**19SFC162- CLOUD SECURITY MODULE 3 NOTES**

**1.Illustrate Various features that constitutes Traditional Security**

**Traditional Security**

Traditional or Physical Security of the cloud computing service provider’s facility is important and needs to be thoroughly assessed from various parameters.

A holistic view and understanding of the “people, process, technology” model or philosophy of the CSP would immensely help in evaluating the maturity of the CSP and give pointers to their approach towards security.

Organizational maturity and experience contributes to a great deal in effective handling of physical security program and any contingencies arising thereof. Invariably, there is a strong human element involved in the effective running of physical security program. The caliber of the security leadership and the level of management support to the security program are critical factors in spelling success for the organization in terms of business reputation and protecting company assets.

As you are aware, physical security is generally the first line of defense against unauthorized access to an organization’s physical assets and the physical theft of records.

**7.2 Recommendations**

o Onsite visit to the CSP’s facility or data center would help in performing an on-the-spot assessment and have a clear understanding of the different security measures that have been put in place.

o To enhance effectiveness of the onsite assessment, the visit to the CSP facility or data center should be carried out unannounced (if need be with the CSP being informed about a broad time window rather than specific times). This will enable to have real assessment on the ground on a normal business day instead of giving an opportunity to the CSP to ‘keep up appearances’ during a client visit.

o The assessment team should comprise at least 2 members or more with specialists drawn from IT, Information Security, Business Continuity, Physical Security and Management functions.

**7.3 Requirements**

• While evaluating the traditional security of a CSP, please do consider the following aspects:

Physical Location of the CSP Facility

• Check if the location of the facility falls under any active seismic zone and the risks thereof.

• Facility should not be located in a geographic region which is prone to:

• Flooding, landslides or other natural disasters

• Political, ethnic, communal or social unrests

• Easy and quick accessibility of the facility’s location

**Documentation Review**

• Physical & Environmental Security Policy

• User Account Termination Procedures

• Contingency Plan

• Incident Reporting & Response Plan

• Emergency Response Plan

• Facility Layout – emergency exits, positioning of CCTV cameras, secure entry points

• Fire Exit Route Map & Fire Order Instructions

• Emergency Evacuation Plan & Procedures

• Crisis Communication Procedures

• Emergency Contact Numbers

• User Facility Access Review/Audit Records

• Security Awareness Training documentation, presentation, handouts, etc

• Security Awareness Attendance Records

• Succession Planning for key executives

• Technical Documents – electrical wiring diagrams, BMS, UPS, AHU details

• Maintenance Schedule of Electrical, Generator & CCTV

• List of Authorized Personnel allowed entry inside facility

• Security Staff profiles – bio & background information

• Background Check Reports of Security Staff (must be performed every year)

• Annual Maintenance Contracts for key equipments& devices (focus on SLAs for equipment/devices downtime & restoration)

Check whether all the documents are updated and current. The documents must be reviewed by the CSP at least once in a year. The revision dates and sign off from competent employees must be mentioned in all the documentation as proof of them being reviewed internally.

Further, the policy and procedure documents (that are suitable for employee viewing) should be made available through a common Intranet site where authorized employees of the CSP can access them anytime for reference. Adequate care must be taken by the security team to ensure the uploaded documents are the latest versions duly approved by the management.

All policies and procedures would be effective only when employees are aware of them. To this effect, check whether the CSP has security awareness program in place. At the minimum, the CSP should ensure that employees are given adequate security awareness training at least once a year and receive sign off from them. Also, new employees joining the organization shall undergo a security orientation session as part of the induction program where key policies and procedures are to be covered. To make the program effective, a senior staff from the security team must conduct the session.

**Compliance with International/Industry Standards on Security**

If the CSP is compliant with global security standards like ISO 27001 ISMS or any other industry-specific standard it would be helpful in assessing the level of security program and its maturity.

• Verify the compliance certificate and its validity.

• Look for verifiable evidence of resources allocation – budget and manpower to sustain the compliance program.

• Verify internal audit reports and evidence of remedial actions for the findings.

Visual Walk Through Inspection of the CSP’s facility

Area Coverage

• Perimeter security

• Data Center

• Administrative areas

• Reception

• Parking Area

• Storage Area

• Fire Exits

• CCTV Command Center

• AHU Room

• Locker Room

• UPS Room

• Generator Room

• Fuel Storage Tanks

Signages

Look out for the following signages that must be displayed prominently in the facility at appropriate places:

• Fire Escape Route Maps & Emergency Exits

• Fire Order Instructions

• Fire Safety Signages

• Security Posters & Instructions

• Anti-tailgating Posters

• Temperature/Humidity-related information

• Warning & Instructional Signages

• Emergency Contact Numbers

• Escalation Chart

**Security Infrastructure**

Perimeter security is important as it serves as the first line of protection against intruders and unwanted visitors. The principles of perimeter security has undergone sea change with technological advancements. The Four D’s of Perimeter Security consists of Deter, Detect, Delay and Deny phases for intruders wanting access to the facility.

At the minimum, the following security infrastructure must be available at the CSP’s facility. Due care must be taken to ensure the infrastructure is adequate vis-à-vis the facility’s size and nature & scale of operations, strategically positioned and conforms to acceptable quality standards consistent with prevalent norms and best practices.

• Secure Entry Points – Access control systems (proximity cards/biometric access)

• Access Control System linked with fire control panel for emergency release

• Emergency auto-release buttons near all access card readers

• Motion-sensing alarms, thermal tracking devices

• Fire Safety Equipments – Wet Riser, Hydrants, Hoses,

• Smoke Detectors & Water Sprinklers

• Fire Extinguishers

• Fire Exits (must not be locked)

• Panic Bars in fire exit doors

• Alarm Hooters

• CCTV Cameras and DVR server (including backup timelines)

• Door Closures and time-delay door alarms

• Gas-based fire suppressants inside Data Centers

• Paper Shredders near printers

• Emergency Response Team Kit (ERT Kit)

• Two-way Radio devices (Walkie-talkie handsets) for security staff

• Duress Alarms underneath security desk and vantage (concealed) points

• Door Frame Metal Detectors at entrance & Hand-held Metal Detectors (if needed)

• Fire-proof Safe to safe keep important documents/media

**Human Resources Security**

**Competent Security Personnel**

Check to see if the CSP deploys competent security personnel for its physical security function. A dedicated security manager is highly recommended to provide the necessary leadership and drive to the physical security program. Leading industry certifications like CPP (from ASIS) would be helpful in validating the incumbent’s knowledge & skills in physical security.

A careful scrutiny of the reporting structure of the security manager would help in determining whether the position has been given due significance it deserves. Ideally, the security manager should report to a functional superior and not to any other department like Facilities or IT. Better still, if the position reports to the CEO directly it would be better in terms of independence and objectivity of the position.

**Training**

Check to see if the CSP’s operational and maintenance personnel are trained adequately on procedures and tasks that are pertinent to their day-to-day job responsibilities. Periodic (annual) training must be imparted to all staff on:

• security awareness (including social engineering attacks)

• emergency response procedures

• safety training

• crisis management

• business continuity

**Procedures**

The CSP should ensure that the following documents are made available for inspection on demand by clients.

• Background Checks (yearly once) by third party vendors

• Non Disclosure Agreements

• Implement ‘need to know’ & ‘need to have’ policies for information sharing

• Segregation of duties

• User Access Administration

• Defined Job Description (Role & Responsibilities)

• Role-based Access Control System

• User Access Reviews

**Security Guarding Personnel**

Where human monitoring and intervention is necessary, physical security staff comprising of guards, supervisors and officers shall be posted (on 24/7 basis) inside the CSP’s facility.

Among other things, the Site and Post instructions shall include the following:

a. Checking employee, contract staff and visitor credentials and use of the sign-in log.

b. Issuing and recovering visitor badges.

c. Curbing tail-gating by employees.

d. Handle visitors and movement within the facility.

e. Handling phone calls.

f. Monitoring intrusion and fire alarm systems and dispatch personnel to respond to alarms.

g. Controlling movement of materials into and out of the building and enforcing property pass regulations.

h. Enforcing rules and regulations established for the building.

i. Patrolling inside facility.

j. CCTV monitoring.

k. Key control and management.

l. Frisking and checking housekeeping and maintenance personnel during entry and exit.

m. Emergency response procedures.

n. Escalating security-related issues to security manager.

o. Accepting and dispatching mail.

p. Escort unattended business visitors inside the office.

**Contingency Plan**

In particular, review the existence of the following organizations or teams within the CSP’s security program.

