Cloud Security Best Practices

Version 1.0

Ministry of Electronics & Information Technology, Government of India

Cloud Management Office

DISCLAIMER

This document has been prepared by Cloud Management Office (CMO) under Ministry of Electronics and Information Technology (MeitY). This document is advisory in nature and aims to provide information in respect of the GI Cloud (MeghRaj) Initiative.

Certain commercial entities, technology, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by MeitY.

While every care has been taken to ensure that the contents of this Document are accurate and up to date, the readers are advised to exercise discretion and verify the precise current provisions of law and other applicable instructions from the original sources. It represents practices as on the date of issue of this Document, which are subject to change without notice. The document enlists practices around basic controls and is not prescriptive in nature. The readers are responsible for making their own independent assessment of the information in this document.

In no event shall MeitY or its' contractors be liable for any compensations whatsoever (including, without restriction, damages for loss of profits, business interruption, loss of information) arising out of the use of or inability to use this document.

Contents

1. Purpose

This document is prepared to assist the Government Departments in easier understanding & navigating through the best practices for Cloud Security. Cloud Security is one of the key aspects while considering cloud deployment options and imbibing the best practices laid down in this document shall further the Government Department's trust on Cloud and thereby facilitate a better use and adoption.

The document has primarily been segmented into 3 sections of which the first section shall deal with the approach and need of cloud security. The second section shall compare the aspects of traditional vs cloud security along with best practices of cloud security broken down across the various layers of Cloud. The final section elaborates on the shared responsibility model of Cloud Security wherein the Departments and Cloud Service Providers play critical roles in ensuring security of the cloud deployment.

2. Background

The Government of India has paved the way for mass adoption of Cloud services by the Government and Public sector organizations by empaneling the CSPs with Ministry of Electronics & Information Technology (MeitY). The CSPs are empaneled to offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) under the three Cloud Deployment models namely, Public Cloud (PC), Virtual Private Cloud (VPC) and Government Community Cloud (GCC).

With time, the Government Departments have started evaluating, planning, and adopting Cloud Services from the empaneled CSPs. As the adoption of technology within the Government Departments is evolving, it is intrinsic that the application workloads of the Government Departments are becoming complex in nature. Hence, it has become a prerogative for the Government Departments to imbibe certain practices around security while designing the cloud deployment for the workload.

Gaps in Cloud Security: While Cloud adoption across departments is progressing, Security is the key area to safeguard the Government data, so Department stakeholders must be aware of Cloud security best practices to address the security of data, information processing and technical measures in Cloud computing to protect it against unauthorized access of the data processing and travelling over internet/network and prevent accidental or unlawful tempering of data or loss/theft of data. Departments to adopt the required controls to restrict unauthorized use of data/information. Thus, it is imperative to develop certain practices around Cloud Security which will enable the Government Departments in ensuring a robust cloud deployment architecture and application security on CSP platform.

3. Introduction

3.1 Security in Cloud

Information Technology Security also known as, IT Security is the process of implementing measures and systems designed to securely protect and safeguard information (department and personal data, conversational information, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions.

Cloud security encompasses managing people, process & technology with thorough policies, that safeguard data and applications operating in the cloud. Cloud security includes examining how a Government department processes and stores data and then outline a customized approach to comprehensively protect the data. Departments can rarely afford a monumental hit to their reputation, so employing the best cloud security practices is critical for any modern department.

Cloud security has evolved pretty much as security has evolved for all new technologies and innovations. In the unfortunate event of a Government department experiencing such a breach, having a cloud incident response plan in place is crucial to mitigate the impact of suspicious activity and minimize damage. Enduring any catastrophic event is traumatic enough, but how the department reacts after such an event will often determine the fate of that department. The department's response plan will often determine the cost of a cyber breach.

> *Today, Government Departments can build security as an integrated part of the migration to IaaS services by optimizing security processes and identifying security components that would integrate seamlessly with their cloud requirement*

The adoption of cloud computing within Government Departments has created tremendous opportunity not only for cloud service providers, but also for cloud security specialists.

Security Requirements as published in the empanelment RFP (refer Empanelment of Cloud Service Providers (CSPs) https://meity.gov.in/content/gi-cloud-meghraj) elaborate on the security requirement needed to be complied by the aspirant CSPs when applying for

empanelment to offer their services to the Government Departments. The services offered by CSPs are to be availed by Government Departments as per their requirements.

Virtual Private Cloud allows for logical separation of infrastructure (server, storage, network) from other offerings of the Cloud Service Provider with strong/robust tenant isolation

Government Community Cloud allows for physical separation of infrastructure (server, storage, network) from Public and Virtual Private Cloud offering of the Cloud Service Provider

In a public cloud offering ensuring cloud security through the use of software controls, role-based permissions, storage, hypervisor separation is made available. In case the Departments seek further level of isolation or separation of workload and data between the cloud consumers, other Cloud Deployment Models such as GCC or VPC may be considered.

With inherent benefits of cloud enabling Government Department to focus majorly on their applications, cloud security has always been an area which draws major attention while evaluating cloud. Though the empanelment addresses security requirements to be met by the empaneled CSPs, Government Departments would additionally need to adopt certain practices to securely roll-out their applications/services. Certain practices around cloud security which the Departments may adopt in their cloud enablement journey are highlighted in this document.

In the cloud environment, Departments rely on CSP security and control to maintain the secure environment and mitigate potential risk, if Cloud Service Provider (CSP) does not adequately manage the responsibility of addressing IT and Cyber security parameters / controls at each layer, the way it should be placed in Cloud environment. So, Departments needs to ensure required Security Service Level Agreements (SLAs) are in place for CSP to adhere with necessary security services.

3.2 Need for Cloud Security

Although cloud computing services are a great option for Government Departments, there are some risks that come with the technology offered. Since the inception of cloud computing by Government of India, multiple Departments have been steadily switching to the empaneled cloud service providers. This availability of valuable data in a single location makes CSPs a prime target for malicious activity.

Government Departments directly or through their SIs, MSPs need to collaborate with CSPs in order to secure their critical data and ensure necessary security measures are in place. Apart from MeitY imposed regulations/ compliances, a security fabric needs to be merged at the data centre and cloud level. Issues such as insider threats are becoming a prevalent concern for many CSPs. Certain security concerns (including some OWASP Cloud Security risks) have been covered below:

Figure 1: Cloud Security Concerns

1. **Data Breaches**

   Though Cloud computing services are new and critical, yet data breaches in all forms have existed for decades. One of the main questions which generally Government Departments come across is "With department's sensitive data being stored online rather than on premise, is the cloud safe?"

   Cloud would provide the User Departments with enhanced security measures and necessary certifications. As per the MeitY empanelment of Cloud Service Provider (CSP), all CSPs enforce security controls as per ISO 27001, 27017 etc. but due to non-enforcement of security policies by the Government Department users it may lead to data breaches.

2. **Improper Cloud Account Management**

   The development and execution of the cloud in many organizations has opened a whole new set of issues in account attacks and hijackings.

   Attackers now can use the department's cloud login accounts information to remotely access critical/sensitive data stored on the platform / cloud; additionally, attackers can misrepresent and manipulate information through hijacked credentials.

   Hence appropriate cloud account management methodologies need to be implemented. In some cases, a Managed Service Provider (MSP) may also have access to Government Department cloud account hence appropriate controls should be implemented for such a condition as well.

3. **Insider Threat**

   An intrusion in Government department may seem unlikely, but the insider threat does exist. Government Department's users can use their authorized access to department's cloud-based services to misuse or access information such as citizen information, financial information, and other sensitive information.

   Hence it becomes imperative for Government Departments to implement a secure strategy for their cloud implementation and access and ensure that proper access control mechanism is in place to avoid security issues.

4. **Regulatory Compliance**

   Data that is perceived to be secure in one country may not be perceived as secure in another country or region. Hence data ownership and governance become important factors while choosing cloud.

As per MeitY's empanelment all empaneled Cloud Service Provider would be offering cloud services out of Indian Data Centre facilities and ensure data residency within the country. Data ownership resides with the Government Department.

5. Insecure APIs

Application Programming Interfaces (API) give operators the opportunity to customize their cloud platform. Even though APIs give users the ability to customize features of their cloud services to suffice the needs, but they also affect encryption , authentication and provision for access / controls.

The growth of APIs provides better services and do increase security risks. APIs give programmers the gears to build their programs to integrate their applications. The vulnerability of an API lies in the communication that takes place between applications. They also originate an opportunity for exploitable security risks.

6. Denial of Service Attacks

Unlike other kinds of cyberattacks, which are launched to establish a foothold and extract sensitive information over a longer span of time, denial-of-service attacks do not attempt to just breach the security perimeter. Rather, they attempt to make the services and servers unavailable to Department's legitimate users. In certain cases, DoS is also used as a cover for malicious activities and directed attack to take down security appliances such as WAF (Web Application Firewalls).

7. Insufficient Due Diligence

The issues listed above are technical in nature, however this particular security gap occurs when a Government Department doesn't have a clear path for its resources and policies for the cloud.

Due diligence for controls internal to cloud services need to be monitored by the Government Departments. There are multiple service parameters which need to be configured in a manner that they may not lead to operational, reputational or compliance issues. Insufficient due diligence may pose a major security risk when a Government Department overlooks certain cloud configurations at the user level.

8. Shared Responsibilities

Cloud security is a shared responsibility between the Cloud Service Provider and the Cloud consumer. This collaboration between consumer and provider requires the consumer to take necessary actions to protect their data. While major global Cloud Service Providers do have standardized procedures to secure their side, fine grain controls are up to the consumers.

The bottom line is that consumers and providers have shared responsibilities and omitting the user's responsibilities can result in their data being compromised. For further details kindly refer to Section 5 Cloud Security as a Shared Responsibility Model.

