

Preparation for Handling Cloud Security Incidents

Note: Prior to starting the preparation to handle cloud security incidents, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 3: Checklist for CCs and CSPs to Handle Cloud Security Incidents	
Actions	Completed
Whether an SLA is crafted with a clear division of incident handling responsibilities based on the type of service and attack	<input type="checkbox"/>
Whether the SLA includes provisions for gathering or obtaining the required data to contain and eradicate incidents	<input type="checkbox"/>
Whether the responsibilities of the CC and CSP are mentioned in the SLA during and after an incident according to the type of service	<input type="checkbox"/>
Whether the incident response plans and policies are devised according to the SLA	<input type="checkbox"/>
Whether the incident response objectives are determined after consulting with stakeholders, legal advisors, and organizational leaders	<input type="checkbox"/>
Whether the team members have experience in handling cloud environments	<input type="checkbox"/>
Whether the roles and responsibilities of team members are defined for security incident response	<input type="checkbox"/>
Whether the members are trained in handling cloud security incidents through mock drills	<input type="checkbox"/>
Whether the employees are trained regarding safe usage practices and proper reporting of security incidents	<input type="checkbox"/>
Whether a knowledge base for the IR team is maintained on various cloud file formats and the team is prepared to use different tools to convert and analyze virtual memory files	<input type="checkbox"/>
Whether the tools and resources required to handle cloud security incidents are gathered	<input type="checkbox"/>
Whether a proper incident response team is built for CCs and CSPs that may work closely for improved incident response	<input type="checkbox"/>
Whether regular backups of critical data are created on the CC and CSP sides, including databases, applications, and logs	<input type="checkbox"/>

Whether the communication channels are defined with a contact list of incident response team members	<input type="checkbox"/>
Whether exchange of incident data between CCs and CSPs is agreed and the format and means of exchange are decided	<input type="checkbox"/>
Whether the details of changes, security measures, incident response testing, and other activities that may impact the cloud are exchanged	<input type="checkbox"/>
Whether the members are provided with training and proper practice and equipped them with tools that are required to handle cloud security incidents	<input type="checkbox"/>
Whether a forensics lab is created for analyzing and validation of security incidents. Additionally, whether it is ensured that the lab has the updated tools that are required to extract, analyze, and validate the forensics data	<input type="checkbox"/>
Whether the IH&R teams properly documented the incident response process, maintained the chain of custody for evidentiary data, and created detailed reports	<input type="checkbox"/>
Whether the cloud disaster recovery and backup services are established to quickly restore the affected systems	<input type="checkbox"/>
Whether copies of logs, snapshots, and other evidence are kept in a centralized cloud account	<input type="checkbox"/>
Whether it is ensured that the response mechanisms can be executed multiple times if necessary	<input type="checkbox"/>
Whether automation is implemented after identifying repetitive cloud security incidents, and human response is used only for unique and critical incidents	<input type="checkbox"/>
Whether the cloud services inventory, service components, corresponding service model, and deployment model are identified and prepared	<input type="checkbox"/>
Whether a tracking system is implemented to record and track the incident status	<input type="checkbox"/>
Whether the third-party threat intelligence services are utilized to understand potential incidents	<input type="checkbox"/>
Whether an automated system is created for providing support and distributing information	<input type="checkbox"/>

