI DSS Forensics Investigation

Entity must initiate investigation of the suspected or confirmed loss or theft of account information **within 24 hours of compromise**. The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk: Number of accounts at risk, identify those stored and compromised. Identify type of account information at risk (Account number, Expiration date, Cardholder name, Cardholder address, CVV2, Track 1 and Track 2), any data exported by intruder.
2. Perform incident validation and assessment
    a. Establish how compromise occurred
    b. Identify the source of the compromise
    c. Determine timeframe of compromise
    d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections
    e. Determine if compromise has been contained
3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.)
4. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed
5. Perform remote vulnerability scan of entity's Internet facing site(s)

2.2.5.3 Special notification: GDPR

According to the GDPR, the **scheme[3] in Appendix 8** must be followed to assess the necessity to notify an incident to a data protection authority and, if the case may be, to the affected data subjects.

Notification to data protection authorities:

If the incident involves a data processing activity **under the control of Accor SA**, the French data protection authority (the "CNIL") must be notified of the breach. As a reminder, the CNIL has been designated as the lead data protection authority for Accor.

In accordance with GDPR, the notification to a European data protection authority should be performed as follows:

- Where feasible, the personal data breach must be notified to the data protection authority **within 72 hours after having become aware of the data breach**, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

  Unless specific circumstances, an incident of medium or high severity according to the table in section **Error! Reference source not found.** should always be notified to the data protection authority; in case of an incident of low severity according to the same table, the Incident Response Team will perform an *in concreto* analysis and decide whether the incident is likely to result in a risk for natural persons or not;

[3] Source: Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)

- Where the notification to the data protection authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- Elements included in the notification should:
  - Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
  - Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
  - Describe the likely consequences of the personal data breach
  - Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Please refer to **Appendix 5** for a step-by-step description of how to notify the data breach to the CNIL.

In case of an incident involving a trans-border data processing activity targeting data subjects in several European or non-European countries, the Incident Response Team analyses potential other notification duties according to the applicable regulations.

If the incident involves a data processing activity where **Accor SA is acting as a processor** (i.e. where it processes personal data on behalf of a data controller), then Accor SA must notify the controller of the incident without undue delay after becoming aware of a personal data breach. This notification should include all information as listed above in order for the data controller to comply with its own notification duties.

Notification to the affected data subjects:

In accordance with GDPR the data controller is required to notify the affected data subjects in the case of an incident, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Unless specific circumstances, an incident of high severity according to the table in section 3.3.1 above should always be notified to the affected data subjects; in case of an incident of low or medium severity according to the same table, the Incident Response Team will perform an *in concreto* analysis and decide whether the incident is likely to result in a high risk for natural persons or not;

The notification should, in clear and plain language:

- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

This notification is prepared with the support of the Communication team. In all cases the notification should make reference to the measures described in **Appendix 6** that data subjects can take to mitigate possible adverse effects depending on the kind of information involved in the incident.

Communication to the impacted data subjects is not required if any of the following conditions are met:

- The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The relevant data protection authority may decide to classify the incident as high risk and require communication to be made, or that communication is not necessary if one of the conditions above is met.

2.3. Containment, Eradication and Recovery

2.3.1. Choosing a Containment Strategy

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored **remediation strategy**. An essential part of containment is decision-making (e.g. disconnect it from a network, and disable certain functions). Criteria for determining the appropriate strategy include:

- Need for evidence preservation.
- Service availability (e.g. network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy (e.g. partial containment, full containment)
- Duration of the solution (e.g. temporary workaround to be removed in two weeks, permanent solution).

2.3.2. Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal or investigation cases. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer.

2.3.3. Identifying the Origin

During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming process that can prevent a team from achieving its primary goal—**minimizing the business impact**.

Creating a Root Cause Analysis Map

This connects individual cause and effect relationships to reveal the root cause of the incident. At a high level, the cause map helps to create a visual representation of the event by determining the following:

- What happened?
- Why it happened?
- What to do to reduce the likelihood of it happening again?