9. **Data Loss**

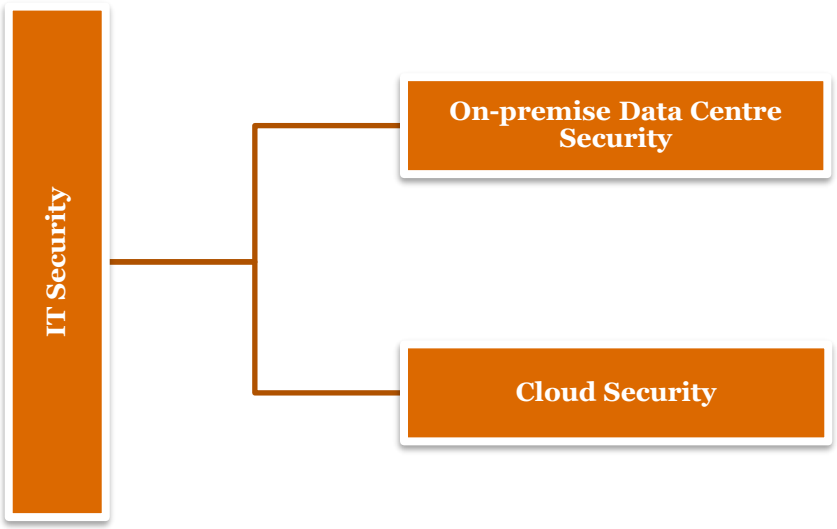
   Data on cloud platform can be lost through a natural disaster, data deletion or malicious attack by the service provider. Losing critical data / information can be devastating to businesses without a recovery plan.

The Open Web Application Security Project (OWASP) has additionally listed certain Cloud Security concerns such as User Identity Federation, Business Continuity and Resilience, Service and Data integration, Multi-tenancy and Physical security, Infrastructure Security which have been addressed in the requirements laid down as a part of empanelment of Cloud Service Providers by MeitY. These requirements make CSPs accountable for their responsibilities towards cloud security.

3.3 On-premise Data Centre Security and Cloud Security

Today, data is the key that drives the operations of departments. Such data helps keeping track of the performance, discover value adding insights, and improve security.

Data also plays a primary role in defining and outlining various IT security policies, be it on-premise or cloud setup. While some departments prefer in-house data collection and management, others opt for cloud migration because of its services availability and scalability. Cloud technologies have ensured easier management of data, especially ensuring enhanced data security. As the cloud ensures on demand infrastructure access, Departments are able to implement and maintain effective and efficient cloud security frameworks that can manage and tackle emergent threats.



Differentiating between traditional IT security and cloud security is very important. Each has its own set of advantages / limitations and being aware of both approaches will strengthen the Department's operational decision making.

3.3.1 On-premise Data Centre Security

An effective IT framework involves installing, purchasing, and maintaining the devices on-site. The traditional IT framework ensures collection, storage, and processing of data for various functions. Additionally, traditional IT infrastructure enables the departments to implement data security plans. This implies Government Departments to have the freedom of choosing the right security devices that need to be incorporated in the architecture, ways to manage network controls, and respond to incoming threats. The department would also take charge of detecting incoming threats and responding to it and maintaining a disaster recovery plan.

A traditional IT approach gives the department increased control over daily usage of each device. It is possible to monitor and control data along with daily data management and the data resides within department premises. Though an on-premise setup would need training of existing Department resources on emerging security technologies.

However, the biggest challenge with traditional IT systems is the Capital Expenditure required to install and maintain the security components. Asset refresh for end of life security components would also add to capital expenditure for the departments. The department is tasked with the responsibility to manage and monitor security related compliances / certifications which in turn are capital intensive and would require internal capabilities within the Department. Hence gaps in the security related practices may give rise to vulnerabilities.

Traditional IT systems also demand larger in-house personnel to manage the hardware and handle security incident responses and monitoring. While this may lead to additional control over data processes, there lies considerable cost implications.

3.3.2 Cloud Security

Unlike traditional IT systems, cloud computing refers to on demand access of infrastructure and services. Herein the CSP is responsible for making available the cloud platform and services portfolio which is configured and managed by the MSP for the client/user. Depending on the skillset, the user may themselves configure and manage the cloud platform in which case an MSP may not be required.

Cloud computing allows the Government Departments to access the software, hardware, and other necessary infrastructure required to run its daily operations. Furthermore, the cloud ensures easier data management and system security. Instead of controlling every aspect of data security control on-site, the Department can easily outsource the data security needs to a prominent and reputable Managed Service Provider.

On-premises infrastructure may be more exposed to small slip-ups and errors that can be prone to cyber-attacks. Furthermore, most cloud developers are more experienced with advanced security and data governance models. This means that the Departments will be able to plan appropriate strategies to ensure real time risk mitigation. An important reason for the reluctance to move more data into the cloud are the concerns around security.

A comparison between On-premise and cloud setups with security at the centre has been highlighted below:

	On-premise/ Co-located DC	Cloud
Technical Expertise	Government Department's own team or an IT Managed Service Provider	Cloud Managed Service Provider
Security Technology Upgrade	Less frequent	More frequent
Physical DC Security	Government Department/ Co-location DC Provider	Cloud Service Provider
IT Infrastructure Security	Government Department/Co-location DC Provider	Cloud Service Provider
Vulnerability/ Security Patching	Depends on support levels and technical expertise of in-house team	More frequent and up to date
Certifications & Compliances	Government Department	Cloud Service Provider
Resiliency (Downtime)	Less Resilient with varying commitments on downtime	More Resilient and committed uptime and availability SLAs

Though the On-premise setup for the Government Department allows complete control over the setup, in terms of cloud, multiple features such as infrastructure provisioning and maintenance, compliances and certifications, technology refresh are handled by the Cloud Service Provider allowing Government Department to focus on application delivery. Previous

constraining factors such as concerns for data security and privacy are weakening as the cloud providers continue to invest in successfully hardening their security and privacy profiles and standards.

4. Cloud Security Design Principles / considerations

The security design principles are the key pillars for adoption and implementation of Cloud Security to protect system, application and platform to improve overall security architecture.

Below are the key design principles which needs to be considered for Cloud technology adoption:

1. **Security at all layers:** Ensure robust Security is applied to all layers (Physical, network, Data, Application, etc.) of their architecture with multiple security controls. This will ensure end to end protecting of application/data hosted by departments on Cloud platform.
2. **Safeguard data while at rest and in transit:** Identify and Classify the data in terms of criticality/sensitivity and define their levels. This can be prevented via using the available security controls like access control, tokenization, encryption, etc.
3. **Monitoring and Auditing:** Ensure monitoring, auditing and alerting is configured to capture the changes in the department's system in real time. Further, log integration and metric collection can automatically investigate, act and respond.
4. **Access management and Controls:** Ensure implementation of principle of selective privileges and impose segregation of duties with appropriate access and authorization. Centralized identity and access management can eliminate any unauthorized access and information loss/theft.
5. **Readiness for security events:** Department/CSP needs to prepare system for any unusual security event. Regular vulnerability and security tests need to be conducted to identify the security gaps and issues. Several drill can be conducted to record the response of the Cloud systems at different layers.
6. **Automate security best practices:** Automating software/hardware/Application based security system via AI/ML/Bots to improve the ability to secure environment which can perform regular checks and implement the controls needed to restrict the attack and enhance cloud security.
7. **Cloud Vendor Lock-in:** Departments to ensure that there is no vendor lock-in by Cloud services provider while hosting the application/data, as there is no standard guidelines between different cloud providers for data migration and exports, so it becomes difficult to migrate data from one cloud provider to another or migration to on-premise Data centre.

5. Guidelines/Best practices for Cloud Security Adoption

For a Government Department migrating to cloud it is imperative to observe security discipline at various levels which ensures a secure adoption of cloud. The objective is to highlight certain industry best practices in cloud security which can be imbibed in the architecture of the Government Department's cloud requirement which shall facilitate a sense of security and increase the confidence to adopt cloud.

Data	Application	Host/ Compute	Network	Identity & Access	Physical

In this section we shall look at best practices to be observed at various layers of a cloud deployment architecture along with standards to be adopted or understood while choosing cloud for delivery of services.

5.1 A Layered Approach towards Security

IT security encompasses the lowest security layers, from physical facilities through the Department's implementation and configuration of IT infrastructure components. These are the basic components from which cloud is built, including networking, compute, and storage security.

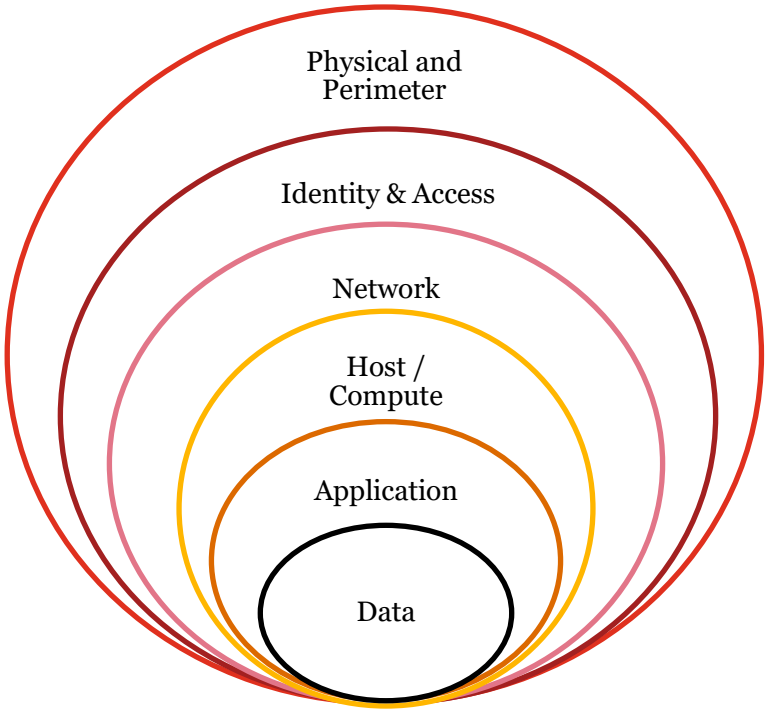


Figure 2: Layered Approach towards Security

It is important to be aware of the infrastructure security parameters of the CSP. The provider (one who maintains the private cloud platform) in the shared security model has the responsibility to ensure the security of the underlying physical, abstraction, and orchestration layers of the cloud. While in this section we highlight the cloud security best practices across all the layers mentioned above, we shall also touch upon Privacy as an important aspect to be considered under cloud-based security.

5.1.1 Data

The cloud data protection methods do not particularly require any new technique. Data protection in the cloud is very similar to data protection in a traditional data centre. Identity and authentication, encryption, access control, secure deletion, data masking and integrity checking are all data protection methods that are applicable in cloud computing.

