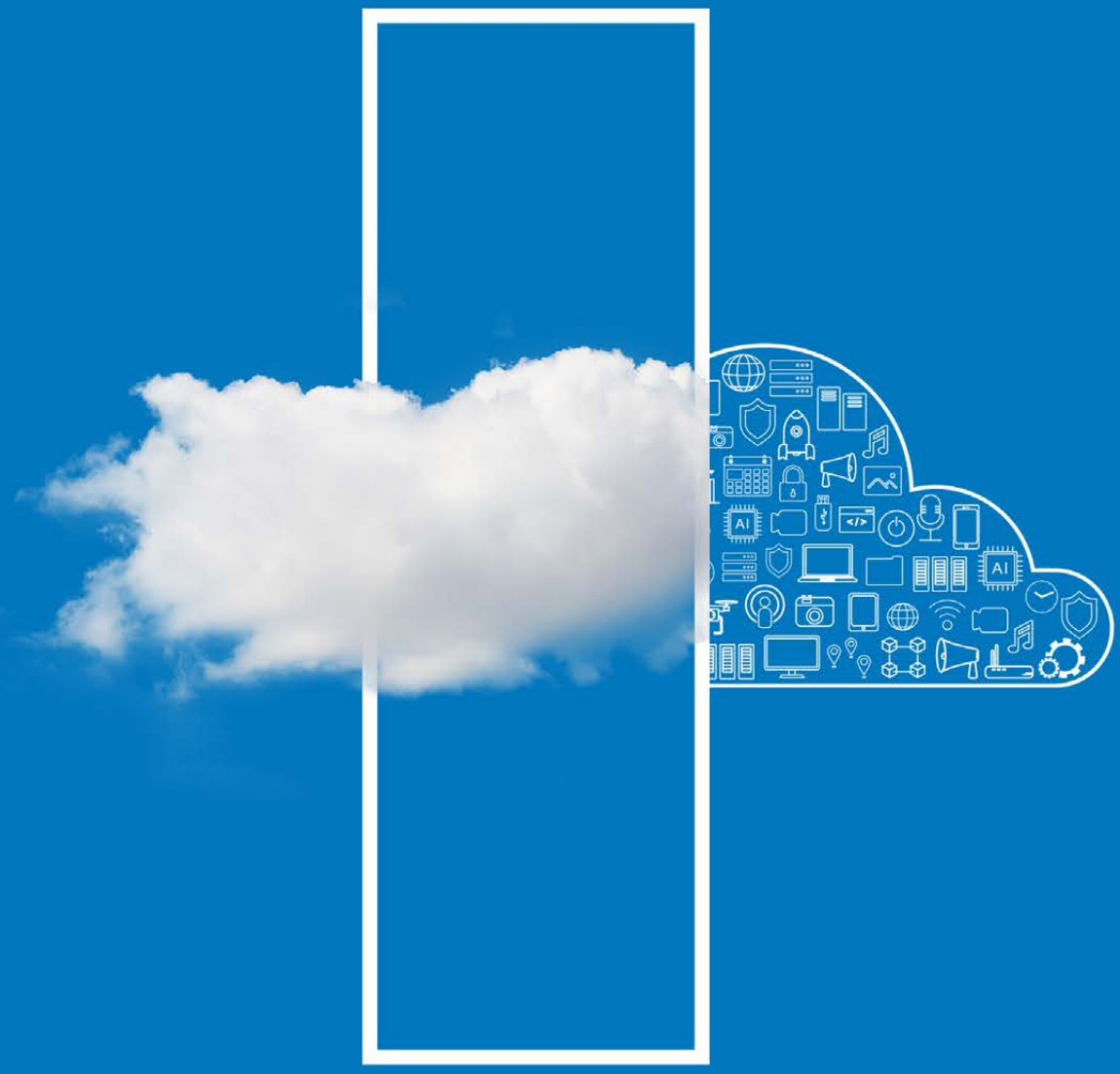
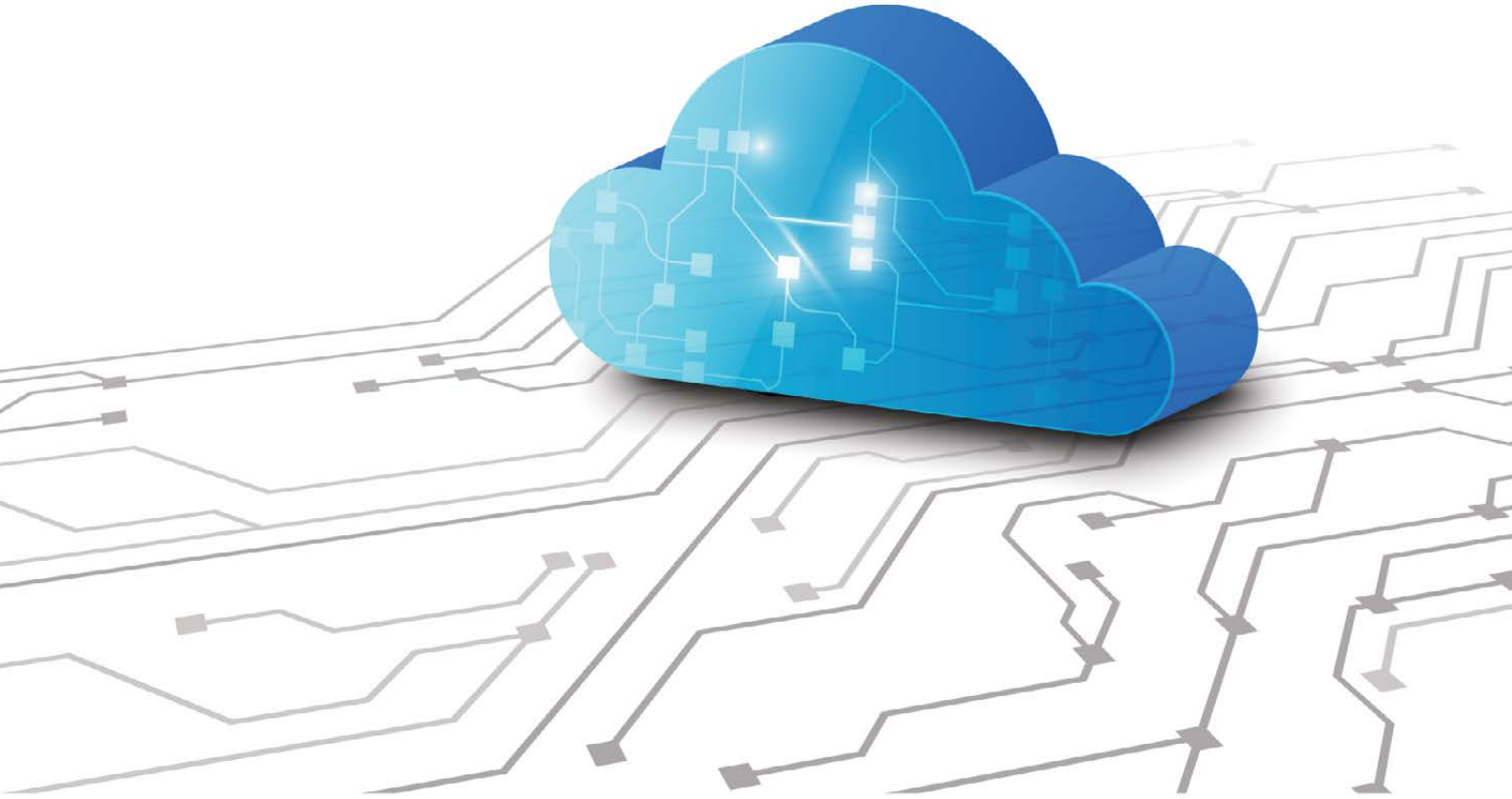
Infosys cobalt