Of course, each of these steps requires careful and objective analysis. This must be performed by those with both subject matter expertise (SME) and background knowledge of the circumstances leading up to the incident

2.3.4. Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected assets within the organization so that they can be remediated.

For some incidents, eradication is either not necessary or is performed during recovery. In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions.

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents.

Examples on Containment, Eradication and Recovery

Below some examples on reaction taking into account the outlined steps in section "2.3".

Incident #1: theft of company unclassified proprietary data (Medium)

- Containment strategy
  - Conduct an IT check to monitor and contain the breach:
    - If possible, record details about the intruder identity (when speaking about an IT incident, details can be: user ID, IP address, computer name)
    - Use approved controls to temporarily or permanently block the intruder's access
- Evidence gathering and handling
  - Collect evidences (logs and traces) to accurately identify all events on systems.
  - Gather evidences related to impacted or suspicious user accounts.
- Eradication and recovery
  - Review involved assets and ensure that such attack vector can't be similarly exploited.
  - Maintain vigilance for future break-in attempts from this user or IP address.

Incident #2: theft of company personal customer's data (High)

- Containment strategy
  - Contain the intrusion and decide what action to take; consider unplugging the network cables, applying highly restrictive ACLs (Access Control List), deactivating or isolating the switch port, deactivating the user ID, terminating the user's session/change password etc.; consider ceasing all business operations linked to the application
- Evidence gathering and handling
  - Collect and protect information associated with the intrusion via offline methods; for IT security incidents occurring from the Internet, request assistance from the Internet Service Provider (ISP) to get more information; appropriate teams (IT, Legal, Security) will be involved to identify forensic needs and coordinate appropriate forensic specialists; contact law enforcement when applicable
  - Research potential risks related to or damage caused by intrusion method used

- Eradication and recovery
  - Cease contract with the contractor, in case of an external application, until it enhances its security
  - Immediately notify management of the situation and maintain notification of progress at each step

The Incident Response Team is in charge of documenting the incident and all actions taken in the Incident Report Sheet using the template in **Appendix 3**.

2.4. Post-Incident activity

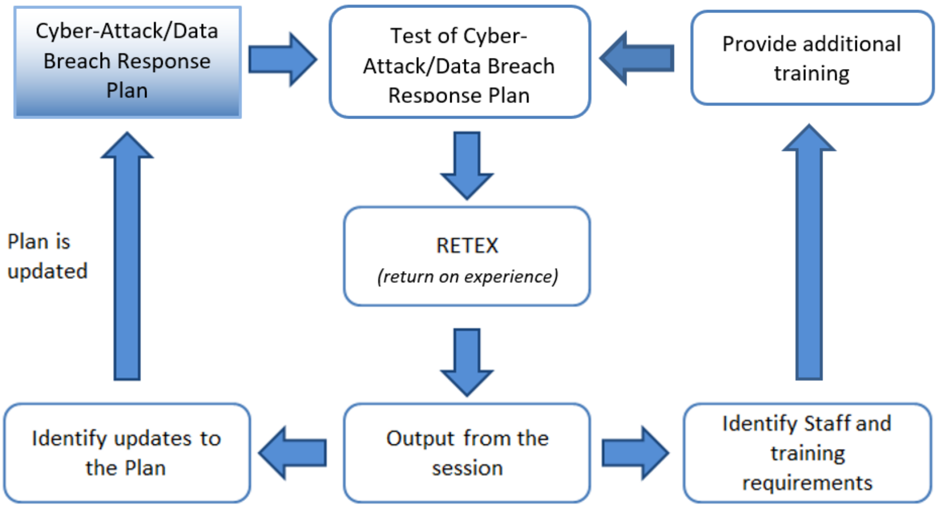
2.4.1. Lessons Learned

One of the most important parts of incident response is also the most often omitted: learning and improving. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically, can be extremely helpful in improving security measures and the incident handling process itself. Examples of useful questions:

- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What indicators should be watched for in the future to detect similar incidents?

2.4.2. Annual testing and review

The following Cyber-Attack/Data Breach Response Plan should be tested and reviewed annually to ensure that everyone is aware of the actions and contact points in case of an incident.