Maintaining control over the data is paramount to cloud success. Today, with virtualization and the cloud, data may be under the Government Department's logical control, but physically reside in infrastructure owned and managed by another entity. This shift in control is the primary reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can User Departments be assured that Departmental or regulatory data remains private and secure, and that the User Department is protected from damaging data breaches?

Questions around assessing data security in Government Departments

- What sensitive data do we possess?
- What sensitive data do we have outside a secured location?
- Is any particular sensitive data overexposed?
- Who can access what kind of data?
- Who owns the particular file or folder?
- Have there been any changes to permissions of sensitive files?

Government Departments may adopt certain practices around data protection in order to overcome any reluctance around data security in Cloud.

- Department need to be aware of the type of data being handled by them and hence they at their discretion may categorize and deploy relevant data on cloud considering protecting from inadequate Data access / deletion, backup Vulnerabilities, data leakage, compromise of management interface, malware attacks, etc.
- Departments should adopt a data usage policy which clearly outlines various data access types, who has access to data and what conditions may constitute correct usage of data. There should be safeguards for policy violations and subsequent impact-based consequences.
- Access control is one of the most key and crucial aspect of data protection in cloud wherein Government Departments would be responsible for ensuring Administrative and Technical Controls to manage data access on the cloud.

The CSP shall be responsible for ensuring Physical Security of the deployed cloud infrastructure. Some of the practices around data security in cloud have been captured in this section.

Important points to remember

- Encryption is key to protect and secure data in transit and data at rest.
  - Multiple type of encryption can be implemented by CSP (i.e. Full Disk Encryption (FDE), Format Preserving Encryption, (FPE) Application layer Encryption, File Encryption, Database Encryption, etc.)
  - For protecting data in transit, choose encryption of sensitive data prior to moving to cloud and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit.
  - For protecting data at rest, Departments can simply encrypt sensitive data prior to storing them.
- Consider use of service provider-managed encryption options. Where possible, use customer-managed keys as they provide better control.
- Consider extra layer of data security via implementation of Data classification (Restricted, Confidential, Sensitive and Unclassified).
- Ensure integrity of data while replicating from one site to another.
- Create a data usage policy (data access control management, repercussion of policy violations, correct usage of data etc.)
- Backup (Full, Incremental, Differential) data regularly to ensure availability of data and perform periodic recovery operations to check correctness.
- Ensure data-level monitoring is in place, and logs meet all the compliance requirements, if any, of the department.

Data	Application	Host/ Compute	Network	Identity & Access	Physical

5.1.2 Application

Applications are hosted on independent virtual machines. Applications/ Sensitive data are more vulnerable in cloud-platforms, as cloud environments are hosted on shared resources. So, special security measure / controls are required to safeguard the client environments. Cloud service providers ensure that departments / users only have access to the data which they are authorized to access on shared Cloud model.

Use of micro-service architectures enhances the security further. Since optimizing the use of physical servers by the consumers is not a requirement, developers can instead deploy additional, smaller virtual machines, each dedicated to a specific function or a specific service. This minimizes the attack surface of the individual VMs and supports granular security controls.

DevOps is an advanced methodology for application development focused on automating the end to end process of application development and deployment. DevOps builds many opportunities for security to improve version control management, change management, and enhanced security operations in general.

DevOps isn't just about development and operations teams. The agility and responsiveness of a DevOps approach can be fully utilized if IT security plays an integrated role in the full life cycle of the application development.

Why? any Department may ask. In the past, the role of security was siloed to a specific team towards the final stage of development. That wasn't as problematic when development cycles followed a waterfall methodology. DevOps ensures rapid and frequent development cycles (sometimes weeks or days) followed by Continuous Integrations and Continuous Deployments, but outdated and traditional security practices can adversely affect even the most efficient DevOps initiatives.

Web application security refers to a process of protecting web apps and services available over internet and accessed through a browser. It protects against various security threats that exploit vulnerabilities in core / non-core applications. Key targets of attacks are sensitive data, content management system and other management/administrative applications. Key tools are being leveraged to protect department applications from intrusion. A web application firewall helps protect web applications by monitoring and filtering HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as, cross-site-scripting, SQL injection, file inclusion, as cross-site forgery, etc. It is implemented with defined set of rules / policies for protection.

"DevSecOps" emphasizes the need to build a security foundation into DevOps initiatives

Cloud APIs being provided by CSP's to software developers to develop the interfaces to interact with provided cloud services. Addition of another layer requires security from vulnerabilities and attacks, so implementation of security tools /appliances on Cloud provider's interface and enabling authentication / access control mechanism will help in enhancing the security layer for Cloud API. DevSecOps means introducing the role of application and infrastructure security teams from the start of the application development lifecycle. It also means automation of security gates to protect the DevOps workflow pipeline from slowing down. Selection of the right tools to continuously integrate security, like agreeing on an integrated development environment (IDE) with security features, can help achieve the desired objectives. However, the requirement of effective DevOps security is much more than just new tools—it builds on the cultural changes of DevOps to involve and integrate the work of security teams sooner rather than later. DevSecOps is making a significant difference in the IT industry, by ensuring a seamless software development life cycle (SDLC). Breaking the traditional trend of having security as a siloed process, DevSecOps calls for security integration across all stages of the software development process chain, addressing security concerns at the very start of every stage. DevSecOps approach to cloud security requires detailed planning that demands cultural change in an IT environment, especially for security automation and configuration of cloud assets.

The success of DevSecOps implementation in a cloud environment is administered by the following factors:

- Code Analysis – Continuous improvements to software means extensive code reviews.
- Automated Testing – Automated testing ensures effort minimization and saves time. As a primary aspect of DevSecOps process, automated testing makes the testing process faster and easier through efficient execution of repeatable test cases.
- Change Management – Fostering team collaboration to ensure that each team is aware of every other team's operations. If developers are informed about security-related activities from the start, it can help in timely address possible vulnerabilities.
- Compliance Monitoring – Compliance continues to play a major role in an organization's growth. Regulations help in code creation and source code modification. This helps in real time auditing.
- Threat Investigation – Threat investigation is important to define the security readiness of any organization. It's important for organizations to have a close and

continuous watch on identifying probable threats, periodic security scans and code reviews to address prevalent challenges in security.

- Personnel Training – Organizing hands-on training sessions and certification courses build the strength of the company by equipping teams with appropriate domain knowledge.

For Multi-tier applications, deciding where to ensure security would perplex a lot of Government Departments: at the web server level or database level or across every component in the cloud setup?

While multi-tier applications possess complex design methodologies, increase in the number and complexity of security mechanism may result in performance decline and unpredictable application behavior. Hence ensuring security while designing such complex multi-tier applications must involve more robust security assessment. Ensuring security provision and authorized access at the application level should be focused on post which the database may trust the application to authenticate and authorize end users to access data in the database. Database should be secured against any access except through the application. Ensure audit and logging at the application level while designing multi-tier applications.

Important points to remember

- Build security while initial design process of application. Creating Cloud Native applications presents an opportunity to engage cloud-based security early.
- Deployment process to be integrated with security testing.
- Encryption key management to maintain controls of all private / public encryption keys. Departments should understand the new architectural options and services available in the cloud. The departments should update their standards and security policies to support them and shouldn't merely attempt to enforce existing standards entirely on model.
- Segregation: Web facing application should be deployed in DMZ (De-militarized) zone and the Database Server should be deployed in the secured zone while deploying the application on cloud.
- Use of Web Application Firewall for Web apps and online portals
- Application integration and information exchange to happen over secured API channels.
- Security controls for interfaces and API's
- Log and monitor API calls.
- Use software-defined security to automate security controls.
- Use event-driven security such Anti-virus, when available, to automate detection and remediation of security issues.

Government Department may refer "Checklist for Secure Code Programming in Applications" (https://meity.gov.in/writereaddata/files/checklist_development.pdf) as well as "General Guidelines for Secure Application and Infrastructure" (https://meity.gov.in/writereaddata/files/General_Guidelines.pdf) published on MeitY website while designing their applications.

Data	Application	Host/ Compute	Network	Identity & Access	Physical

5.1.3 Host/ Compute

A workload is a unit of processing, which can be either a virtual machine, a container, or other abstraction. Workloads run on a processor and consume memory. Workloads include various processing tasks, that range from traditional applications running on a virtual machine on a standard OS to high GPU intensive workloads. It is recommended that virtual machine may be treated as if it was a physical machine for majority of the activities. Though an important point to note is that virtual machines are equally vulnerable to factors as in physical machines such as data loss/corruption, hardware failures, viruses, and hackers.

Multiple types of compute offering in the cloud are described as below:

- The Virtual Machine Manager (hypervisor) is responsible for abstraction of an underlying hardware from operating system. Hypervisors can tie into the capabilities of the underlying hardware to enforce isolation while supporting high-performance operations. Virtual machines are prone to certain memory attacks, but this is increasingly difficult due to ongoing hardware and software enhancements to reinforce isolation. VMs on today's hypervisors are generally an effective security control, and advances in hardware isolation for VMs and secure execution environments continue to improve these capabilities.

- Containers are code execution environments running within an operating system (for now) and sharing resources of that OS. Unlike VM which is an exact abstraction of an operating system, a container is an enclosed place to run distinct processes by utilizing the kernel and other capabilities of the base OS. Multiple containers can run on the same virtual machine or run directly on hardware without any OS.

- Serverless is a category that refers to a situation where the cloud consumers don't manage any of the underlying hardware or virtual machines, and just access exposed functions. But in the hindsight, they still utilize capabilities such as virtual machines, containers, or specialized hardware platforms.

Any given processor and memory will always be running multiple workloads, often from different tenants. Multiple tenants share the same physical compute node, and there is a range of segregation capabilities on different hardware stacks.