Section 4: Checklist for Cloud Service Providers (CSPs)	
Actions	Completed
Whether distributed storage is used for the cloud and all databases are placed at different geographical locations	<input type="checkbox"/>
Whether multiple databases are prepared to store copies of the data and proper backup and recovery systems are used	<input type="checkbox"/>
Whether separate IH&R teams are assigned at different geographical locations with the required tools and equipment	<input type="checkbox"/>
Whether the IH&R teams are provided with proper communication channels, including teams at distant locations	<input type="checkbox"/>
Whether physical security monitoring and authentication systems are implemented to ensure authorized entries in every facility	<input type="checkbox"/>
Whether strict policies are framed regarding physical access to the cloud infrastructure	<input type="checkbox"/>
Whether alarms are installed in case of a physical security breach, disasters, and other physical threats	<input type="checkbox"/>
the logging is enabled on all devices, servers, networks, databases, OSes, and applications	<input type="checkbox"/>
Whether the syslog servers are employed to collect logs at a centralized location	<input type="checkbox"/>
Whether the security information and event management (SIEM) tools are installed to perform event correlation and alert the incident response teams in the event of an attack	<input type="checkbox"/>
Whether database activity monitoring (DAM), data leakage prevention (DLP), and log analysis tools are installed to simplify the detection of incidents	<input type="checkbox"/>
Whether it is ensured that the location of databases is never disclosed to the public or clients, unless necessary to prevent physical attacks or physical access events	<input type="checkbox"/>
Whether the backups of cloud data are created on various distant servers	<input type="checkbox"/>

Whether the lists of customers, brokers, and other parties related to a cloud premise are maintained along with the details of the services provided and deployment models	<input type="checkbox"/>
Whether the detailed reports are obtained from recent audits and the concerns of the auditor are highlighted	<input type="checkbox"/>
Whether the CC and CSP incident response teams coordinate to jointly detect, contain, and eradicate incidents	<input type="checkbox"/>
Whether the incident response process data along with updates, changes in configuration, and evidentiary data are shared between the CC and CSP IH&R teams	<input type="checkbox"/>
Whether security solutions are provided, and the chain of custody data is shared with clients	<input type="checkbox"/>
Whether it is ensured that the services comply with relevant international standards and laws in regions where the CSP stores data and clients operate	<input type="checkbox"/>
Whether provisions for clients and government agencies are made to perform forensic imaging of compromised systems and services in case of an attack	<input type="checkbox"/>
Whether there is constant monitoring of applications and infrastructure via proactive system and data scanning	<input type="checkbox"/>
Whether a robust business continuity plan (BCP) is provided to enhance resiliency to manage and recover from incidents	<input type="checkbox"/>

Section 5: Checklist for Cloud Consumers (CCs)	
Actions	Completed
Whether there is a list and regular audit of all services, accounts, virtual systems, applications, and other elements of the cloud governed by CCs	<input type="checkbox"/>
Whether the privileges of employees accessing the cloud are clearly mentioned	<input type="checkbox"/>
Whether the IH&R team is trained and mock cloud security incidents are performed for practice	<input type="checkbox"/>
Whether the tools are gathered and a forensics lab is built to detect and analyze cloud security incidents	<input type="checkbox"/>
Whether the critical data resources are sensitized and servers and databases stored in distant locations are used to create backups	<input type="checkbox"/>
Whether a contact list of the CSP IH&R team members is prepared for contact and report in case of an incident	<input type="checkbox"/>
Whether the CSP IH&R team is asked to discuss their response methodology, and an incident response strategy is created accordingly	<input type="checkbox"/>
Whether the critical assets, data, services, applications, and other aspects are identified for running the business	<input type="checkbox"/>
Whether the aspects of cloud such as clock synchronization, geographical location, new cloud resources, virtualization components, and data formats are considered during incident response	<input type="checkbox"/>
Whether the importance of data and its requirements are determined during the selection of cloud services and deployment model	<input type="checkbox"/>
Whether the service offers proper backup and recovery options along with damage protection and forensics support	<input type="checkbox"/>
Whether the incident response and handling are considered according to the type of service	<input type="checkbox"/>
Whether policies for access, authentication, and use of cloud services are framed and implemented across the organization	<input type="checkbox"/>