Cyber-Attack/Data Breach Response Plan
Test of Cyber-Attack/Data Breach Response Plan
Provide additional training
Plan is updated
RETEX
(return on experience)
Identify updates to the Plan
Output from the session
Identify Staff and training requirements

The Business Owners and IT Leaders are responsible for the frequent testing of their application and must be available for exercises organized by the Incident Response Team. The test must be recorded to ensure that an effective debrief can occur. The return on experience (RETEX) will help to identify improvements to the plan, staff training and overall process. The following template can be used:

Incident	Date and time	Person expected to respond	Expected response	Who responded?	Description of the response	Lessons learned
<<incident description>>	<<date & time>>	*<<name of the team or person that is expected to handle the incident>>*	*<<description of the expected actions, according to this Cyber-Attack/Data Breach Response Plan>>*	*<<who did actually handled the incident during the test>>*	*<<short description of actions performed>>*	*<<Was the response appropriate or did the test highlighted something to fix>>*
			Examples			
Stolen payment terminal in hotel Hxxxx	*15th may 2018*	*Hotel employee*	*Alert hotel GM*	*Front desk employee*	*Mentioned the incident during hotel team meeting*	*OK*
		Hotel GM	*Contact country security manager*	*Hotel GM*	*Explained the issue to the security manager by email*	*OK*
		Security manager	*Qualify incident, contain, monitor & warn*	*Security manager*	*Informed the hotel GM that it was an exercise. Report sent to the central incident response team. "Stolen" terminal sent back to the hotel*	*Forgot to gather video recordings*
Critical file modified on the e-commerce server	*15th May 2018 16:06 GMT*	*IT security team*	*Qualify incident*	*IT security team*	*Checked that no modifications where planned on the server. Raised alert to the project team.*	*OK*

		Project team	*Coordinate containment methods*	*E-Commerce project manager*	*Production traffic migrated to backup site. Suspected server removed from the production pool and request sent to security team to cut the network flows at firewall level*	*OK*
		IT security team	*Collect and protect forensic evidence. Communicate with management. Identify intrusion source.*	*IT security team*	*All relevant logs were extracted. Inform other teams that it was an exercise.*	*Discovered that some logs where missing on the log centralization server.*

APPENDIX 1
APPLICATION SPECIFIC PROCEDURE TEMPLATE

Appendix 1 -
Application Specific Pı

APPENDIX 2
REPORT ON INITIAL OBSERVATIONS TEMPLATE

Appendix 2 - Report on initial obsevations

APPENDIX 3
INCIDENT REPORT SHEET TEMPLATE

Appendix 3 - Incident
Report Sheet Templat

APPENDIX 4
INCIDENT RESPONSE TEAMS

Appendix 4 - Incident Response Teams.docx

APPENDIX 5
TEMPLATE OF NOTIFICATION TO THE FRENCH DATA PROTECTION AUTHORITY (CNIL)