• Emergency Response Team (ERT)

• Crisis Management Team

The composition of the above teams shall be reviewed in detail along with crisis communication procedure.

**7.3.2 Environmental Security**

The CSP’s facilities shall protect both personnel and assets by implementing controls that will protect the environment from environmental hazards. These controls may include but are not limited to: temperature and humidity controls, smoke detectors and fire suppression systems.

**Environmental Controls**

• The facility shall be equipped with specific environmental support equipment according to published internal standards, local and/or regional rules or laws including an emergency power supply.

• The data center shall be equipped with specific environmental support equipment according to published internal standards, local and/or regional rules or laws including Uninterruptible Power Supply.

• Equipment/devices required for environmental controls must be protected to reduce risks from environmental threats and hazards and to reduce the risk of unauthorized access to information.

**Equipment Location and Protection**

The following controls must be considered for systems classified as containing Restricted or Confidential information:

• Equipment is located in a physically secure location to minimize unnecessary

access.

• Environmental conditions are monitored for conditions that could adversely affect the operation of computer systems.

• Security staff shall take into cognizance of potential impact of a disaster happening in nearby premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street.

**Equipment Maintenance**

To ensure continued availability and integrity, equipment is properly maintained, Equipment Maintenance controls includes:

• Maintaining equipment in accordance with the supplier’s recommended service intervals and specifications.

• Permitting only authorized maintenance personnel to carry out repairs and service equipment.

• Maintenance by System Operators of records of all suspected or actual faults and all preventive and corrective maintenance.

• Use of appropriate controls when sending equipment off premises for maintenance. Examples of appropriate controls include proper packaging and sealing of containers, storage in safe and secure places, and clear and complete shipping and tracking instructions.

In conclusion, a thorough review of the CSP’s facility would enable the prospective client to understand and evaluate the maturity and experience of the security program. Generally, with the focus on IT security, physical security gets limited attention. However, with the range of threats prevalent in today’s scenario its imperative that the physical security warrants the attention it deserves. Especially, in an environment where the clients data would be co-hosted with a number of other clients (including competitors), physical security assumes great significance and it is the first line of defense against intruders and corporate saboteurs who may want access to a CSP’s facility for nefarious purposes.

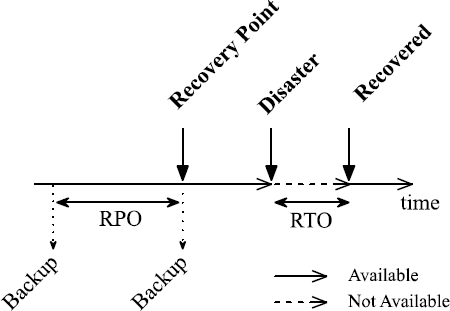
**2.Draw the architecture of Business Continuity and elaborate its key points**

With the dramatical improvement the information sector in addition to the escalating of world-wide businesses, a massive enterprise information has considered as the core for the worldwide business connections and data safe-keeping gets to be particularly significant. When the data this is simply not utilized in the short term but vital, it's going to be stored in cloud storage [35]. Several corporations would like to boost their opportunity to get over system failures and data loss, particularly to safeguard themselves from natural as well as man-made disasters [22].

A number of small and big corporations nowadays depend on an internet existence. Continuity is an important element the majority of organizations, as a unexpected service interruption can certainly influence organization goals leading to substantial losses with regards to income, business status as well as losses associated with market share [56][22]. As a point of interest in each and every organization, datahasalargemeasureofconcernfrombothscholasticandmechanicalviews.Asdataevolvesinsize, ensuring that it must be safely and securely set aside happens to be challenging[39].

In each and every enterprise there are a significant amount of data in digital format in which needed the safety storage services. Data backup and Business Continuity matters have grown to be essential in networksasthebenefitsandtheneedforelectronicdataisrepeatedlyescalating.Everysingleenterprise demands a business continuity plan (BCP) or disaster recovery plan (DRP) and data backup that comes within the expense limitations whilst getting the goal recovery requirements with regards to recovery time objective (RTO) as well as recovery point objective (RPO) [22]. [57], strengthen this statement by saying that, every enterprise needs BCP or DRP which often falls within expense constraints while getting the concentrating on recovery requirements with regards to RTO andRPO.

The DR levels are classified through those two important measures RTO and RPO which are the primary goals that should be achieved anytime assessing a great choice in a given operating and capital costs [42][15]. Furthermore, RPO states the data we might afford to lose, the lower the RPO, the higher the total expense of preserving the actual infrastructure environment for recovery [44]. This is more investigatedby[49]whomstatedthat,RPOindicatesthehighestpossibleappropriateperiodinbetween a couple of backups while RTO describes the most acceptable time period a business process might be disrupted as revealed in Figure8.



**Figure 8.** Recovery point objective (RPO) and recovery time objective (RTO)

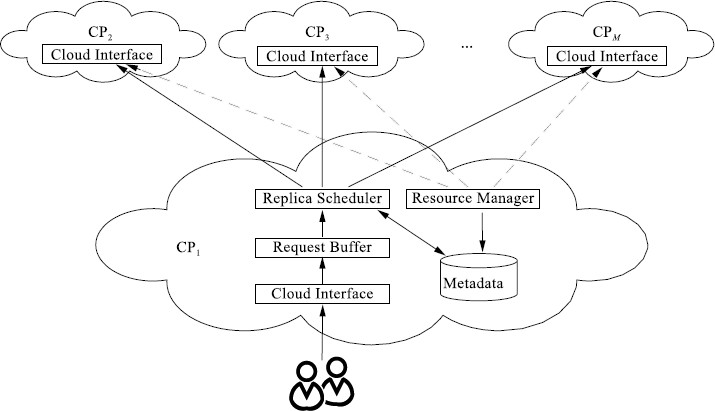
Disaster Recovery Planning (DRP) is related with the recovery of a key set of IT systems as well as infrastructure elements. While, the Business Continuity Planning is associated with the business as a complete piece handling business processes [44]. [22] Reinforces this statement by saying that, a key principle in a DRP is the actual physical separation of the main and also back-up sites. A substantial fraction of disasters consisting of those brought on through failures tend to be geographical as demonstrated in Table 2.

**Table 2.** Disaster faced in five years period

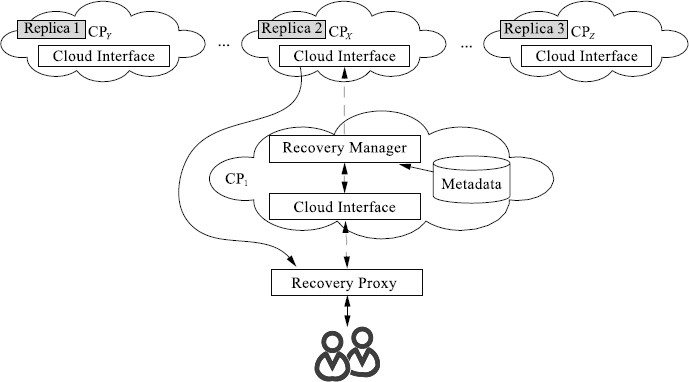
| **Cause** | **Organization** |
| --- | --- |
| System upgrades | 72% |
| Power outage | 70% |
| Fire | 69% |
| Configuration change management | 64% |
| Cyber attacks | 63% |
| Malicious employees | 63% |
| Data leakage | 63% |
| Flood | 48% |
| Hurricane | 47% |
| Earthquake | 46% |
| Tornado | 46% |
| Terrorism | 45% |
| Tsunami | 44% |
| Volcano | 42% |
| War | 42% |
| Others | 1% |

TheroleofICTindisastermanagementcontinuestobegrowing,behaviorofessentialinfrastructures has been explained by simulation, and response plans have been made by government departments as well as individual businesses [58]. In addition, existing data storage systems tend to be different and presentfeworperhapsnointegrationfeatures.Tomakethemostofavailabledata,areliableandscalable storage system sustained by data sharing, reuse, integration, as well as evaluation is required[59].

As an promising technology and business model, Cloud Computing has brought commercial computing by storm given it offers quick access to a business' high-performance computing as well as storage infrastructure by web services [38]. Furthermore, [34], stated that, DR-Cloud is consists of data disasterrecoveryservicecustomersandalsomultiplecloudserviceproviders.Thecompletearchitecture of DR-Cloud is shown in Figure 9 while Figure 10 shows the data backup and recovery models correspondingly.