Certain practices around security in compute in cloud are described in the section below:

Important points to remember

- For critical workloads ensure High Availability at all deployment levels – compute, firewall, Load balancers.
- Departments should ensure that as soon as the new application server is deployed, security scans should be enabled, and the servers should be added to continuous monitoring.
- Integrate security testing and policies while VM image creation.
- Disable remote access post application configuration.
- Implement appropriate role-based access controls and strong authentication for all Virtual Machines (VM), Containers and VM images.
- Employ the use of pre-certified VM images from the cloud platform where pre-certification would be an on-going effort.
- Prefer Patching of VM images rather than patching running instances. Ensure patching is up to date for Operating System, Database licenses etc.
- Ensure VM level encryption through Bitlocker, LUKS etc. for security of VM in case of compromise
- Ensure Operating System Hardening is performed on the virtual machine.
- Take periodic VM snapshots and save in a secured repository.
- Prefer use of file integrity monitoring in order to ensure authenticated changes and detect unapproved changes to files.
- Store logs (including Audit logs) externally to workloads.
- Install Anti-virus software on Virtual Machine and ensuring periodic patching is performed.
- Perform periodic vulnerability assessments and penetration testing (VAPT) on Department's cloud infrastructure.
- In case of Business-Critical Applications plan for Disaster Recovery (DR).

Data	Application	Host/ Compute	Network	Identity & Access	Physical

5.1.4 Network

There are various kinds of virtual networks, from basic VLANs to full Software-Defined Networks (SDNs). The data in transit also needs to secure through the network layer. A cloud service provider needs to understand the department network traffic plan to send and receive data. Department to ensure CSP has implemented strong security controls for internal and external network separation / communication. CSP to ensure appropriate network segmentation which separates networks of different sensitivity levels. Most cloud computing platforms today use SDN for virtualizing the networks. SDN abstracts the network management plan from the underlying physical infrastructure, removing many typical networking constraints. For example, department can overlay multiple virtual networks over the same physical hardware, with all traffic properly isolated and segregated.

SDNs are also defined using API calls and software settings, which supports agility and orchestration. Virtual networks are different from physical networks in a way that virtual networks run on physical networks, but abstraction allows deeper modifications on the networking behavior that impact security processes and technologies.

It is pertinent to **secure Cloud data transfers**. Government Departments must ensure data protection as their data exchange to the cloud. This demand understanding the CSP's data migration mechanisms, as leveraging the mechanisms of the provider is often more cost effective and secure than "manual" data transfer methods such as Secure File Transfer Protocol (SFTP). For example, sending data to a CSP's object storage over an API is likely to be more secure and reliable than setting up own SFTP server on a virtual machine in the same provider.

There are a few options for in-transit encryption depending on what the cloud platform supports.

- One option is to follow client-side encryption i.e. encrypt before sending to the cloud.
- Another option is Network encryption (TLS/ SFTP/etc.). Most CSP APIs use Transport Layer Security (TLS) by default as this is an essential security capability.
- Third option can be a Proxy-based encryption, where there is an encryption proxy in a trusted area between the CSP and the cloud consumer and the proxy manages the encryption before data transfer to the CSP.

It's a good practice to isolate and scan the data before integrating it. Logs need to be offloaded and externally collected more quickly due to the higher velocity of change in cloud. A practice such as collecting logs in an auto-scale group before the cloud controller shuts down such unneeded instances would safeguard Government Departments from any losses.

Protection is required from the threat of denial of service against CSP cloud computing resource which is generally an external threat against public cloud services. Distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. So, it is important for department to get the Anti-DDoS services adopted from CSP

Certain practices which the Government Departments may consider while dealing with network security in cloud are as follows:

Important points to remember

- Use Virtual Private Network (SSL or Site to Site) to access Cloud infrastructure and services
- For Department computers connected in a network, refrain from disabling any personal firewalls on the computers.
- Use IP Whitelisting to allow connections from certain IPs and deny all others where applicable
- Pre-certifying additional VLAN, firewall ports and load balancers.
- Separate virtual networks and cloud accounts reduce security risks compared to traditional data centres.
- Restriction of traffic between workloads in the same virtual subnet using a firewall policy needs to be followed whenever possible.
- Dependency on virtual appliances that restrict elasticity or cause performance bottlenecks needs to be minimized
- Implement policies and internal security controls to prevent traffic monitoring without approval or outside contractual agreements and consumer networks modifications
- Departments should ensure that all new network segments should be registered security scans on deployment and then should be added to continuous monitoring.
- An automated response to attacks should be configured and additional information on the intrusion must be acquired. IP blocking, connection termination and signature analysis are some of the processes under such an automated response.
- Regularly monitor network traffic logs or implement a SIEM to get real-time security alerts generated by application and network devices.
- Prefer use of SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.

Data	Application	Host/ Compute	Network	Identity & Access	Physical

5.1.5 Identity and Access

Identity and Access Management (IAM) refers to defining and managing access privileges of individual network users, along with the circumstances in which users are permitted (or forbidden) those privileges. These users may either be external to the Department (e.g. citizens) or internal to the Department (e.g. employees). The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it is utmost important to be maintained, modified and monitored throughout each user's "access lifecycle."

Identity Management and Access Control security would include the following:

- Using Multi-Factor Authentication (MFA)
    - MFA may be utilized wherein a conditional access policy may be defined and authentication to be subject to LDAP or AD authentication. Detect potential vulnerabilities that affect the Department's identities. Automated responses can be configured to detect suspicious actions that are related to the Department's identities. It is important to investigate suspicious incidents and take appropriate action to resolve them.
    - MFA offers the option for reducing account takeovers as relying on a single factor (password) for cloud services poses high risks. MFA can be delivered using the following:
        - Hard tokens are physical devices that generate one-time passwords for human entry or need to be plugged into a reader. These ensure highest level of security.
        - Soft tokens are similar to hard tokens but are software applications that run on end device. Soft tokens are also a viable option but could be compromised if there is a compromise in the user's device, and this risk needs to be considered in any threat model.
        - Out-of-band Passwords are text messages sent to a user's phone (usually) and are then entered like one-time password generated by a token. Any threat model must consider message interception, especially with SMS.

- Using Access Control methodologies

    - While using Cloud services, access management of Cloud resources is critical for any Department. For instance, an identified access management methodology, such as Role-Based Access Control (RBAC), helps in managing access to cloud resources by end users, what these end users can do with the allocated resources, and what areas the end users would have access to.

    - Designating activities to specific roles in Cloud helps avoid confusion, which usually lead to human and automation errors thereby resulting in creating potential security risks.

    - The Department's security team needs to be able to evaluate potential risks to Cloud resources. The security team therefore needs relevant privileges to gain the required visibility into Cloud resources by enabling the necessary permissions. The Department or its security team can use various methods to assign permissions to relevant users, user groups, and applications pertaining to a certain scope. The scope of a role may be a subscription, a resource group, or a single resource.

    - The appropriate permissions necessary for security teams to perform their operational responsibilities is the responsibility of the Department. This includes review of the built-in roles for roles assigned. Custom roles may also be created in cases where the built-in roles fail to meet the specific needs of the Department. In case data access controls are not enforced by the Departments, more than necessary privileges may be assigned to their end users.

- Active Monitoring of suspicious activities

    - Identity monitoring systems are tasked with prompt detection of suspicious activity and consequently triggering alerts for further actions

    - As a practice, Departments should have a method of identifying brute force attacks, sign in attempts from multiple locations, suspicious IP addresses, sign in from infected systems to their cloud deployments.

A comprehensive plan needs to be institutionalized by departments that clearly articulates the processes of managing user identities and authorizations of the Cloud services.

Important points to remember

- Department to adopt Identity-as-a-Service (IDaaS) for implementation of single sign-on
- Department and CSP to restrict the use of root and generic accounts for Cloud Management and operations
- Departments to Adopt a role-per-group model for access of systems
- Department to ensure resource-level access controls to access Web, Application and cloud resources
- Implementation of Multi-factor authentication and separate Cloud Accounts
- Departments to govern the user details and their access levels, periodically.

Data	Application	Host/ Compute	Network	Identity & Access	Physical

5.1.6 Perimeter and Physical

Perimeter defense is largely about controlling the network traffic coming in and out of a data centre network. Best practices include the implementation of a layered set of defenses working in tandem. Beyond a router, which connects the internal and external networks, the primary protection layer is the perimeter protection through a firewall, which filters out potentially dangerous or unknown traffic that may constitute a threat based on a set of rules about the types of traffic and permitted source/destination addresses on the network. Data centre providers also deploy intrusion detection or intrusion prevention systems (IDS/IPS), which look for suspicious traffic once it has passed through the firewall.

The Cloud Service disruption can be caused by unwanted physical access of hardware. CSP should secure their data centre facilities and consider resiliency by implementing availability strategies. The threat increases where Cloud Service Provider has not implemented adequate secure or remote working environments from internal and external sources.

Government Departments need to seek assurance from the selected CSPs that necessary security controls are in place. CSPs need to provide assurance by means of relevant audits and assessment reports. Additionally, they can also demonstrate compliance to security standards as included in Section 4.3 Standards applicable for Security.

Ensuring perimeter security and physical security of the Data Centre, shall be the responsibility of the CSP, and in accordance with the norms laid down for empanelment for Cloud Service Providers by MeitY. Unauthorized personnel gaining access to the data centre shall result in a compromise and the CSPs are responsible to ensure sufficient measures such as security guards, secured fencing, security scanners, biometric access, CCTV surveillance, Access Logs etc. are available at the data centre to prevent unauthorized or forceful entry into Data Centre premises.

Important Point to Remember:

Empaneled Cloud Service Provider shall be responsible for maintaining security and sanctity of the physical data centre along with IT infrastructure (compute, network, storage, security) deployed for the cloud.

Some security controls around physical security of data centre to be ensured by the CSPs include:

- Physical infrastructure shall be kept in secure areas – CSP needs to ensure physical and perimeter security are in place to prevent from unauthorized access. This includes having physical entry in controls that ensure access to only authorized personnel for areas containing sensitive infrastructure.

- Protection against environmental threats – CSPs to ensure protection against environmental threats including floods, earthquakes, lightning, fire, natural disasters, civil unrest or other threats that could disrupt operations of a data centre.

- Data Centre IT infrastructure security controls – CSP needs to ensure that necessary controls are in place to prevent damage, loss, compromise or theft of assets.

- Safety against failure of equipment – CSP need to ensure that necessary controls are in place to execute preventive maintenance of all data centre equipment in order to avoid disruption of services due to detectable equipment failures.

- Procedure for data centre asset removal/theft – CSP need to ensure that appropriate controls exist against removal or theft of sensitive assets.