Appendix 5 -
Template of notificiati

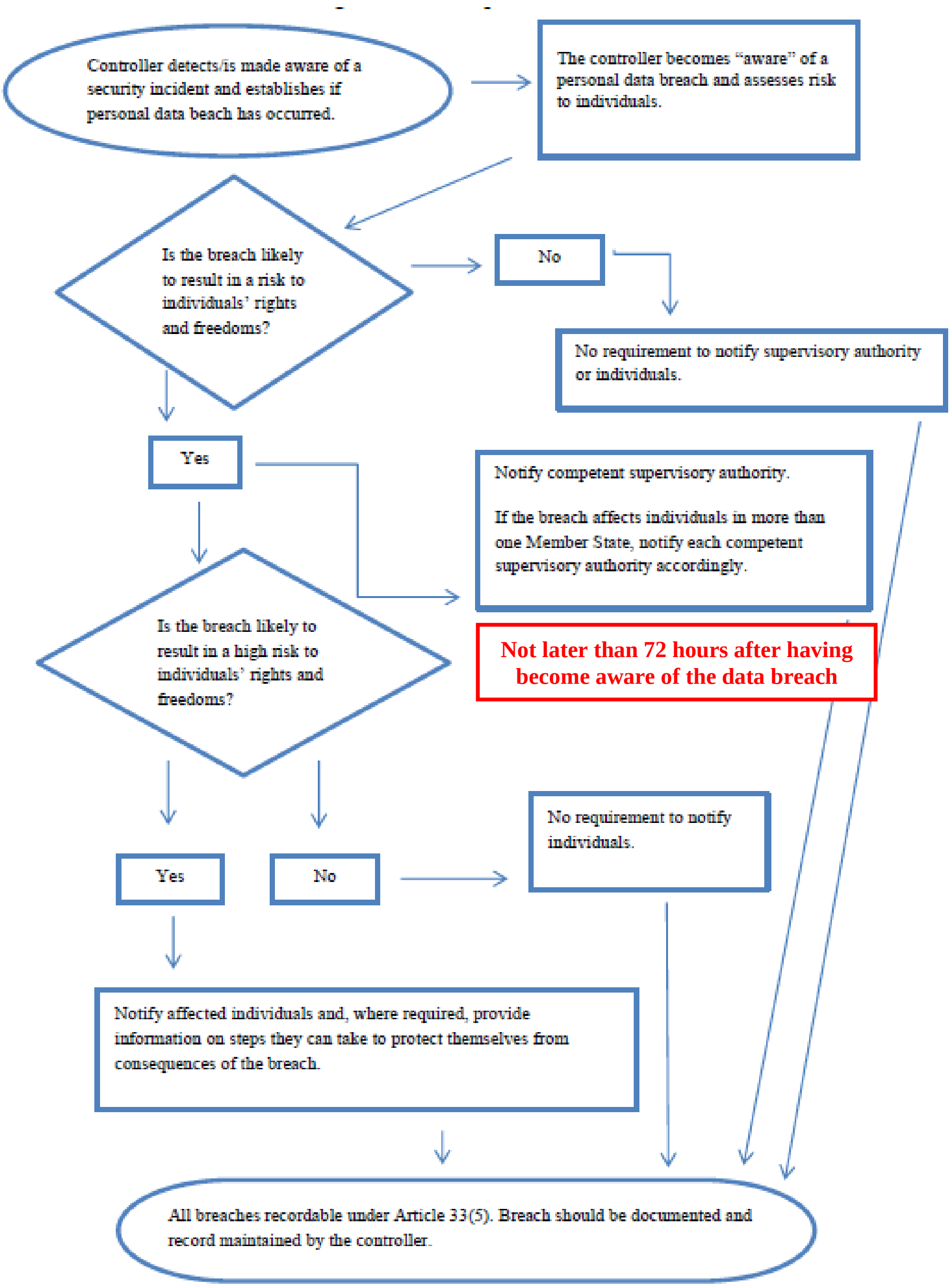
APPENDIX 6
MEASURES TO BE TAKEN BY AFFECTED DATA SUBJECTS

Appendix 6 - Measures to be taken

APPENDIX 7
CONTACTS OF CARD SCHEMES USED BY ACCOR FOR CREDIT CARD SERVICES

Appendix 7 -
Contacts of card scher

APPENDIX 8
Guidelines on Personal data breach notification under Regulation 2016/679


Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.
The controller becomes "aware" of a personal data breach and assesses risk to individuals.
Is the breach likely to result in a risk to individuals' rights and freedoms?
No
No requirement to notify supervisory authority or individuals.
Yes
Notify competent supervisory authority.
If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.
Not later than 72 hours after having become aware of the data breach
Is the breach likely to result in a high risk to individuals' rights and freedoms?
Yes
No
No requirement to notify individuals.
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.
All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

APPENDIX 9
GDPR & PCI DSS REQUIREMENTS

1. GDPR Requirements

Article 4
Definitions

For the purposes of this Regulation:

(…)

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(…)

Article 33
Notification of a personal data breach to the supervisory authority

1.In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34
Communication of a personal data breach to the data subject

1.When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2.The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3.The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