**Figure 9.** Data backup model



**Figure 10.** Data recovery model

Disastersmightstrikeatanytime,anyplace,andmostoftentakeplacealongwithminimalornoalert [44][60]. Therefore, Most of the corporations tend to be seeking an improvement within their IT infrastructure[23].Cloudcomputingtechnologyisapromisingtomodifytheactualsituationassociated with disaster recovery[61].

From the IT point of view, recovery will most likely stand for creating assistance for the running as well as communications features regarded as essential by the enterprise society and then setting up assistance regarding subsidiary systems. From the business viewpoint recovery usually means, having the capacity to perform the business functions which are in the center of the enterprise then having the capability to carry out subsidiary functions [44].

ClientsatisfactionisamongthemajorobjectivesassociatedwithaServiceprovider.Suchsatisfaction isabletobringlonglastingbusinessexpansionandfarbetterbusinessearnings[46][62][63].Inaddition, businesses can make use of DR services that are served by cloud service providers. By using these services, information safety and service continuity tend to be assured for clients at several levels [1]. Table 3. Displays an overview of frequent difficulties as well as relevant solutions in DRplans

**Table 3.** Challenges and solutions of DR plans

| **Challenges** | **Solutions** | **Technique** |
| --- | --- | --- |
| Dependency cost | Local backup Scale up/down,  Dual-Role operation | * Using a Linux box at the customerpremises * Allocating resources to high priority services. * Hiring and running idle physical nodes on the secondarysite |
| Failure prediction and detection Security | Resource Management , GRB  SDDB | * Prediction and replacement of riskyhardware * Using monitoringunit * Using encryption, scrambling andshuffling techniques |
| Replication latency | Pipelined replication | * Performing replication andprocess operations inparallel |
| Data storage Lack of redundancy | IPCS  GRB, IPCS | * Using an inter privatecloud * Multiplebackup |

AnimportantconcernindeliveringDRserviceswouldbetoassistBusinessContinuity(BC),enabling applications to quickly come back on-line after having a disaster [42]. Therefore, DR thoughts are element of the BC, business Continuity safeguards that a corporation might recover its IT systems as wellasenterpriseprocedures[44].Furthermore,DRandBCdemandthatessentialbusinessinformation is backed up occasionally and also saved in separated and safe locations[64].

DR includes the procedure and policies associated with planning for recovery or continuation of technology infrastructure of corporation after having a natural or human-induced disaster. It is an essentialcomponentofBusinessContinuityManagement(BCM)[23].Inaddition,BCMisatoolwhich mightbeutilizedtodeliverbetterconfidencethattheresultsassociatedwithprocessesandservicescould be provided in case there is hazards [10].

DifferentresearchershaverecommendedseveraldevelopmentcyclesforBCM,eachofwhichplaces focus on specific elements of BCM [10][65-68]. BCM involved nine levels that are program initiation, project initiation, risk analysis, selecting risk mitigation strategies, monitoring and control, implementation, testing, education and training, andreview.

**3.Categorize the important features of Disaster Recovery in cloud security**

**Disaster Recovery In Cloud Computing: All You Need To Know**

Data is the most valuable asset of modern-day organizations. Its loss can result in irreversible damage to your business, including the loss of productivity, revenue, reputation, and even customers. It is hard to predict when a disaster will occur and how serious its impact will be. However, what you can control is the way you respond to a disaster and how successfully your organization will recover from it. Get to discover post how you can use disaster recovery in cloud computing for your benefit.

* **How does disaster recovery in cloud computing differ from traditional disaster recovery?** – Traditional disaster recovery involves [building a remote disaster recovery (DR) site](https://www.nakivo.com/blog/overview-disaster-recovery-sites/), which requires constant maintenance and support on your part. In this case, data protection and disaster recovery are performed manually, which can be a time-consuming and resource-intensive process. Disaster recovery in cloud computing entails storing critical data and applications in cloud storage and failing over to a secondary site in case of a disaster. Cloud computing services are provided on a pay-as-you-go basis and can be accessed from anywhere and at any time. Backup and disaster recovery in cloud computing can be automated, requiring minimum input on your part.
* **How does disaster recovery planning work in cloud computing?** – Creating, testing, and updating a DR plan can prepare your organization for an unexpected disaster and ensure safety and continuity for your business. A comprehensive DR plan should take into account your infrastructure, potential threats and vulnerabilities, most critical assets and the order of their recovery, and workable DR strategies. Integration of cloud computing services in disaster recovery allows you to design a DR plan and automate each step of the recovery process.

**Backup and Disaster Recovery in Cloud Computing**

Cloud computing is the on-demand delivery of computing services over the internet (more often referred to as ‘the cloud’) which operates on a pay-as-you-go basis. Cloud computing vendors generally provide access to the following services:

* Infrastructure as a service (IaaS) allows you to rent IT infrastructure, including servers, storages and network component, from the cloud vendor.
* Platform as a service (PaaS) allows you to rent a computing platform from the cloud provider for developing, testing, and configuring software applications.
* Software as a service (SaaS) allows you to access software applications which are hosted on the cloud.

As you can see, each cloud computing service is designed to help you achieve different business needs. More so, cloud computing can considerably improve data the security and high availability of your virtualized workloads. Let’s discuss how you can approach disaster recovery in the cloud computing environment.

**Cloud disaster recovery vs. traditional disaster recovery**

Cloud disaster recovery is a cloud computing service which allows for storing and recovering system data on a remote cloud-based platform. To better understand what disaster recovery in cloud computing entails, let’s compare it to traditional disaster recovery.

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

* A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
* Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
* Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
* Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

However, traditional disaster recovery can often be too complex to manage and monitor. Moreover, support and maintenance of a physical DR site can be extremely expensive and time-consuming. When working with an on-premises data center, you can expand your server capacity only by purchasing additional computing equipment, which can require a lot of money, time, and effort.

Disaster recovery in cloud computing can effectively deal with most issues of traditional disaster recovery. The benefits include the following:

* You don’t need to build a secondary physical site, and buy additional hardware and software to support critical operations. With disaster recovery in cloud computing, you get access to cloud storage, which can be used as a secondary DR site.
* Depending on your current business demands, you can easily scale up or down by adding required cloud computing resources.
* With its affordable pay-as-you go pricing model, you are required to pay only for the cloud computing services you actually use.
* Disaster recovery in cloud computing can be performed in a matter of minutes from anywhere. The only thing you need is a device that is connected to the internet.
* You can store your backed up data across multiple geographical locations, thus eliminating a single point of failure. You can always have a backup copy, even if one of the cloud data centers fails.
* State-of-the-art network infrastructure ensures that any issues or errors can be quickly identified and taken care of by a cloud provider. Moreover, the cloud provider ensures 24/7 support and maintenance of your cloud storage, including hardware and software upgrades.

**Why Choose Disaster Recovery in Cloud Computing**

The primary goal of disaster recovery is to minimize the overall impact of a disaster on business performance. Disaster recovery in cloud computing can do just that. In case of disaster, critical workloads can be failed over to a DR site in order to resume business operations. As soon as your production data center gets restored, you can fail back from the cloud and restore your infrastructure and its components to their original state. As a result, business downtime is reduced and service disruption is minimized.

Due to its cost-efficiency, scalability, and reliability, disaster recovery in cloud computing has become the most lucrative option for small and medium-sized businesses (SMBs). Generally, SMBs don’t have a sufficient budget or resources to build and maintain their own DR site. Cloud providers offer you access to cloud storage, which can become a cost-effective and long-lasting solution to data protection as well as disaster recovery.

**How to Design a Cloud-Based Disaster Recovery Plan**

After considering the benefits of cloud computing in disaster recovery, it is time to design a comprehensive DR plan. In fact, you can read one of our blog posts which walks you through [the entire process of a creating a DR plan](https://www.nakivo.com/blog/components-disaster-recovery-plan-checklist/). Below, we are going to discuss how to create a DR plan which works in the cloud environment.

As a rule, an effective cloud-based DR plan should include the following steps:

1. Perform a risk assessment and business impact analysis.
2. Choose prevention, preparedness, response, and recovery measures.
3. Test and update your cloud-based DR plan.

Let’s discuss how disaster recovery planning works in cloud computing.

**Perform a risk assessment and business impact analysis**

The first step in a disaster recovery planning in cloud computing is to assess your current IT infrastructure, as well as identify potential threats and risk factors that your organization is most exposed to.

A risk assessment helps you discover vulnerabilities of your IT infrastructure and identify which business functions and components are most critical. At the same time, a business impact analysis allows you to estimate how unexpected service disruption might affect your business.