- Safe disposal or reuse of data centre equipment – CSP need to ensure that necessary control are in place for the suitable disposal of any data centre equipment, in particular any devices that might contain important data like storage media.

- Security controls for DC personnel – Suitable controls need to be instituted for all employee working at the facilities of a CSP, including all temporary staff.

- Ensuring Backup, Redundancy and Continuity Plans – CSP needs to provision appropriate mechanism to carry out regular backup of stored data, redundancy of equipment, as well as continuity plans for handling situations leading to equipment failure.

On the other hand, Government Departments would need to ensure physical security of their endpoints from both physical and logical perspective to ensure a complete secured access and operation from the Cloud.

5.2 Cloud Security Assessment

While institutionalizing practices around Cloud security, as mentioned in the section above, Government Departments may focus on performing a security assessment for their Cloud projects. There are certain critical questions which Departments must ask themselves as well as their Cloud Service Providers during each step of security assessment.

This section explains an efficient method of evaluating security capabilities of the CSPs, and also evaluating their individual risks, by the Department. Following is a set of guiding questions for Government Departments ask and conduct assessment across each of the listed security domains.

Security Step	Guiding Questions for Security Assessment
Ensuring Governance, Risk and Compliance processes exist	• What information security regulations or standards are applicable to the Department's domain? • Does the Department have any governance and compliance processes instituted for the use of cloud services? • Does the CSP have appropriate governance and incident notification processes for their services, consistent with the Department's requirements? • Do the Master Services Agreement and Service Level Agreement clearly outline responsibilities between the provider and customer? • Are there any risks related to data location?
Auditing and Reporting	• Is a report by an independent audit agency available for covering the CSP's cloud services? Does the audit information conform to one of the accepted standards for security audit such as ISO 27001?

Security Step	Guiding Questions for Security Assessment
	• Does the CSP have provisions to report to the customers about routine and exceptional behavior related to its offered services? Are all appropriate events and actions having security implications logged? • Do the security controls encompass not only the cloud services themselves, but also the management interfaces offered to customers? • Is there an Incident Reporting and Incident Handling process that meets the requirements of the customer?
Managing People, Roles and Identities	• Do the provider services offer fine grained access control? • Is multi-factor authentication supported for provider services? • Can the provider give reports for monitoring user access? • Is it possible to integrate or federate customer identity management systems with the identity management facilities of the provider?
Ensuring Data and Information Protection	• Is there a catalog of all data that will be used or stored in the cloud environment? • Have roles and responsible of different stakeholders involved in data management been defined? • Has the handling of all forms of data been considered, in particular unstructured data such as images?

Security Step	Guiding Questions for Security Assessment
	• For structured data held in databases in a multi-tenant cloud environment, is there proper separation of data belonging to different customers? • Have appropriate confidentiality, integrity, and availability measures been applied to data used or stored in the cloud?
Privacy Policies	• Is PII going to be stored/processed by the cloud services? • Is the Department aware of data protection laws and regulations applicable? • Does the CSP's services have appropriate controls in place for handling PII? • Are responsibilities for handling PII stated in the cloud service agreement? • Are there appropriate data residency restrictions in the Cloud Service Agreement? • If there is a data breach, are responsibilities for reporting and resolving the breach clearly outlined, including priorities and timescales?
Assessing security for cloud applications	• Based on the cloud services model used, is it clear who has responsibility for the security of the applications (Department or CSP)? • If it is the Department, do they have policies and methodologies in place to ensure the appropriate security controls for each application?

Security Step	Guiding Questions for Security Assessment
	• If it is the CSP, does the cloud service agreement make the responsibilities clear and require specific security controls to be applied to the application? • In either case, does the application make use of appropriate encryption techniques to protect the data and the user's transactions?
Ensuring Cloud Network security	• Is network traffic screening possible? • Does the CSP have the provisions to deal with distributed denial of service attacks? • Does the CSP's network have intrusion detection & prevention? • Does the CSP have the provisioning for logging the network and providing notification? • Is separation of network traffic possible in a shared multi-tenant provider environment?
Ensuring controls for physical infrastructure security	• Can the CSP demonstrate appropriate security controls applied to their physical infrastructure and facilities? • Does the service provider have facilities in place to ensure continuity of service in the face of environmental threats or equipment failures? • Does the CSP have necessary security controls for their personnel?
Managing security terms in cloud service agreements	• Does the cloud service agreement specify security responsibilities of the CSP and of the Department?

Security Step	Guiding Questions for Security Assessment
	• Does the service agreement have metrics for measuring performance and effectiveness of security management? • Does the service agreement explicitly document procedures for notification and handling of security incidents?
Understanding security requirement in exit process	• Is there a documented exit process as part of the cloud service agreement? • Is it clear that all cloud service customer data is deleted from the provider's environment at the end of the exit process? • Is cloud service customer data protected against loss or breach during the exit process?

5.3 Next Generation Model in Cloud Security – Zero Trust

The term 'zero trust' was coined by a Forrester Research Inc. analyst in 2010 when the concept's model was first presented. A few years later, Google implemented zero trust security in their network, that led to a growing interest in adoption within the tech community.

Zero trust security is a next generation IT security model that requires stringent verification of identity for each device and person trying to access resources on a private network, regardless of their position within or outside of the network perimeter. There is no specific technology that is associated with zero trust; it is rather a holistic and comprehensive approach to network security that encompasses several different technologies and principles.

Traditional IT network security is based on the castle-and-moat concept. In castle-and-moat security, obtaining access from outside the network is difficult, but there is by default trust for everyone inside the network. The limitations with this approach are that when an attacker gains access to the network, they have a free rule over everything that is available inside. This limitation and vulnerability in castle-and-moat security systems is worsened by the fact that Organizations/Departments do not have their data in just one place. In the present day, information is often spread across cloud service providers, making it even more difficult to have a single security control for an entire network.

Departments may adopt a zero trust microsegmentation strategy that allows traffic to flow between approved systems and connections, regardless of the environment they are in.

Zero trust security means that by default, not everyone is trusted from inside or outside the network, and verification is mandatory for everyone trying to access the resources on the network. This additional layer of security has been introduced to prevent data breaches.

5.3.1 Principles of Zero Trust Model

With Zero Trust all users are presumed to be untrustworthy. The primary concept behind a zero-trust network assumes that there exist potential attackers both inside and outside the network, so no machines or users should be trusted automatically. According to Forrester Research, the principles of Zero Trust Model are as follows:

- Ensure only legitimate traffic or application communication is allowed by segmenting and enabling Layer 7 policy.

- Leverage a least-privileged access strategy and strictly enforce access control. This means users should only be given access as per the need and the requirement, on a need-to-know basis. This minimizes user exposure to sensitive parts of the network.

- Inspect and log all cloud traffic. Otherwise, it may be considered simple for an attacker to access a Department's network

- Zero trust networks utilize the concept of microsegmentation. Microsegmentation is the practice of breaking up security perimeters into small zones and maintain separate access for separate parts of the network. Example, a network with files residing in one data centre that adopts microsegmentation may consist dozens of separate and secure zones. A program or person with access to any one of these zones shall not have access to any of the other zones without separate and unique authorization.

- Multi-factor authentication (MFA) is also at the core of the zero-trust model. MFA simply needs more than a single piece of evidence for user authentication; simply entering a password is not enough to access. In addition to password entry, cloud services users are required to enter a code sent to another device, such as a mobile phone, thus enabling a two-factor authentication.

- In addition to user access control, zero trust also needs strict controls on device access. Zero trust systems need to monitor the number of distinct devices that are trying to access their network and ensure that every such device is authorized. This minimizes the attack surface of the network further.

Implementing zero trust security through cloud-based architecture is more cost-effective and flexible for organizations of any size or type. Without the associated upkeep of on-prem hardware, IT teams can enjoy increased security without sacrificing ease of use.

Important points to remember

- Begin with passive application discovery by closely monitoring the network. Allow for discovery of the relationships in place along with coordination with relevant stakeholders who understand what normal traffic patterns and intersystem communications look like. Once the appropriation of relationships along with application behavior are confirmed accordingly the enforcement policies should be enacted.
- Design a zero-trust architecture based on data movement across the network and the ways in which users and applications access sensitive information. This will assist in determining how the network should be segmented. It may also assist security teams in identifying positioning of access controls between the borders of different network segments.
- Implement monitoring and real-time audit to track all privileged sessions and metadata, auditing everything across all systems to paint a comprehensive picture of intentions and outcomes.

5.4 Standards applicable for Security

To facilitate the planning on information security management for the Government Departments, there is comprehensive list of NIST Controls referred from published document "**Indian Governmental Cloud Selection Framework**" on MeitY Portal.

There are certain internationally recognized information security standards highlighted below which department can follow while adoption of cloud platform:

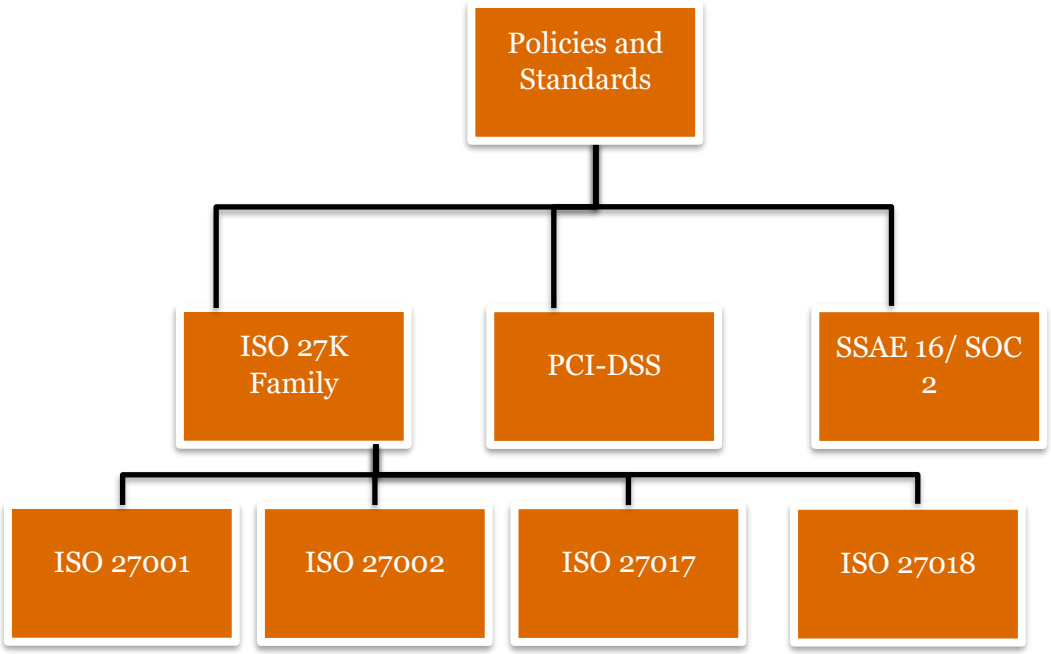


Figure 3: Standards in Information and Cloud Security

ISO 27001

This standard provides best practice to an Information Security Management System (ISMS). This Management System Standard is designed to manage an organizations sensitive data along with its set policies and procedures. Absence of ISMS makes the organization vulnerable to cyber-attacks and data leaks. Therefore, this system is a critical component within an organization.