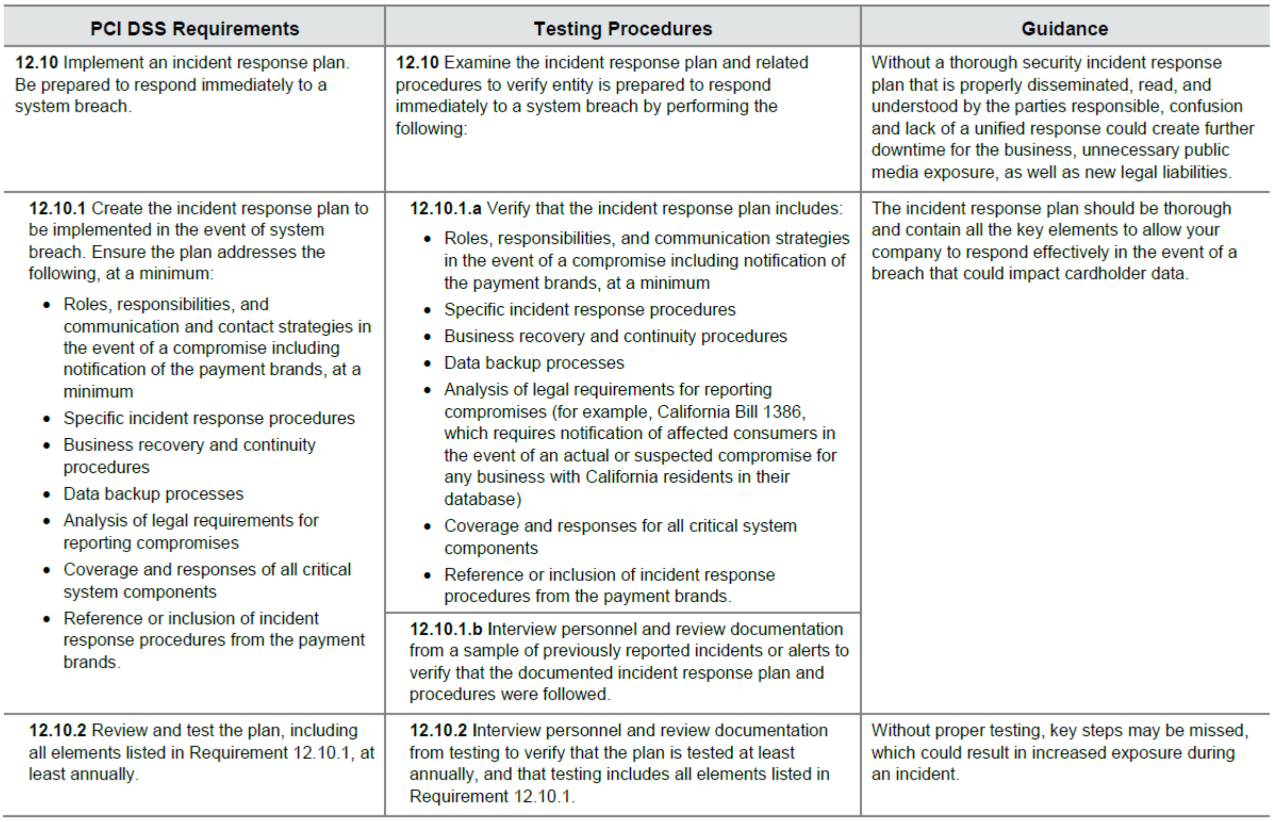
(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