Based on these estimations, you can also calculate the financial and non-financial costs associated with a DR event, particularly Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The RTO is the maximum amount of time that IT infrastructure can be down before any serious damage is done to your business. The RPO is the maximum amount of data which can be lost as a result of service disruption. Understanding the RTO and RPO can help you decide which data and applications to protect, how many resources to invest in achieving DR objectives, and which DR strategies to implement in your cloud-based DR plan.

**Implement prevention, preparedness, response, and recovery measures**

The next step is to decide which prevention, preparedness, response, and recovery (PPRR) measures should be implemented in disaster recovery of the cloud computing environment. In a nutshell, PPRR measures can accomplish the following:

* Prevention allows you to reduce possible threats and eliminate system vulnerabilities in order to prevent a disaster from occurring in the first place.
* Preparedness entails creating the outline of a DR plan which states what to do during an actual DR event. Remember to document every step of the process to ensure that the DR plan is properly executed during a disaster.
* Response describes which DR strategies should be implemented when a disaster strikes in order to address an incident and mitigate its impact.
* Recovery determines what should be done to successfully recover your infrastructure in case of a disaster and how to minimize the damage.

After you have determined which approach to disaster recovery to implement, you should choose a data protection solution capable of putting your DR plan into action and achieving DR objectives. Choose the solution which meets your business needs and complies with your infrastructure requirements. For this purpose, consider the following criteria:

* Available services
* Hardware capacity
* Bandwidth
* Data security
* Ease of use
* Service scalability
* Cost
* Reputation

**Test and update your cloud-based DR plan**

After you have created and documented the DR plan, you should run regular tests to see if your plan actually works. You can test whether business-critical data and applications can be recovered within the expected time frame.

Testing a cloud-based DR plan can help you identify any issues and inconsistencies in your current approach to disaster recovery in cloud computing. After the test run, you can decide what your DR plan lacks and how it should be updated in order to achieve the required results and eliminate existing issues.

**4.Illustrate various factors that leads to Risk of insider abuse**

Overall, there are three common types of insider threats: compromised insiders, such as an employee whose credentials were stolen; negligent insiders, for example, if an employee misplaces a laptop or incorrectly sends an email; and malicious insiders, including disgruntled employees, who commit acts such as theft, fraud, sabotage, espionage and blackmail.

These threats can be further broken down by how sensitive data is leaked. Here are six common insider threats that pose a danger to sensitive data, along with mitigation strategies for each.

**1. Exploiting information via remote access software**

**Problem:** A considerable amount of insider abuse is performed offsite via remote access tools. Users are less likely to be caught stealing sensitive data when they can do it off site. Plus, inadequately protected laptops, for example, may end up in the hands of an attacker if left unattended, lost or stolen. A number of remote access tools, namely Microsoft's remote desktop protocol ([RDP](https://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP)), are particularly susceptible to infiltration.

**Solution:** Solid share and file permissions are critical, as are OS and application logging. With many remote access options, you can enable tighter security controls on certain features and system access, monitor employee usage in real time and generate usage logs. Look into the configuration of your system and determine which features and audit trails can provide better management, reporting and security. It's also common for abuse to take place during nonbusiness hours, so consider limiting the times that users can remotely access systems.

Strong passphrase requirements can thwart guessed logins, and requiring users to log in after power-saving timeouts can keep unauthorized users locked out. Encrypting system hard drives also helps protect systems that are lost or stolen. To prevent RDP risks, it's best to disable the protocol when possible. Otherwise, proper patching and using Group Policy [are recommended](https://searchvirtualdesktop.techtarget.com/tip/Best-practices-to-prevent-RDP-security-issues).

**2. Third-party threats**

**Problem:** Third parties that have access to enterprise systems -- think contractors, part-timers, customers, suppliers and service providers -- can present a major risk to sensitive data. Also known as supply chain attacks or value-chain attacks, third-party attacks leave sensitive data and a company's reputation vulnerable, as evidenced in the [2013 Target breach](https://searchsecurity.techtarget.com/news/4500253983/Internal-report-on-Target-data-breach-reveals-glaring-security-holes) in which customer data was stolen after an HVAC contractor's credentials were obtained by hackers.

**Solution:** Make sure any third party you work with is trustworthy -- look at their background and get references if possible. Second, have a sound [third-party risk management program](https://searchsecurity.techtarget.com/tip/3-ways-to-shore-up-third-party-risk-management-programs) in place. Monitoring tools are instrumental in identifying malicious or anomalous behavior. User behavior analytics can detect erratic conduct. Restrict third-party access through the principle of least privilege to prevent access to anything on the network beyond what is needed to complete their job.

It is also important to regularly review third-party accounts to ensure system permissions are terminated after their work is completed. Regular [user access reviews](https://searchsecurity.techtarget.com/answer/How-to-conduct-a-periodic-user-access-review-for-account-privileges) for employees and third parties alike is a critical security practice.



**3. Leaking data via email and instant messaging**

**Problem:** Sensitive information included in or attached to an email or IM can easily -- and, often, unintentionally -- end up in the wrong hands. This is one of the easiest types of insider threats to eliminate.

**Solution:** One of the most effective mitigation strategies to catch sensitive information leaving the network is to set up a network analyzer to filter keywords, attachments and so forth. Utilizing client- or server-based [content filtering](https://searchsecurity.techtarget.com/feature/Introduction-to-email-security-gateways-in-the-enterprise) can also catch and block sensitive information from going out. Likewise, perimeter-based or outsourced messaging security mechanisms offer easy-to-manage content filtering and blocking.

Keep in mind that none of these options work well if message traffic is encrypted. However, filtering will at least highlight the fact that such communication is taking place. Speaking of which, be sure to regularly [review enterprise firewall rules](https://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls) to determine not only what's allowed in, but also what's allowed out of the network.

Another email and messaging threat to consider is phishing and other social engineering scams. Be sure to include [security awareness training](https://searchsecurity.techtarget.com/feature/IT-pros-stress-importance-of-security-awareness-training) as part of your insider threat program.

**4. Insecure file sharing**

**Problem:** Whether or not you permit file-sharing software such as Dropbox or Google Drive, or collaboration tools such as IM, Slack or Skype, odds are they're on your network and waiting to be abused. The services themselves are not the problem; it's how they're used that causes trouble. All it takes is a simple misconfiguration to serve up your network's local and network drives to the world.

**Solution:** If your organization allows file-sharing and collaboration software, it behooves you to ensure that users are aware of the dangers. Monitoring tools can help enterprises [detect and manage](https://searchstorage.techtarget.com/opinion/Security-top-concern-in-online-file-sharing-and-collaboration) the use of file-sharing and collaboration tools.

If you don't want these services used, you can try blocking them at the firewall; however, sometimes the software is smart enough to find open ports to go out. Also note that if you have business-grade Dropbox, for example, you cannot disable personal Dropbox use and keep the enterprise version. Be sure to use a network analyzer and regularly perform a firewall rule audit.

**5. Careless use of wireless networks**

**Problem:** One of the most unintentional types of insider threats is [insecure wireless network usage](https://searchnetworking.techtarget.com/tip/11-common-wireless-security-risks-you-dont-have-to-take). Whether it's at a coffee shop, airport or hotel, unsecured airwaves can easily put sensitive data in jeopardy. All it takes is a peek into email communications or file transfers for valuable information to be stolen. Wi-Fi networks are most susceptible to these attacks, but don't overlook Bluetooth on smartphones and tablets. Also, if you have wireless LANs inside your organization, employees could use them to exploit the network after hours.

**Solution:** You cannot control the airwaves outside of your office, but you can enable secure Wi-Fi use. This entails using a VPN for remote network connectivity, a personal firewall to keep users from connecting to the wireless computer and SSL/TLS for all messaging.

Also ensure your internal wireless networks are secure. Use proper encryption and authentication -- [WPA3](https://searchsecurity.techtarget.com/definition/WPA3) is the latest iteration of the Wi-Fi security protocol -- and enable logging. Disabling Bluetooth if it's not needed or at least making your devices nondiscoverable can also cut down on wireless attacks.

**6. Posting information to discussion boards and blogs**

**Problem:** Users often post support requests, blogs or other work-related messages on the internet. Intentional or not, this can include sensitive data and file attachments that may put your organization at risk.

**Solution:** Filtering HTTP content and email communications at the network perimeter is the best way to check for and block sensitive information from going out to such sites. However, there's always a chance that information may leak out via encrypted transmissions or from users' personal machines. In either case, it pays to stay abreast of new information about your organization on the web. A good way to do this is to subscribe to Google Alerts so you can be alerted anytime certain keywords show up on the internet. General Google queries can often uncover material as well. However, this only works for information made available to Google's bots, which may exclude some discussion boards.