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative



Cloud Security
Governance & Assurance
A DSCI-Infosys Point of View



Contents

Context of the POV

Cloud as a Digitization Enabler

In the current context of rapid digitization, cloud has emerged as a key enabler for organizations across the board for adopting technology at a faster pace and reaping the benefits associated with the same. Be it enhanced productivity, or the ability to attain scalability of operations or drive innovative delivery of products and services, cloud has become an integral part of the overall digitization journey. From a sectoral standpoint, banking financial services and insurance, manufacturing, healthcare, e-commerce, government, and others, have been adopting cloud and pushing the digitization agenda forward.

Securing Cloud for Enhanced Trust in Digital Economy

While the cloud adoption agenda pushes ahead, it is of utmost importance to examine the cyber risk landscape of cloud critically and holistically. Cloud environment has been the recipient of several targeted and persistent attacks and intrusions. Organizations which are already leveraging cloud and the ones which are contemplating migration to cloud often grapple with questions around security and privacy of data being accessed, availability, integrity, and legitimate use.

Enterprises should strive towards systematically dealing with the potential security & privacy threats to their cloud environments. There should be a continual attempt at adhering to sound security best practices and principles as this would pave the way for inculcating trust in the customers and consumers. However, security environment tends to be complex. On cloud, enterprises would be able to orchestrate and manage security better by using existing pool of tools, technologies, and services on the cloud. Organizations may not have all the expertise in-house to cater to all the aspects of security on cloud and may partner with other stakeholders like managed service providers, capability providers to effectively manage security on cloud.