Whether the logs are enabled to record access time and duration, location of the user, IP and MAC addresses of systems used for access, network protocols, and other relevant information	<input type="checkbox"/>
Whether the backup of all cloud components is maintained in the IaaS model and it includes a backup for data stored in the cloud in the PaaS and SaaS models	<input type="checkbox"/>
Whether the incident response team is built with members having experience in handling cloud security incidents	<input type="checkbox"/>
Whether regular backups of critical data, systems, and applications are created	<input type="checkbox"/>
Whether logging is enabled on the systems and devices that are used to access the cloud services	<input type="checkbox"/>
Whether protective measures such as redundancy for critical processes, backup systems, intrusion detection and prevention systems, data integrity monitoring systems, antivirus, and vulnerability assessment solutions are defined	<input type="checkbox"/>
Whether internal documentation is verified for port lists, asset lists, network diagrams, and current network traffic baselines	<input type="checkbox"/>
Whether there is awareness of the CSP logging configuration and how it varies from on-premises logging	<input type="checkbox"/>

Section 6: Checklist for Handling Azure Cloud Security Incidents	
Actions	Completed
Whether an incidence response plan is established describing all stages of incidence response, including the roles of all individuals involved	<input type="checkbox"/>
Whether a naming system is employed to identify and prioritize Azure resources, specifically for the resources that manage sensitive data	<input type="checkbox"/>
Whether frequent tests on systems are conducted to determine the effectiveness of the incident response process in the Azure environment and the plans are updated accordingly	<input type="checkbox"/>
Whether the security incident contact information is provided to Microsoft Security Response Center (MSRC), which notifies on identifying a security-related issue	<input type="checkbox"/>
Whether the Continuous Export feature of Azure Security Center is used to export alerts into the incident response system	<input type="checkbox"/>
Whether the Workflow Automation feature in Azure Security Centre is used to generate automatic responses through “Logic Apps” to alerts and provides recommendations to secure resources	<input type="checkbox"/>
Whether awareness is created among the security team about the Azure platform and technology, such as identity protocols, tools, data sources, and logs to secure cloud assets	<input type="checkbox"/>
Whether accountability is assigned to speed up the process of cloud security decision-making	<input type="checkbox"/>
Whether personnel are assigned to monitor the security posture of the Azure environment regularly	<input type="checkbox"/>
Whether the incidence response plans and playbooks are established considering the applications and Azure services used	<input type="checkbox"/>
Whether Azure native security controls such as firewall are implemented rather than integrating third-party capabilities	<input type="checkbox"/>
Whether the native threat-detection capability of Azure is incorporated into security solutions	<input type="checkbox"/>

Whether the shared responsibilities across IaaS, PaaS, and SaaS environments of Azure are validated	<input type="checkbox"/>
Whether it is ensured that the alerts are received from authorized sources or contacts within the Azure environment	<input type="checkbox"/>
Whether the industry best practices and guidelines are accumulated before initiating the response process	<input type="checkbox"/>
Whether the incident alerts are customized in different Azure services based on requirement	<input type="checkbox"/>
Whether an independent communication channel is established for reporting the incidents	<input type="checkbox"/>
Whether a list of participants (SOC, technical team, incident handlers) and tools (Defender, Sentinel, etc.) required to investigate the incidents is developed	<input type="checkbox"/>
Whether a process maturity model is implemented to review the incident process	<input type="checkbox"/>

Section 7: Checklist for Handling AWS Cloud Security Incidents	
Actions	Completed
Prepare People:	
Whether relationships are built with the developers and application SMEs for incident response	<input type="checkbox"/>
Whether the response mechanisms for incident response are defined based on the governance, risk, and compliance (GRC) model	<input type="checkbox"/>
Whether the team's AWS account numbers, the IP ranges of your virtual private clouds (VPCs), corresponding network diagrams, logs, data locations, and data classifications are identified	<input type="checkbox"/>
Whether the external AWS security APN Partners are identified to provide expertise and different insight to improve your response capabilities	<input type="checkbox"/>
Whether the security assertions are defined to identify unknown risks	<input type="checkbox"/>
Whether the cloud security experts on the team are trained or enlist the support of expert partners to monitor the AWS environment	<input type="checkbox"/>
Whether a subscription is made to the global continuous feed of current and relevant threats, risks, and indicators for threat intelligence	<input type="checkbox"/>
Whether the notifications are generated that alerts unusual, malicious, or expensive activities	<input type="checkbox"/>
Whether the machine learning functionalities are used to identify complex anomalies and unusual behaviors	<input type="checkbox"/>
Prepare Technology:	
Whether it is ensured that the teams have appropriate access to AWS accounts to fulfill their responsibilities	<input type="checkbox"/>
Whether there is a discussion with the organization's cloud architects about the AWS account strategy and cloud identity strategy to determine the level of access necessary for handling the incident	<input type="checkbox"/>
Whether the organization and governance of AWS accounts are understood before implementing new access mechanisms	<input type="checkbox"/>