The threat of malicious insiders isn't going away. The "[2019 Verizon Data Breach Investigations](https://enterprise.verizon.com/resources/reports/dbir/)" report said that 34% of all data breaches the previous year were the result of inside actors, up from 28% and 25% in 2017 and 2016, respectively.

**5.Classify different aspects of Security baseline in cloud security**

Security Baseline is one of the [Five Disciplines of Cloud Governance](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/governance-disciplines) within the [Cloud Adoption Framework governance model](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/index). Security is a component of any IT deployment, and the cloud introduces unique security concerns. Many businesses are subject to regulatory requirements that make protecting sensitive data a major organizational priority when considering a cloud transformation. Identifying potential security threats to your cloud environment and establishing processes and procedures for addressing these threats should be a priority for any IT security or cybersecurity team. The Security Baseline discipline ensures technical requirements and security constraints are consistently applied to cloud environments, as those requirements mature.

Security Baseline governance does not replace the existing IT teams, processes, and procedures that your organization uses to secure cloud-deployed resources. The primary purpose of this discipline is to identify security-related business risks and provide risk-mitigation guidance to the IT staff responsible for security infrastructure. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

Making the correct security decisions is critical to the success of your cloud deployments and wider business success. If your organization lacks in-house expertise in cybersecurity, consider engaging external security consultants as a component of this discipline. Also consider engaging [Microsoft Consulting Services](https://www.microsoft.com/enterprise/services), the [Microsoft FastTrack](https://azure.microsoft.com/programs/azure-fasttrack) cloud adoption service, or other external cloud adoption experts to discuss concerns related to this discipline.

**Policy statements**

Actionable policy statements and the resulting architecture requirements serve as the foundation of a Security Baseline discipline. To see policy statement samples, see the article on [Security Baseline Policy Statements](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/policy-statements). These samples can serve as a starting point for your organization's governance policies.

**Caution**

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

**Develop governance policy statements**

The following six steps offer examples and potential options to consider when developing Security Baseline governance. Use each step as a starting point for discussions within your cloud governance team and with affected business, IT, and security teams across your organization to establish the policies and processes needed to manage security-related risks.

**Security Baseline motivations and business risks**

This article discusses the reasons that customers typically adopt a Security Baseline discipline within a cloud governance strategy. It also provides a few examples of potential business risks that can drive policy statements.

**Security Baseline relevancy**

Security is a key concern for any IT organization. Cloud deployments face many of the same security risks as workloads hosted in traditional on-premises datacenters. However, the nature of public cloud platforms, with a lack of direct ownership of the physical hardware storing and running your workloads, means cloud security requires its own policy and processes.

One of the primary things that sets cloud security governance apart from traditional security policy is the ease with which resources can be created, potentially adding vulnerabilities if security isn't considered before deployment. The flexibility that technologies like [software defined networking (SDN)](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/software-defined-network/index) provide for rapidly changing your cloud-based network topology can also easily modify your overall network attack surface in unforeseen ways. Cloud platforms also provide tools and features that can improve your security capabilities in ways not always possible in on-premises environments.

The amount you invest into security policy and processes will depend a great deal on the nature of your cloud deployment. Initial test deployments may only need the most basic of security policies in place, while a mission-critical workload will entail addressing complex and extensive security needs. All deployments will need to engage with the discipline at some level.

The Security Baseline discipline covers the corporate policies and manual processes that you can put in place to protect your cloud deployment against security risks.

Note

While it is important to understand [Identity Baseline](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/identity-baseline/index) in the context of Security Baseline and how that relates to Access Control, the [Five Disciplines of Cloud Governance](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/index) calls out [Identity Baseline](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/identity-baseline/index) as its own discipline, separate from Security Baseline.

**Business risk**

The Security Baseline discipline attempts to address core security-related business risks. Work with your business to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks will differ between organization, but the following serve as common security-related risks that you can use as a starting point for discussions within your cloud governance team:

* Data breach: Inadvertent exposure or loss of sensitive cloud-hosted data can lead to losing customers, contractual issues, or legal consequences.
* Service disruption: Outages and other performance issues due to insecure infrastructure interrupts normal operations and can result in lost productivity or lost business.

**Security Baseline metrics, indicators, and risk tolerance**

This article will help you quantify business risk tolerance as it relates to Security Baseline. Defining metrics and indicators helps you create a business case for making an investment in maturing the Security Baseline discipline.

Metrics

Security Baseline generally focuses on identifying potential vulnerabilities in your cloud deployments. As part of your risk analysis you'll want to gather data related to your security environment to determine how much risk you face, and how important investment in Security Baseline governance is to your planned cloud deployments.

Every organization has different security environments and requirements and different potential sources of security data. The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Security Baseline discipline:

* Data classification: Number of cloud-stored data and services that are unclassified according to on your organization's privacy, compliance, or business impact standards.
* Number of sensitive data stores: Number of storage end points or databases that contain sensitive data and should be protected.
* Number of unencrypted data stores: Number of sensitive data stores that are not encrypted.
* Attack surface: How many total data sources, services, and applications will be cloud-hosted. What percentage of these data sources are classified as sensitive? What percentage of these applications and services are mission-critical?
* Covered standards: Number of security standards defined by the security team.
* Covered resources: Deployed assets that are covered by security standards.
* Overall standards compliance: Ratio of compliance adherence to security standards.
* Attacks by severity: How many coordinated attempts to disrupt your cloud-hosted services, such as through Distributed Denial of Service (DDoS) attacks, does your infrastructure experience? What is the size and severity of these attacks?
* Malware protection: Percentage of deployed virtual machines (VMs) that have all required anti-malware, firewall, or other security software installed.
* Patch latency: How long has it been since VMs have had OS and software patches applied.
* Security health recommendations: Number of security software recommendations for resolving health standards for deployed resources, organized by severity.

**Risk tolerance indicators**

Cloud platforms provide a baseline set of features that enable small deployment teams to configure basic security settings without extensive additional planning. As a result, small dev/test or experimental first workloads that do not include sensitive data represent a relatively low level of risk, and will likely not need much in the way of formal Security Baseline policy. However, as soon as important data or mission-critical functionality is moved to the cloud, security risks increase, while tolerance for those risks diminishes rapidly. As more of your data and functionality is deployed to the cloud, the more likely you need an increased investment in the Security Baseline discipline.

In the early stages of cloud adoption, work with your IT security team and business stakeholders to identify [business risks](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/business-risks) related to security, then determine an acceptable baseline for security risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how security metrics, such as those discussed above, can justify an increased investment in the Security Baseline discipline.

* Mission-critical workloads trigger. A company deploying mission-critical workloads to the cloud should invest in the Security Baseline discipline to prevent potential disruption of service or sensitive data exposure.
* Protected data trigger. A company hosting data on the cloud that can be classified as confidential, private, or otherwise subject to regulatory concerns. They need a Security Baseline discipline to ensure that this data is not subject to loss, exposure, or theft.
* External attacks trigger. A company that experiences serious attacks against their network infrastructure *x* times per month could benefit from the Security Baseline discipline.
* Standards compliance trigger. A company with more than *x%* of resources out of security standards compliance should invest in the Security Baseline discipline to ensure standards are applied consistently across your IT infrastructure.
* Cloud estate size trigger. A company hosting more than *x* applications, services, or data sources. Large cloud deployments can benefit from investment in the Security Baseline discipline to ensure that their overall attack surface is properly protected against unauthorized access or other external threats.
* Security software compliance trigger. A company where less than *x%* of deployed virtual machines have all required security software installed. A Security Baseline discipline can be used to ensure software is installed consistently on all software.
* Patching trigger. A company where deployed virtual machines or services where OS or software patches have not been applied in the last *x* days. A Security Baseline discipline can be used to ensure patching is kept up-to-date within a required schedule.
* Security-focused. Some companies will have strong security and data confidentiality requirements even for test and experimental workloads. These companies will need to invest in the Security Baseline discipline before any deployments can begin.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Security Baseline discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your cloud governance team.

**Security Baseline sample policy statements**

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

* Technical risk: A summary of the risk this policy will address.
* Policy statement: A clear summary explanation of the policy requirements.
* Technical options: Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common security-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be proscriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business, security, and IT teams to identify the best policies for your unique set of risks.

**Asset classification**

Technical risk: Assets that are not correctly identified as mission-critical or involving sensitive data may not receive sufficient protections, leading to potential data leaks or business disruptions.

Policy statement: All deployed assets must be categorized by criticality and data classification. Classifications must be reviewed by the cloud governance team and the application owner before deployment to the cloud.