ISO 27002

ISO 27002 Standard is all about the guidelines for organizational Information Security Management System (ISMS) practices including the selection, implementation and

management of controls taking into considerations the organization Information Security Risk environment.

ISO 27017

ISO 270017 is designed to assist in implementation of controls for cloud-based organizations. This standard is relevant to organizations who store information in the cloud, but also for organizations who provide cloud-based services to other organizations who may have sensitive information.

ISO 27018

ISO 27018 is for cloud computing organization, specifically designed to protect Personally Identifiable Information (PII) stored and/or processed in the cloud. The primary focus of this standard is relevant to cloud providers and not cloud consumers. This standard gives additional level of confidence to consumers, specifically when working with organizations who handle sensitive information.

5.4.2 PCI DSS

Cloud security is the shared responsibility between the Cloud Service Provider (CSP) and its users / clients. If card payment data is stored, transmitted or processed in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the client's usage of that environment. The allocation of responsibility between client and provider for managing security controls does not exempt a client from the responsibility of ensuring that their cardholder data is properly secured according to applicable PCI DSS requirements. Payment Card Industry Data Security Standard (PCI DSS) comprises of a set of logical, procedural and physical security requirements for organizations that process credit and debit card transactions, as well as payment applications. All organizations that store, process or transmit cardholder information, need to comply with this standard.

5.4.3 Sector specific standards

SSAE 16/ SOC 2

Statements on Standards for Attestation Engagements No. 16. SSAE 16 requires Data Centre organizations, to provide written report that describes controls at organizations that provide services to customers.

SOC 2 is a report which focuses on controls at service provider relevant to security, processing integrity, availability, confidentiality and privacy of a system. It ensures customers that their data is kept private and secure while in storage and in transit and which is available for the customer to access at any time.

5.5 Cloud Security in a Multi-cloud/ Hybrid Cloud environment

Securing a hybrid IT environment that is operating from across multiple Clouds is an uphill task. Government Departments intending to function from a mix of on-premise and Cloud systems would believe that the hybrid model is more secure than the exclusive in-house systems. Hence, improved security would act as an important factor to increase their usage of the hybrid or multi-cloud services. Until recently, many CSPs didn't have the necessary controls or guarantees of compliance and security that the Government Departments would expect, but that setup has changed radically.

Multicloud refers to the use of multiple Cloud and storage services within a single heterogeneous architecture. This heterogeneous environment also refers to the distribution of Cloud assets, software, applications, etc. across several cloud-hosting environments. With a typical multicloud architecture, using two or more public Clouds, or multiple private clouds, this multicloud environment intends to eliminate the dependency on any single CSP.

Protecting the Cloud infrastructure is mandatory for the selected CSP, but it is the Government Department's responsibility to secure any data that it puts into the Cloud. Therefore, ultimately the Government Department needs to carry out the necessary due diligence while selecting the CSPs/MSPs in order to ascertain that they meet the applicable regulatory and security requirements.

The emphasis in a multi-cloud environment shifts from securing the perimeter of the network to securing data everywhere it is, at rest or in transit

Pertaining to the department's responsibility to safeguard its data, the importance in a multi-cloud environment shifts from securing the perimeter of the network, to securing the data - whether at rest or in transit. In a multi-cloud environment, the focus is to comprehensively understand data flows and protect it in accordance to its degree of sensitivity.

Certain measures which may be kept in mind while considering a multi-cloud deployment/ environment are as follows:

- Department's central strategy towards security

  To identify threats across a hybrid multiple Cloud platform, and effectively integrate security strategies to address needs of each of the Cloud platforms, department's internal security teams or MSPs would need to centralize the security control in order to maximize

data visibility. Information about all security measures and tools implemented is needed to be shared across the identified points of contacts that are responsible for each Cloud platform, to advance the department's security capabilities. Having a uniform protocol for security enforcement helps ensure a consistent approach to Cloud platforms, thereby facilitating a secure integration within a multi-cloud architecture. Using third-party services for automation can help in scaling Cloud security.

- Evolve an approach for security of a hybrid multi-cloud environment

While the Departments need to ensure that their applications are up to date, it is also imperative to ensure that their security functions are constantly upgraded to meet their evolving IT landscape and its security requirements. In today's world, Cyber-attackers are continuously searching for vulnerabilities to exploit and adopting innovative ways to breach security. Monitoring threats to a multi-cloud architecture is a continuous process that requires security experts to constantly analyze the security of the multi-cloud through real-time reports.

- Secure communications that run the application

Even though the communications between applications in a multi-cloud environment and within the applications themselves are secure, many Departments may neglect to protect the communications that are designed to control how the applications function. This is known as the control plane, and a good multi-cloud security strategy should take into account the necessity to encrypt communications that come within the domain of the control plane. Department's security teams need to ensure encryption of these communications that control container and virtual machines. Often, these communications are left unencrypted and unsecured, thereby allowing the possibility of exploitation of these weak areas by malicious entities.

- Ensure that Departmental employee's follow security protocol

One of the biggest security breaches would comprise of situations where certain end users would have access to unauthorized data and services. When unrelated people are allowed access to unauthorized or sensitive data, they are at risk of exposing the data to security breaches and even cyberattacks. In such cases, Departments need to confirm that any acquired software is patched and secured before rolling it out to its employees. Employees also need to be trained to adhere to the stringent security protocols that are designed to prevent the occurrence of a security breach.

In order to maintain security controls throughout the Department's hybrid or multicloud deployments, Cloud Access Security Brokers (CASBs) may also be utilised.

CASBs (or Cloud Security Gateways) discover internal use of cloud services using various mechanisms such as network monitoring, integrating with an existing network gateway or monitoring tool, or even by monitoring DNS queries. After discovering the services that users are

connecting to, most of these products then offer monitoring of user activity on approved services, majorly through API connections (whenever available) or inline interception (man in the middle monitoring). Many support security alerting, including DLP and also offer controls to effectively manage use of sensitive data in Cloud services (SaaS/PaaS/and IaaS).

Regardless of where the application is deployed, security policies need to be maintained as per the policy definitions. This can be achieved by utilizing a centralized policy management solution which spans across different Clouds and data centre facilities. This solution needs to have the capability to uniformly enforce, monitor and manage the policies.

Infrastructure and application logs from the multiple CSP environments interacting to provide services, should be gathered at a central location to facilitate centralized security monitoring, incident management and event analysis. This will enable a single view of emerging threats across the organizations' data assets. This solution shall be based on Artificial Intelligence (AI) / Machine Learning (ML),with capabilities of User and Entity Behavior Analysis (UEBA). This would help in reducing the efforts and time taken to detect anomalies, which in turn reduces the incident contentment time and thus a reduced cost of data breach.

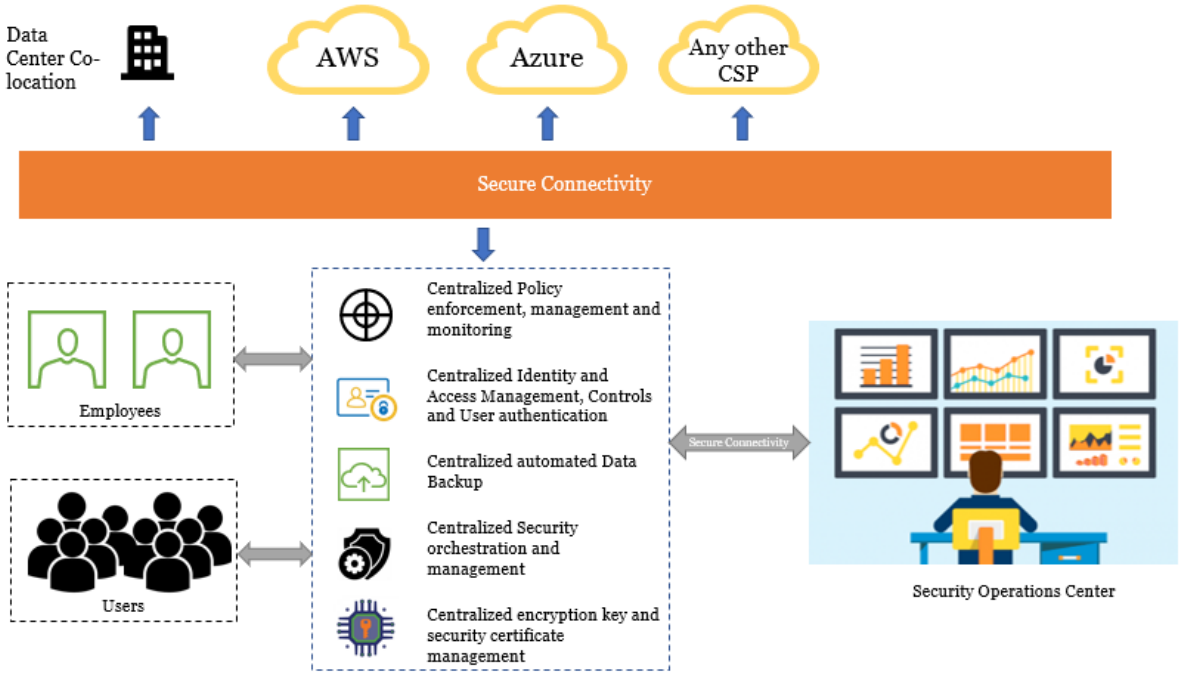


Figure 4: Cloud Security in a Multi-Cloud Environment

All end users should go through a centralized identity access management solution (IDAM solution). . This solution is capable of accommodating multiple user identities and managing

different user types, facilitating a single sign-on mechanism and integrating or having the feature to enable multi-factor authentication.