Whether an AWS IAM role is created for the incident responders to use during a security incident	<input type="checkbox"/>
Whether a new, purpose-built AWS account is used such that the incident responders can work from a separate secure infrastructure	<input type="checkbox"/>
Whether appropriate access controls are prepared for delegating access to secure alternative AWS accounts using IAM policies	<input type="checkbox"/>
Whether IAM roles are created for automation resources such as Amazon EC2 instances or AWS Lambda functions	<input type="checkbox"/>
Whether the AWS Systems Manager Agent (SSM Agent) is used to remotely and securely administer Amazon EC2 instances	<input type="checkbox"/>
Whether the responsibilities and relationships of each managed service partner are identified in the cloud environments before an incident occurs	<input type="checkbox"/>
Prepare Processes:	
Whether the incident response team is defined and has prepared the related processes required for investigation and remediation	<input type="checkbox"/>
Whether a decision tree with other teams and stakeholders is created to assist in the creation and documentation of decisions	<input type="checkbox"/>
Whether the incident responders are allowed to access logs or other evidence to analyze and provide the ability to view or copy data	<input type="checkbox"/>
Whether the Amazon Elastic Block Store (Amazon EBS) snapshots are used as part of investigating a security incident	<input type="checkbox"/>
Whether the AWS Key Management Service (AWS KMS) and Customer Managed Key (CMK) are used to encrypt the snapshot	<input type="checkbox"/>
Whether a CloudWatch Logs subscription is used to share Amazon VPC Flow Logs with your centralized security account	<input type="checkbox"/>
Whether the data is moved from Amazon S3 to Amazon S3 Glacier using object lifecycle policies to securely store data for long-term usage	<input type="checkbox"/>
Whether immutable storage is used to protect data integrity at the source	<input type="checkbox"/>
Whether forensic workstations such as the base Amazon Machine Image (AMI) are prepared and launched for analyzing disc images, file systems, RAM dumps, or other incident artifacts	<input type="checkbox"/>

Section 8: Checklist for Handling Google Cloud Security Incidents	
Actions	Completed
Whether GCP's automated and manual processes are configured to get alerts for the potential incidents	<input type="checkbox"/>
Whether a team of experts is prepared for various specialized functions to manage the challenges of each incident efficiently	<input type="checkbox"/>
Whether the required tools and resources are readily available with the IH&R team during any security incident	<input type="checkbox"/>
Whether a proper communication technique such as IRC, a phone bridge, etc., is established to use during a security incident	<input type="checkbox"/>
Whether some templates and a contact list have been developed to share information across the teams during an incident	<input type="checkbox"/>
Whether necessary training is provided to the IH&R team periodically for handling security incidents across GCP	<input type="checkbox"/>
Whether it is ensured that the team has a proper skillset with the generic mitigations such as rolling back changes, draining, etc. for minimizing the time to mitigate (TTM)	<input type="checkbox"/>
Whether an effective dashboard layout is created such that the responders can quickly pinpoint any changes or issues across the GCP	<input type="checkbox"/>
Whether the links to the playbooks are available and can be referred by the responders after an incident is notified	<input type="checkbox"/>
Whether the incidence response drills are conducted to practice the skills required to handle Google Cloud security incidents	<input type="checkbox"/>