Potential design option: Establish [resource tagging standards](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging/index) and ensure IT staff apply them consistently to any deployed resources using [Azure resource tags](https://docs.microsoft.com/azure/azure-resource-manager/resource-group-using-tags).

**Data encryption**

Technical risk: There is a risk of protected data being exposed during storage.

Policy statement: All protected data must be encrypted when at rest.

Potential design option: See the [Azure encryption overview](https://docs.microsoft.com/azure/security/security-azure-encryption-overview) article for a discussion of how data at rest encryption is performed on the Azure platform. Additional controls such as in account data encryption and control over how storage account settings can be changed should also be considered.

**Network isolation**

Technical risk: Connectivity between networks and subnets within networks introduces potential vulnerabilities that can result in data leaks or disruption of mission-critical services.

Policy statement: Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.

Potential design option: In Azure, network and subnet isolation is managed through [Azure Virtual Networks](https://docs.microsoft.com/azure/virtual-network/virtual-networks-overview).

**Secure external access**

Technical risk: Allowing access to workloads from the public internet introduces a risk of intrusion resulting in unauthorized data exposure or business disruption.

Policy statement: No subnet containing protected data can be directly accessed over public internet or across datacenters. Access to those subnets must be routed through intermediate subnets. All access into those subnets must come through a firewall solution capable of performing packet scanning and blocking functions.

Potential design option: In Azure, secure public endpoints by deploying a [DMZ between the public internet and your cloud-based network](https://docs.microsoft.com/azure/architecture/reference-architectures/dmz/secure-vnet-dmz?toc=https://docs.microsoft.com/azure/cloud-adoption-framework/toc.json&bc=https://docs.microsoft.com/azure/cloud-adoption-framework/_bread/toc.json). Consider deployment, configuration and automation of [Azure Firewall](https://docs.microsoft.com/azure/firewall).

**DDoS protection**

Technical risk: Distributed denial of service (DDoS) attacks can result in a business interruption.

Policy statement: Deploy automated DDoS mitigation mechanisms to all publicly accessible network endpoints. No public facing web site backed by IaaS should be exposed to the internet without DDoS.

Potential design option: Use [Azure DDoS Protection](https://docs.microsoft.com/azure/virtual-network/ddos-protection-overview) Standard to minimize disruptions caused by DDoS attacks.

**Secure on-premises connectivity**

Technical risk: Unencrypted traffic between your cloud network and on-premises over the public internet is vulnerable to interception, introducing the risk of data exposure.

Policy statement: All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.

Potential design option: In Azure, use ExpressRoute or Azure VPN to establish private connections between your on-premises and cloud networks.

**Network monitoring and enforcement**

Technical risk: Changes to network configuration can lead to new vulnerabilities and data exposure risks.

Policy statement: Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.

Potential design option: In Azure, network activity can be monitored using [Azure Network Watcher](https://docs.microsoft.com/azure/network-watcher/network-watcher-monitoring-overview), and [Azure Security Center](https://docs.microsoft.com/azure/security-center/security-center-network-recommendations) can help identify security vulnerabilities. Azure Policy allows you to restrict network resources and resource configuration policy according to limits defined by the security team.

**Security review**

Technical risk: Over time, new security threats and attack types emerge, increasing the risk of exposure or disruption of your cloud resources.

Policy statement: Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud.

Potential design option: Establish a regular security review meeting that includes relevant IT and governance team members. Review existing security data and metrics to establish gaps in current policy and Security Baseline tooling, and update policy to remediate any new risks. Leverage [Azure Advisor](https://docs.microsoft.com/azure/advisor/advisor-overview) and [Azure Security Center](https://docs.microsoft.com/azure/security-center/security-center-intro) to gain actionable insights on emerging threats specific to your deployments.

**6.Illustrate your view of Customers actions to be done when security violation occurs**

**1. Loss or theft of intellectual property**

Companies increasingly store sensitive data in the cloud. An analysis by Skyhigh found that 21% of files uploaded to cloud-based file sharing services contain sensitive data including intellectual property. When a cloud service is breached, cyber criminals can gain access to this sensitive data. Absent a breach, certain services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.

**2. Compliance violations and regulatory actions**

These days, most companies operate under some sort of regulatory control of their information, whether it’s HIPAA for private health information, FERPA for confidential student records, or one of many other [government](https://www.skyhighnetworks.com/skyhigh-for-government/) and industry regulations. Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected. BYOC often violates every one of these tenets, putting the organization in a state of non-compliance, which can have serious repercussions.

**3. Loss of control over end user actions**

When companies are in the dark about workers using cloud services, those employees can be doing just about anything and no one would know—until it’s too late. For instance, a salesperson who is about to resign from the company could download a report of all customer contacts, upload the data to a personal cloud storage service, and then access that information once she is employed by a competitor. The preceding example is actually one of the more [common insider threats](https://www.skyhighnetworks.com/cloud-security-blog/5-devious-instances-insider-threat-cloud/) today.

**4. Malware infections that unleash a targeted attack**

Cloud services can be used as a vector of data exfiltration. Skyhigh uncovered a [novel data exfiltration technique](https://www.skyhighnetworks.com/cloud-security-blog/in-plain-sight-how-hackers-exfiltrate-corporate-data-using-video/) whereby attackers encoded sensitive data into video files and uploaded them to YouTube. We’ve also detected malware that exfiltrates sensitive data via a private Twitter account 140 characters at a time. In the case of the Dyre malware variant, cyber criminals used file sharing services to deliver the malware to targets using phishing attacks.

**5. Contractual breaches with customers or business partners**

Contracts among business parties often restrict how data is used and who is authorized to access it. When employees move restricted data into the cloud without authorization, the business contracts may be violated and legal action could ensue. Consider the example of a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

**6. Diminished customer trust**

Data breaches inevitably result in diminished trust by customers. In one of the larges breaches of payment card data ever, cyber criminals stole over 40 million customer credit and debit card numbers from Target. The breach led customers to stay away from Target stores, and led to a loss of business for the company, which ultimately impacted the company’s revenue. See number 9 below.

**7. Data breach requiring disclosure and notification to victims**

If sensitive or regulated data is put in the cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims. Certain regulations such as [HIPAA and HITECH](https://www.skyhighnetworks.com/cloud-compliance/hipaa-encryption-compliance-requirements/) in the healthcare industry and the [EU Data Protection](https://www.skyhighnetworks.com/cloud-compliance/gdpr-general-data-protection-regulation-compliance-requirements-download-ebook/) Directive require these disclosures. Following legally-mandated breach disclosures, regulators can levy fines against a company and it’s not uncommon for consumers whose data was compromised to file lawsuits.

**8. Increased customer churn**

If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust. A growing chorus of critics are instructing consumers to avoid cloud companies who do not protect customer privacy.

**9. Revenue losses**

News of the Target data breach made headlines and many consumers stayed away from Target stores over the busy holiday season, leading to a 46% drop in the company’s quarterly profit. The company estimated the breach ultimate cost $148 million. As a result, the CIO and CEO resigned and many are now calling for increased oversight by the board of directors over cyber security programs.

According to the Ponemon BYOC study, a majority (64 percent) of respondents say their companies can’t confirm if their employees are using their own cloud in the workplace. Trust us—they are. In order to reduce the risks of unmanaged cloud usage, companies first need visibility into the cloud services in use by their employees. They need to understand what data is being uploaded to which cloud services and by whom. With this information, IT teams can begin to enforce corporate [data security](https://www.skyhighnetworks.com/cloud-data-security/), compliance, and governance policies to protect corporate data in the cloud. The cloud is here to stay, and companies must balance the risks of cloud services with the clear benefits they bring.

**7.Categorize types of Contract in cloud security**

Here are the top nine points of contention that have been arising:

**1. Who's liable for damages from interruptions in service?**

For the most part, cloud providers refuse to accept liability for issues, the researchers report. “Providers state liability is non-negotiable, and 'everyone else accepts it.'  Even large users had difficulty getting providers to accept any monetary liability, with one global user stating that generally it 'had to lump it,' and another saying, 'they won’t move.'" Some users pushed back in some deals, however, stating that refusal to accept any liability was as a “deal breaker.”

**2. What about service level agreements?**

Service level agreements -- commitments on availability levels and performance -- are another important piece of the cloud contract, and come in many flavors, since standards are lacking in this area. Hon, Millard and Walden note that SLAs are often highly negotiable, as they can be adjusted through pricing -- the more you pay, the better performance you are guaranteed. Larger cloud customers prefer to tag SLAs to key performance indicators, while smaller customers tend to get 5-10 key performance metrics, usually already stipulated by the cloud provider.