A centralized data backup solution ensures that data from all the different environments would be made available, even during a disaster, when this information is needed the most.

Security infrastructure needs to be managed using a centralized analytics and monitoring solution across various environments. This tool may also be used for IT infra orchestration that encompasses security tools and technologies. The encryption keys and certificates can be managed from a central HSM or a key management solution.

Lastly, automated workflows and playbooks will facilitate in empowering the Security Operation Centre (SOC) through automation tools. For instance, having an automated workflow for approval of change requests.

Hence by ensuring certain practices a secure adoption of a multi-cloud deployment may be undertaken by the Departments to leverage benefits of multiple offerings of various CSPs empaneled by MeitY.

6. Cloud Security Governance

In addition to deciding whether to move applications into the cloud, Departments must also ensure their cloud computing efforts are fully integrated into their entire information security program. This means understanding the process as it fits into the ICT Resilience Lifecycle, which takes into account the **prevention aspects**, including risk management and information security, and the **reaction elements**, involving incident management and continuity planning, but also the overall governance process.

- *Governance*: As Departments decide to deploy applications in cloud environments, they must consider their overall IT security governance procedures accordingly. That process should begin with the establishment of an overall vision of how the cloud fits not only into the necessary information security procedures, but also with the goals and objectives of those procedures and a road map for establishing them.

- *Risk management*: Cloud security requirements must be aligned with overall Department-level understanding of risk levels and an internal classification of data.

- *Incident management*: As applications are deployed in the cloud, Department's every Cloud Service Provider must be integrated into the Department's overall centralized incident response procedures.

- *Continuity planning*: Business continuity plans must take into account assets moved into the cloud, and be regularly updated and tested to account for new cloud architecture and provider models.

As part of this effort, security practitioners must define the scope and boundaries of all security functions that may be relevant to cloud environments, and develop an approach to improving and monitoring the performance of all of the cloud's stakeholders, including service providers, users, and technical staff. Finally, they should provide top management with the tools needed to gain visibility into cloud security — such as a security-level dashboard — and the levers needed to manage the overall cloud computing program.

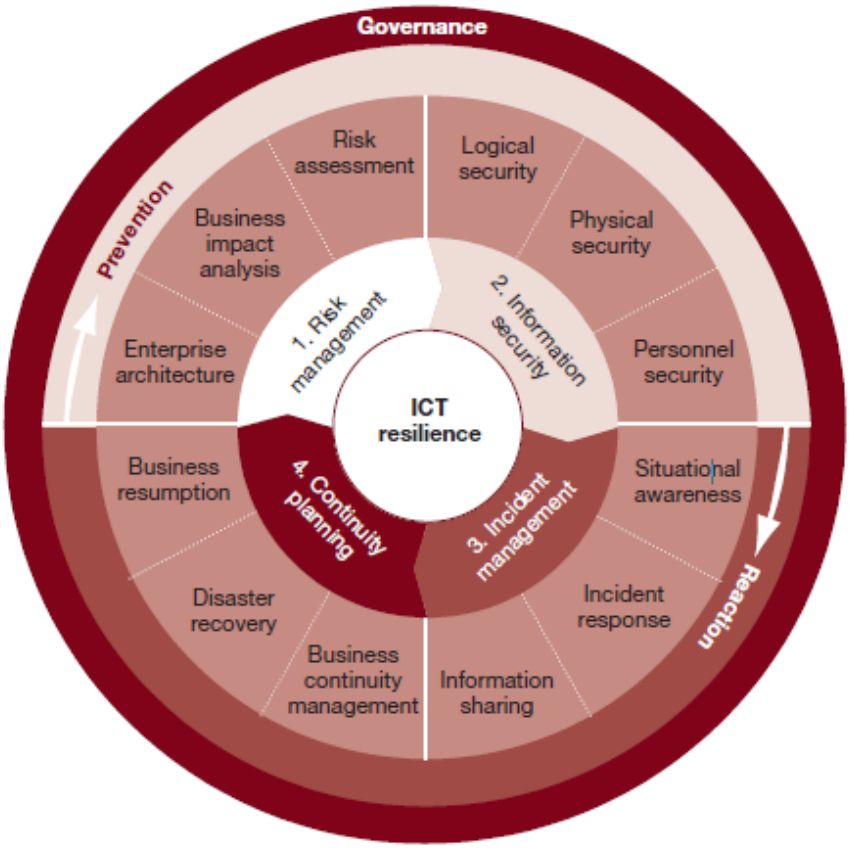


Figure 5: ICT Resilience Lifecycle

7. Cloud Security as a shared responsibility model

One of the most crucial questions while evaluating cloud is "Who is responsible for security in the cloud, the Cloud Consumer or the Cloud Service Provider?" The answer is **both.**

Cloud Computing follows the shared responsibility model to ensure adequate security measures. Securing physical infrastructure and the virtualization platform itself will permanently be the responsibility of the Cloud Service Provider. Meanwhile, the Cloud consumer i.e. the Government Department in this case, is responsible for framing and institutionalizing proper security controls, while understanding the underlying risks. For instance, deciding when to encrypt virtualized storage, properly configuring the virtual network and firewalls, or deciding when to use dedicated hosting vs. a shared host.

In continuation to the practices around cloud security, certain additional pointers which Government Department should timely monitor with respect to their cloud deployments are as follows:

- Upgrade operating system and the installed software with the latest patches.
- Ensure that the MSP / CSP solution satisfies organizational security, privacy and legislative requirements. MeitY through its empanelment RFP has onboarded CSPs which meet certain specific technical and legal requirements. Kindly refer to https://meity.gov.in/content/gi-cloud-meghraj for the list of requirements that need to be met by CSPs to get empaneled by MeitY. Additional requirements if any, may be evaluated by the Department as per their project requirements.
- Use designated computers with MFA, strong password policies, access-controlled privileges, and encrypted communication channel to administer the cloud service.
- Avoid providing the MSP/CSP with account credentials and / or access to sensitive systems outside of their responsibility.
- Use controls to protect data in transit between the Department's end and the Cloud Service Provider.
- Consider full data encryption of critical Department information while at rest, while maintaining control of encryption keys.
- Consider regular scanning and monitoring for non-standard or suspicious code/files/folders on hosts, and ensure regular audits, even if periodic scanning and audits are a service provided under contract with the MSP/CSP.

- Perform periodic cloud audit activity (every 6 months) for ensuring conformance to compliance by the CSP as per Department's project requirement.

- Employ the use of anti-malware and other security tools on Department assets and/or infrastructure. Consider tools which can both detect and remediate infections. Anti-malware programs and other security tools should be maintained and kept updated, and all executables downloaded to Departments' infrastructure should be scanned before execution.

- Ensure that MSP/CSPs conduct regular reviews of network and system logs for any suspicious activity or traffic which may indicate potential compromise.

- Employ a data backup and recovery plan for all critical information. Ensure that MSP/CSP also employs data backups and recovery plans. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Since network storage can also be affected, this data should be kept on a separate device, and backups should be stored offline.

- Contractually retain the ability to receive a copy of a compromised virtual server for Department's internal forensic analysis.

Both, the CSP and the Cloud consumer have distinct responsibilities to ensure security in the Cloud environment, however, in a few areas the responsibility overlaps. In today's scenario, many security problems among cloud consumers involve misunderstanding these shared responsibility areas.

Further, it would be safe to say that there are more areas of cloud security for which the cloud consumer is responsible, rather than the provider. Government Departments who understand the basic delineation of responsibility will be a much better position to maintain a high level of cloud security.

Essentially, the CSP requires to ensure that the infrastructure built within their platform, is inherently robust and secure. On the other side, certain customizable Cloud capabilities including network configuration, account access, application management, compute configuration, and data encryption are the responsibility areas of the Cloud consumer. This shared security model—illustrated below—may be referred to for better understanding the responsibilities between CSP and the Government Departments while configuring cloud security for their infrastructure.