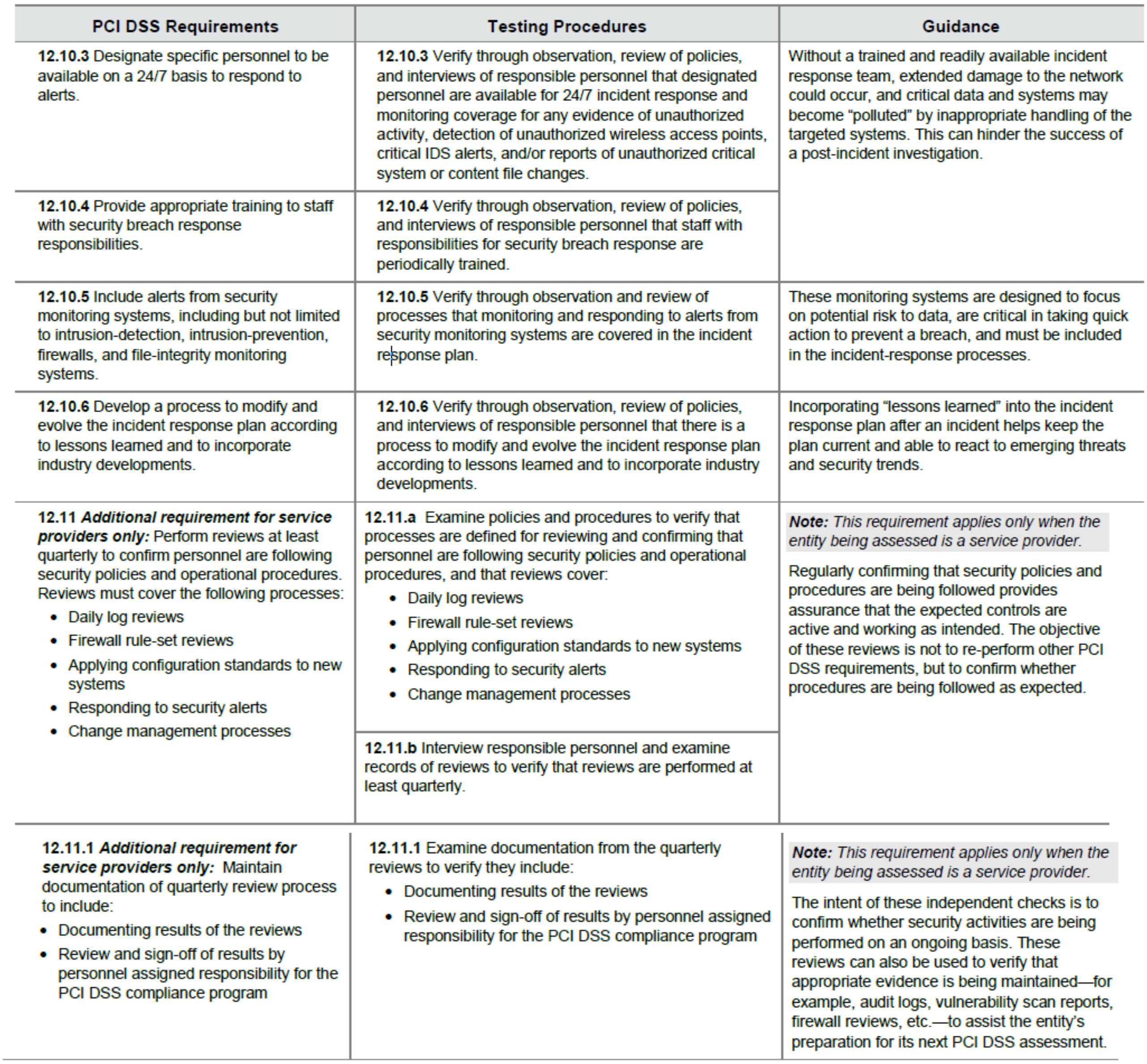
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

2. PCI DSS Requirements



PCI DSS Requirements	Testing Procedures	Guidance
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	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.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	**12.10.1.a** Verify that the incident response plan includes: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) • Coverage and responses for all critical system components • Reference or inclusion of incident response procedures from the payment brands.	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.
	12.10.1.b Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	**12.10.2** Interview personnel and review documentation from testing to verify that the plan is tested at least annually, and that testing includes all elements listed in Requirement 12.10.1.	Without proper testing, key steps may be missed, which could result in increased exposure during an incident.



PCI DSS Requirements	Testing Procedures	Guidance
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	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.
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	**12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained.	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the incident response plan.	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.
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	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.
12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	**12.11.a** Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	***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.b Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.	
12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	**12.11.1** Examine documentation from the quarterly reviews to verify they include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	***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.

Source PCI DSS standard version 3.2.1

End of the document