

# Recovery After Cloud Security Incident Checklist

**Note:** Prior to starting the recovery after 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 Recovery after Cloud Security Incidents	
Actions	Completed
Check whether the databases, applications, VMs, and OSs are free from malware before restarting the services	<input type="checkbox"/>
Install OSs and applications, gather data, media, and other components from backups	<input type="checkbox"/>
Enable compromised accounts after changing access rights and passwords, or assign new accounts	<input type="checkbox"/>
Check whether the systems and applications of the CCs are free from malware	<input type="checkbox"/>
Restart the applications and databases after installing security updates and patching the vulnerabilities	<input type="checkbox"/>
Restart the services on the CC and CSP sides only after obtaining proper permissions from stakeholders and authorities	<input type="checkbox"/>
Reconstruct the system key files	<input type="checkbox"/>
Make sure the Disaster Recovery-as-a-Service (DRaaS) is utilized for faster cloud data recovery	<input type="checkbox"/>
Check whether technologies such as integrated data loss prevention (DLP) tools and cloud access security brokers (CASBs) are employed	<input type="checkbox"/>
Closely monitor systems for any remaining signs of unwanted activity	<input type="checkbox"/>
Ensure to validate whether all services are functioning normally	<input type="checkbox"/>

Section 4: Checklist for Recovery after Azure Security Incidents	
Actions	Completed
If the administrative rights are taken by the attacker, you can remove trust from the current servers	<input type="checkbox"/>
Replace the ADFS servers and create a new one, or rotate the SAML token-signing certificate	<input type="checkbox"/>
Check whether the passwords of the break-glass accounts are reset and minimize them as per requirements	<input type="checkbox"/>
Avoid using on-premises accounts that are synchronized with Azure AD, and restrict the privileged access accounts are cloud-only accounts	<input type="checkbox"/>
Check whether MFA is implemented for all users in the tenant	<input type="checkbox"/>
Check whether administrative access is limited by enforcing conditional access and privileged identity management	<input type="checkbox"/>
Minimize the delegated permissions and consent grant that supports different functions such as accessing mailboxes, SharePoint content, OneDrive, altering the privileged users and roles, etc.	<input type="checkbox"/>
Check whether the refresh tokens instantly are revoked after credential changes	<input type="checkbox"/>
Check whether user access to Azure Active Directory is revoked	<input type="checkbox"/>
Check whether the required files are recovered from Azure VM backups, which are also known as recovery points	<input type="checkbox"/>
Check whether all Azure resources are back to their original configuration for resuming normal operations	<input type="checkbox"/>

Section 5: Checklist for Recovery after AWS Security Incidents	
Actions	Completed
Backup and Restore <input type="checkbox"/> Amazon Elastic Block Store (Amazon EBS) snapshot <input type="checkbox"/> Amazon DocumentDB <input type="checkbox"/> Amazon Aurora DB snapshot <input type="checkbox"/> Amazon EC2 instances <input type="checkbox"/> Amazon Elastic File System (Amazon EFS) file systems	<input type="checkbox"/>
Pilot Light <input type="checkbox"/> Amazon Simple Storage Service (Amazon S3) Replication <input type="checkbox"/> Amazon RDS read replicas <input type="checkbox"/> Amazon DynamoDB global tables <input type="checkbox"/> Amazon DocumentDB global clusters	<input type="checkbox"/>
Warm Standby	<input type="checkbox"/>
Multi-site Active/Active	<input type="checkbox"/>

Section 6: Checklist for Recovery after Google Cloud Security Incidents	
Actions	Completed
When there is a single-server instance active, create a VM using managed instance groups (MIGs) as it will automatically try to recreate the VM in case of a failure	<input type="checkbox"/>
Check whether the static site option is used to restore the service interruptions after the failure of the Compute Engine instances	<input type="checkbox"/>
Make use of Deployment Manager to configure the instances	<input type="checkbox"/>
Check whether the recent data backup in Google Cloud is used by the database server to recover the files	<input type="checkbox"/>
Make sure the recovered application or service is tested with different user scenarios in a recovered environment	<input type="checkbox"/>
Check whether the Cloud DNS is configured to point to the static website or the web server in case any application server is affected	<input type="checkbox"/>
Check whether the database service instance is configured to handle the normal production loads	<input type="checkbox"/>
Create new application instances and web servers by using their snapshots available on Google Cloud	<input type="checkbox"/>
Take necessary snapshots for recreating the disks when there is a zonal failure	<input type="checkbox"/>
Set up the HTTP health checks that can validate that the GCP services are up and running on the instances within a particular group	<input type="checkbox"/>