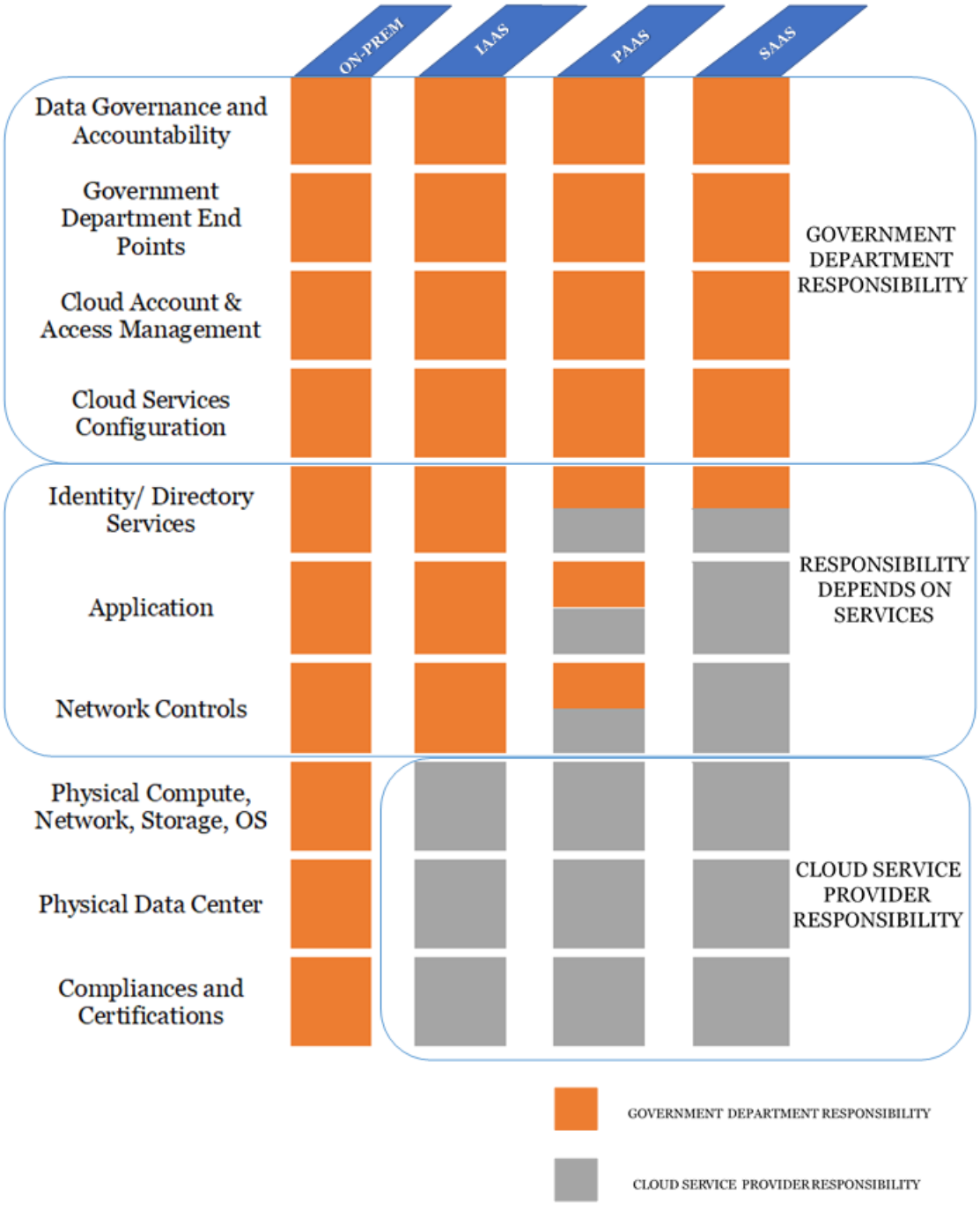


Figure 6: Shared Responsibility Model in Cloud

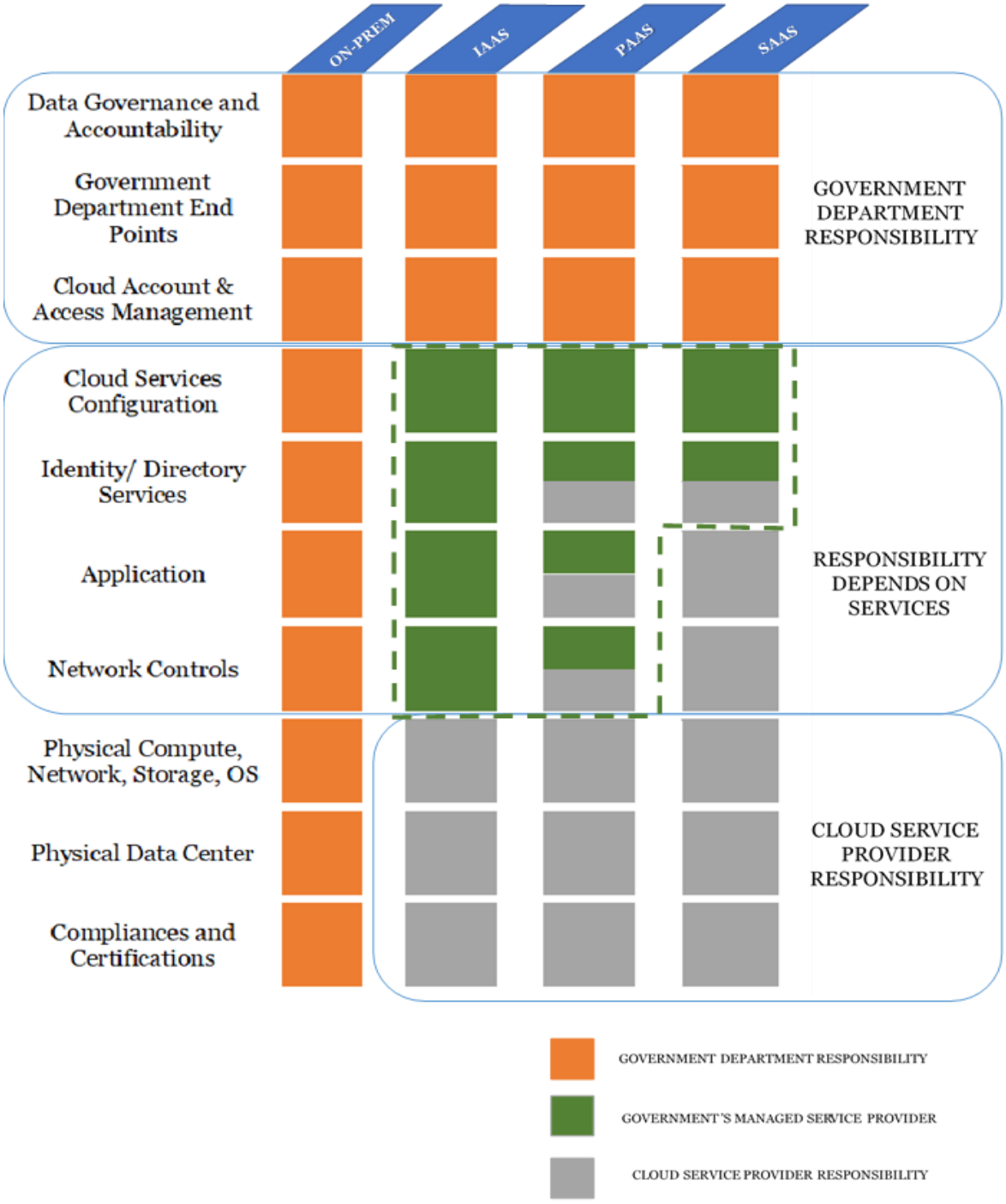


Figure 7: Shared Responsibility Model in Cloud (including MSP)

Cloud security denotes the efforts towards securing data, infrastructure and applications that are inherent to the use of Cloud computing – this includes technologies, organizational policies and controls.

In order to improve agility and reduce costs for the Government Departments, Cloud-based applications and their data, are becoming distributed. This trend is true for private clouds, public clouds (hybrid or dedicated), as well as Software as a Service (SaaS) applications.

The increasing concern over data exposure has made cloud security a priority. The challenge therefore is to balance the Department's need for agility while at the same time, improving security of applications and their data, as it travels among multiple Cloud platforms. It therefore becomes imperative to gain the necessary visibility across all locations that reside applications and data, to prevent attacks that are aimed at exfiltrating data, both through a lateral attack or from an external location.

Multiple teams may be responsible for different areas of Cloud security: application team, network team, security team, compliance team, or the IT infrastructure team. Nevertheless, Cloud security is a shared responsibility between the CSP and the Government Department.

In case of an on-premise setup, the Departments themselves are responsible for all security aspects of the Cloud, as it is hosted locally in their own data centres. This covers all areas includes the infrastructure, physical network, hypervisor, operating systems, virtual network, service configuration, firewalls, identity and access management, etc. In this scenario, the Departments own the data and also its security.

For an IaaS offering in any Cloud deployment model, the CSP owns the infrastructure, hypervisor and physical network. The Departments, on the other hand, own the workload, its applications, virtual network, access to the Cloud environment, and the deployed data.

For a SaaS setup, CSPs are mostly responsible for the security of their own platform, including physical security, infrastructure security and application security. The CSPs cannot own their customer's data, nor assume any responsibility for how the applications are used. Primarily, the Department needs to look after security to prevent and minimize the risk of malicious data exfiltration, accidental exposure, or malware insertion. In this case, the complete responsibility of application security lies with the CSP, and the Departments are responsible for necessary environmental configurations and data on Cloud.

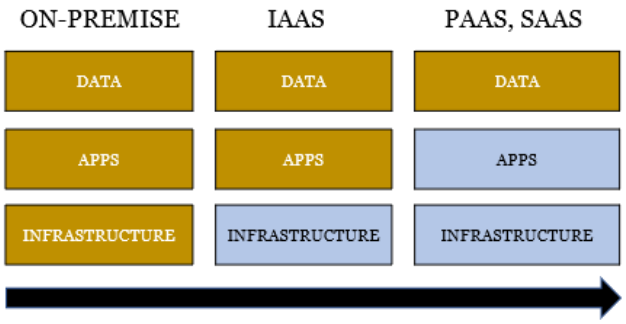
One of the key factors that should be considered while assessing Cloud versus an on-premise environment, is the responsibility of CSPs to ensure and adhere to the latest regulatory compliances and certifications, along with having the certification renewed periodically. Such governance measures may be a cost centre for the Departments in an On-premise setup whereas in cloud the CSP would be responsible for ensuring compliances to the norms needed by the Government Departments.

A detailed model describing the shared responsibility between the Government Departments and the CSP has been illustrated in ***Figure 6*** above.

In case the Department selects a Managed Service Provider (MSP) to manage their Cloud workload, ***Figure 7*** can be referred which discusses the responsibilities between the Government Department, CSP and the MSP in detail.

As Government Departments transition from an on-premise setup to either IaaS, PaaS or SaaS service, the responsibility for security of data, applications and infrastructure is the larger responsibility of the selected CSP than the Department itself. However, irrespective of the platform used, the Department will always be accountable to ensure security of its own data. To safely enable their applications, the Government Departments must be confident that their CSPs have put in place the appropriate security measures.

To compensate for what does not fall under the CSP's purview, a Department must also have the necessary tools in place in order to asses, manage and secure the risks effectively and facilitate data security. For a SaaS offering, these tools may be able to provide visibility into activities within the SaaS application, detailed analytics on the service usage to prevent risk to data and violations of compliance requirements, policy controls to necessitate enforcement and even quarantine in case a violation occurs, real-time threat intelligence on known and to also detect unknown threats to prevent new malware insertion points.



To offer a secure cloud, the CSP manages and controls multiple layers – the host Operating System (OS), the virtualization layer, as well as the physical security of its data centre facilities. To ascertain security within a given Cloud environment, the Department or it's MSP is expected to configure and manage the security controls for the guest OS, and other applications (including updates and security patches), and for the firewall as well. Hence, it is imperative for both CSPs and Government Departments to understand their roles and responsibilities with respect to security while choosing cloud for their deployments.