**3. Does availability extend to data?**

While providers tend to emphasize how redundant and fault-tolerant their clouds are, cloud customers still need to do their due diligence. Like fire insurance for an apartment, the provider will rebuild the structure but not compensate the renter for the damaged contents. "While some will undertake to make the necessary number of backups, most will not warrant data integrity, or accept liability for data loss," the researchers note.

**4. Where is the data actually going to be physically located?**

  The European Union's Data Protection Directive -- which prohibits storing of data outside the boundaries of the EU -- is the greatest area of data security and privacy concern at this time, Hon, Millard and Walden state. “Users were not concerned about colocation within a third party’s data center, so much as geographical location of data centers." The problem is, they continue, "some providers will not disclose data center locations.  Verifying that data are actually processed in the data centers claimed by providers is difficult, technically. One provider noted that some providers were misleadingly labeling servers as 'EU' when they could process data elsewhere.”

**5. How can users avoid vendor lock-in and exit if needed?**

Exit strategies need to be carefully thought out before committing to a cloud engagement. Vendor lock-in typically results from long-term initial contracts, the authors say. "Some providers wanted early termination fees (which may be 'huge') if users terminated a fixed-term contract earlier for convenience, as recovery of fixed set-up costs were designed to be spread over the term." Often, contracts require "notice of non-renewal within a set period before expiry," causing users to miss the window to exit the arrangement, they add, but such onerous automatic renewal provisions can be negotiated out up front. Another way to avoid lock-in, Hon, Millard and Walden add, is encouraging enterprise users to actually use several providers, "to avoid over-reliance on one provider’s service and its (possibly proprietary) application programming interfaces."

**6. Who maintains data for legal or compliance purposes, and what happens to it when contracts are terminated?**

The authors observe there hasn't been a lot of negotiation yet around data retention for legally required purposes, such as litigation e-discovery or preservation as evidence upon law enforcement request. "We think it will become more important in future," they add, but question how much assistance providers will give users -- such as providing long-term storage. One area that is being negotiated with increasing urgency is users’ ability to have data returned upon contract termination, Hon, Millard and Walden add. "There are several aspects here: data format, what assistance (if any) providers will give users, what if anything providers charge for such assistance, and data retention period."  Another question that comes up, they add,  is how long after termination users have to recover data before deletion. "Many providers delete all data immediately or after a short period (often thirty days), but some users obtained longer grace periods, for example two months, perhaps requiring notice to users before deletion," the researchers add.

**7. What happens when providers decide to change their service?**

Unfortunately for cloud customers, “many standard terms allow providers to change certain or all contract terms unilaterally," the researchers have determined. Enterprise cloud providers are more likely to negotiate these provisions up front, as are infrastructure providers. But for the bulk of businesses using more commoditized Software as a Service applications, "users might have to accept providers’ rights to change features." Customers are able to negotiate advance notifications of changes to Infrastructure Platform as a Service engagements, however, as these reach deeper into enterprises, and could result in users "having to rewrite application code created to integrate with proprietary provider application programming interfaces."

**8. How maintains intellectual property rights?**

Intellectual property rights issues are a frequently cited issue, the authors state. "Providers’ terms may specify they own deliverables, for example documentation. "However, the line is sometimes unclear between a user’s application and the provider’s platform and integration tools. Where integrators develop applications for their own customers, customers might require intellectual property rights ownership, or at least rights to use the software free after contract termination or transfer. Another issue of contention concerned ownership rights to service improvements arising from user suggestions or bug fixes, say the authors. "Providers may require users to assign such rights. Yet users may not want their suggested improvements to be made available to competitors.”

**9. What are the grounds for service termination?**

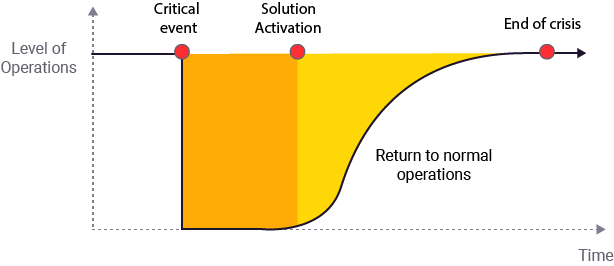
Non-payment is the leading reason providers terminate contracts with users, but there are many other issues that crop up, which may or may not be users' fault. Other reasons providers pull their services include material breach, breach of acceptable use policies, or upon receiving third-party complaints regarding breach of their intellectual property rights. The main issue is that the "actions of one end user customer may trigger rights to terminate the whole service," the authors point out. "However, many services lack granularity. For instance, an IaaS provider may not be able to locate and terminate the offending VM instance, and therefore need to terminate the entire service. Providers, while acknowledging this deficiency, still refused to change terms, but stated they would take a commercial approach to discussions should issues arise."

**8.Classify with keypoints the concepts of Documentation in cloud security**

**9.Illustrate Recovery Time Objectives (RTOs) with its architecture**

The main aspect of every backup and recovery strategy is a balance of [RTO and RPO](https://www.cloudberrylab.com/resources/blog/rto-vs-rpo-difference/) objectives. They regard how quickly and precisely you will be able to get the data back if something goes wrong. In case of disaster, recovery time objective becomes one of the most valuable characteristics in business planning.

What Is RTO in Disaster Recovery?



**RTO** (short for **Recovery Time Objective**) can typically be defined as the *desired* time period needed to conduct all recovery tasks before an application or service will be able to perform requests normally again. RTO, from the perspective of IT infrastructure, has two ends:

* Nothing works at all. Service is down, the server itself is burnt to the ground and everything is very bad
* You have recovered all needed data, restored services and your replicated servers are up and running

This time period between the "everything bad" and "up and running" situations is called unplanned downtime.

RTO for IT departments is influenced by the technologies used, but for businesses, they are far more important. If your company uses IT services as the basis of its financial activities or for back-office support, every minute of downtime will cost you a lot if not everything. The bigger the company – the more money it loses in case of unplanned downtime. That is why business owners are most interested in recovery time objective when creating backup and recovery plans.

If you are planning disaster recovery strategies, these will incorporate Recovery Time Objective, too. In cases of disaster, however, you will most likely use more complex technologies, such as cluster systems, storage replication, a secondary data center, cloud systems, etc.

**Meeting Recovery Time Objective**

Downtime costs depend on long-term effects such as loss of/damage to reputation or violation of a facility’s production plan, and immediate consequences such as failure to execute daily sales plan(s) or the inability to promptly replenish warehouses. Although recovery time objective is crucial for business, this objective is often undervalued or its value is set approximately. One reason behind it - the complexity of changes, that needs to be done, when the RTO is changing.

In conventional organizations, the RTO value is related to its service level agreement, appointed by top management and adopted by IT staff. It is important to understand, that a shorter Recovery Time Objective requires organizations to use special software(s) and hardware to meet agreed objectives.

It is not enough to just set up faster backup storage and LAN – meeting RTO is a complex task which involves the creation of a business continuity plan, to include the following activities:

**1. Create a proper monitoring system** that allows you to be notified in real time about any service failures. Many IT departments waste a lot of time by simply not knowing what has happened.

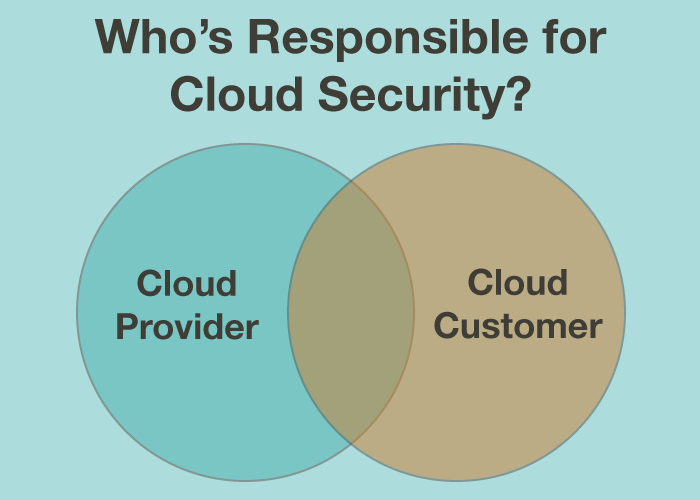
**2. Plan and deploy effective service/application configuration**, in order to be able to restore *all* data in a worst case scenario, and strictly meet the Recovery Time Objective frame. This configuration can include hardware and software solutions.

**3. Create and write down restoring procedure** so that every member of personnel knows what he/shemust do in case of downtime. Even the best-architected solutions can fail the objective by way of human error.

**4. Test overall recovery plan** with real hardware, using an amount of data equivalent to the production load. This testing must be a regular process since backup volumes tend to grow exponentially and the system must be changed, accordingly.

[Disaster recovery testing](https://www.cloudberrylab.com/resources/guides/draas/disaster-recovery-testing/) also allows you to effectively scale the system so that you can determine whether your RTO will be met. By attaining this information, you can assess and justify the need to purchase additional funds for top management. It is a good pattern for IT systems scale since it is directly influenced by actual business needs.

**10.Categorize the key features in Customers responsibility**



As more and more organizations migrate to the cloud, it drives cloud service customers to consider how the cloud will impact their privacy, security, and compliance. First, cloud service customers must understand how their cloud service provider delivers a secure solution. Second, cloud service customers must consider their new role in cloud security. Some cloud service customers mistakenly believe that when they migrate to the cloud, their cloud security responsibilities also shift. Who’s responsible for cloud security? Why do you even need security in the cloud? Let’s discuss the shared responsibility model and help you understand which elements of cloud security that customers are responsible for and which fall under the responsibility of the provider.

**What is the Shared Responsibility Model?**

The shared responsibility model is a method for determining which roles cloud service providers and cloud service customers play in cloud security. In general, the shared responsibility model outlines that providers are responsible for security *of* the cloud, and customers are responsible for security *in* the cloud. Cloud service providers and customers must work *together* to meet cloud security objectives.

To understand the shared responsibility model, let’s think about security requirements as a spectrum. Cloud service customers add together all of the regulatory, industry, and business requirements (GDPR, PCI DSS, contracts, etc.) that apply to their organization and the sum equals all of that organization’s specific security requirements. These security requirements will help ensure that data is confidential, has integrity, and is available. On one end of the security requirement spectrum is cloud service providers and on the other is cloud service customers. The provider is responsible for some of these security requirements, and the customer is responsible for the rest, but some should be met by both parties. Cloud service providers and cloud service customers both have an obligation to protect data.

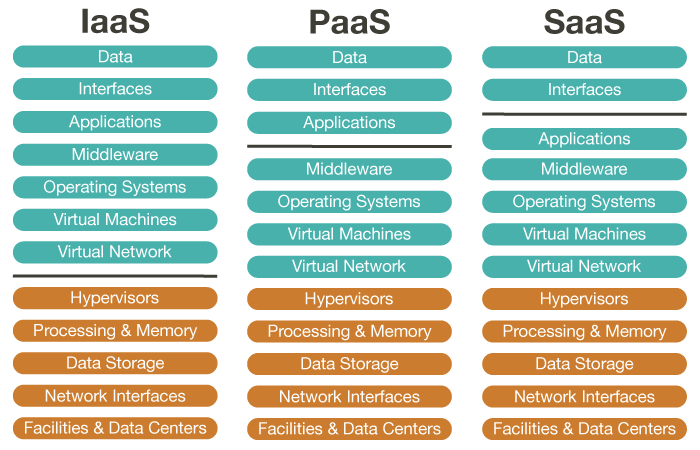
Microsoft Azure’s guidance on the shared responsibility model states, “The importance of understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud service providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications, and service offerings.”

**Shared Responsibility Model Across Service Models**

When choosing which service model (IaaS, PaaS, or SaaS) your organization needs, you should consider which security responsibilities will apply to you. Technology stacks are a great way to see the shared responsibility model across service model types.

* For IaaS solutions, the elements such as facilities, data centers, network interfaces, processing, and hypervisors should be managed by the cloud service provider. The cloud service customer is responsible for securing and managing the virtual network, virtual machines, operating systems, middleware, applications, interfaces, and data.
* PaaS solutions shift the cloud service provider’s responsibilities and add a few elements to their duties. The customer is still responsible for securing and managing applications, interfaces, and data.
* For SaaS solutions, the responsibilities shift again. Now, the cloud service customer is responsible for the security of interfaces and data.

Cloud service providers and cloud customers both have a responsibility to protect data. It’s also important to note that execution of individual security management tasks can be outsourced, but accountability cannot. The responsibility to verify that security requirements are being met always lies with the customer.



**Physical Security in the Cloud**

Physical security in the cloud sounds like an oxymoron, right? Isn’t less management of a physical environment a major benefit of migrating to the cloud? We often hear this case from organizations who haven’t or don’t want to implement cloud security best practices. But…not *everything* is in the cloud. *Everything* can’t possibly be in the cloud. Office locations, employees, servers, heating and cooling systems, power regulation, device management—these things don’t exist in the cloud. That’s why physical security must be a major aspect of cloud security.

**Best Practices for Managing the Shared Responsibility Model**

If you’re a cloud service provider, we believe these best practices will help you better manage the shared responsibility model:

* Consider risks from your customers’ perspectives, then implement controls that will demonstrate you’re doing everything you can to mitigate those risks.
* Document the internal controls you use to manage risks.
* Provide ample documentation on how your customers can use the security features that you provide in your solution. AWS does a great job of this through their educational programs.
* Create a responsibility matrix that defines how your solution will help your customers meet their various compliance requirements.
* Turn to the [CSA’s CAIQ](https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/) and [CCM](https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/) as starting points for establishing the shared responsibility model.

If you’re a cloud customer, consider these best practices:

* Define your cloud security requirements before selecting a cloud service provider. If you know what you’re looking for in a cloud service provider, you can better prioritize your needs.
* Harmonize your corporate governance program between traditional and cloud-based IT delivery. Migrating systems and applications into the cloud is going to require a difference in policy.
* Establish contractual clarity on the roles and responsibilities of each party, especially when you get into the public cloud. Who’s responsible for cloud security? How far does the cloud service provider go?
* Develop a responsibility matrix that defines the security roles and responsibilities for you and for each vendor, including cloud service providers.

**11.Illustrate core concepts in Vendor Security Process (VSP)**

Four Steps to Managing Vendor Security

If hackers gain access to a service providers’ systems, they can likely get to your systems, too. Rest assured, there are steps you can take to keep your cyber risk to a minimum.

**HORNE Cyber**

**Target. Home Depot. Wendys**.  The stories of significant cyber breaches are in the headlines every day.  Board members and CEOs are growing more and more concerned about cyber risk management in their organization.  But most don’t realize that each of the three breaches listed above were linked to 3rd party service providers and business associates.

Most of us do review our vendors for contract compliance and service delivery.  But very few are also reviewing vendors for their security position.  Vendors may or may not follow your security policies which make the vendors a much easier target.  If hackers gain entry into a 3rd party service providers’ systems, they can likely leverage stolen information and credentials to pivot into that your systems.

Vendor security is such a significant part of cyber risk management but it’s often overlooked.  If you want to improve your cyber risk profile, you should consider the following:

* **Build security requirements into contracts** – Vendor contracts should clearly spell out the expectations regarding security policies and procedures.   Protocols around security requirements should be written into the vendor contracts, such as:
  + Specific security policies
  + Access controls
  + Security reviews
  + Periodic audits
  + Incident response
  + Cyber insurance
  + Risk sharing in the event of a breach
* **Conduct regular security audits** – Once the contractual terms are established, you should regularly audit your vendor’s security position.  Questionnaires, on site visits and electronic monitoring can all go a long way in evaluating the effectiveness of the vendor’s security processes.  Questionnaires should be used for lower risk environments with onsite audits scheduled at least annually for higher risk vendors.
* **Demand SOC for cybersecurity** - The current SOC reports do not provide assurance or insight into a vendor’s security risk management program.  However, there is a new SOC report framework ([the SOC for Cybersecurity](http://blog.hornecyber.com/cyber-assurance-insights/cyber-soc-what-board-members-need-to-know)) which does specifically audit cyber risk management.  You should request that your vendors perform a SOC for cybersecurity audit annually or when there are significant changes to the vendor’s cyber environment.
* **Schedule access and security reviews** – Every company should be performing access and security reviews daily.  There are several services which will perform automated monitoring of access and security issues.  The downside to these services is that they may generate false positives.  That being said, the activities of any vendor granted access to the company’s systems should be superficially monitored for unusual activity.

Vendor security management is such a growing and significant portion of cyber risk that the AICPA will be issuing a framework to perform audits of these risks.  Taking steps today to address vendor cyber risks will help mitigate the exposure to your organization -- and reduce the risk of being the next headline.

**PREPARED BY**

**SRINIVASAN.L,Sr.AP,NHCE**