Governing Security Affairs on Cloud

The fundamental intent and object of this POV document is to establish best practices in the area of cloud security governance and assurance. Governing security affairs of your cloud environment is indeed a pristine task and warrants disciplined implementation. This POV would serve as a guidance document for enterprises that are looking to streamline their cloud security governance program and are endeavoring to make it effective and impactful.

Objectives of the POV

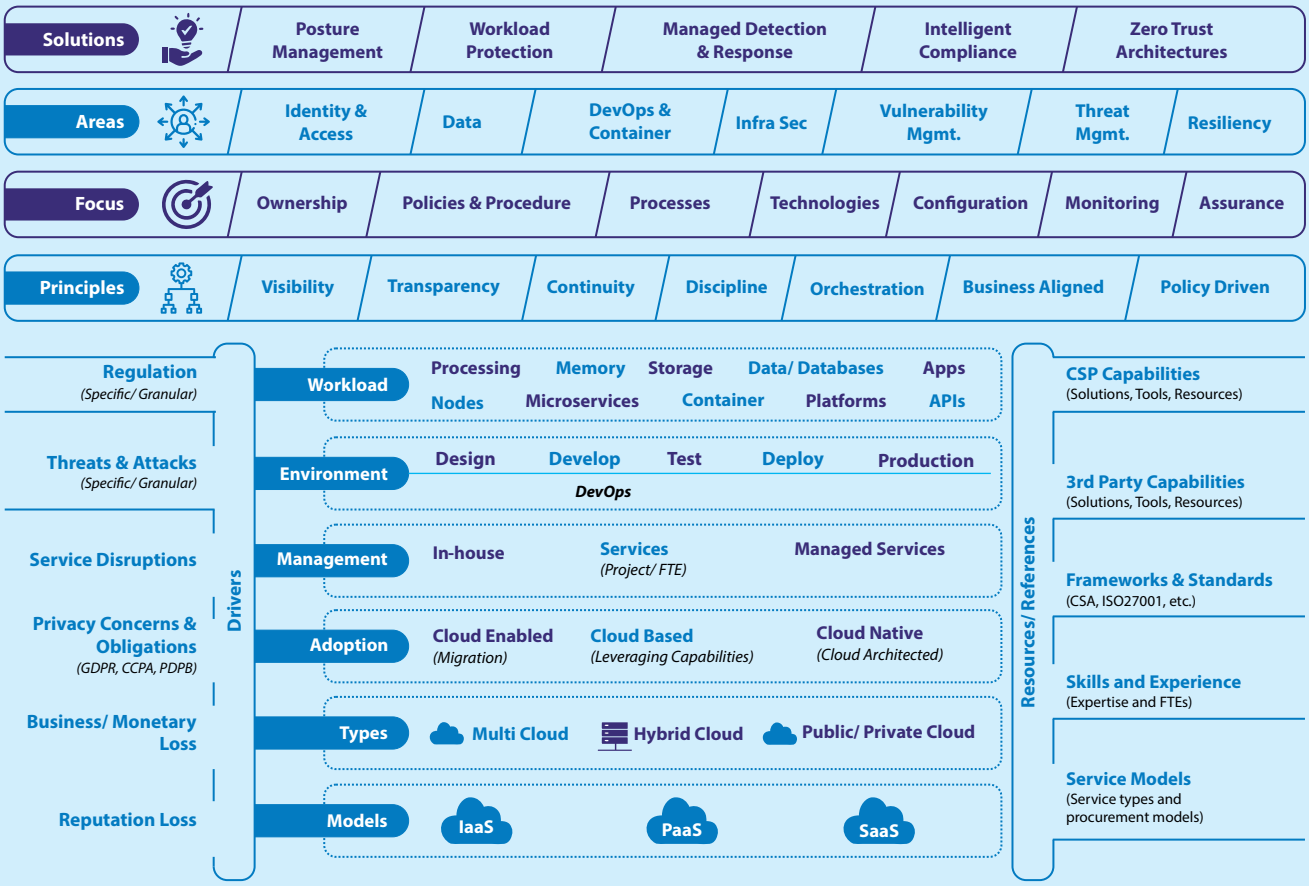
Against the backdrop of rapid digitization and burgeoning adoption of cloud to enable the same, this POV intends to accomplish the below mentioned key objectives pertaining to security governance & assurance in a cloud environment:

- Dissect cyber security governance on the cloud and examine various elements associated with it
- Comprehend the underlying guiding principles of governance and deliberate on ways of leveraging those for achieving trust in cloud
- Unveil the key drivers for having a robust cloud security governance program
- Comprehensively capture the capabilities, references, resources, and areas that hold importance from standpoint of governance
- Examine the standards and frameworks that are getting built for ensuring secured migration to cloud
- Look at ways and means of providing assurance with respect to data ownership and availability of data for building higher levels of resiliency
- Bring out the key aspects of shared responsibility model to shed light on collaborative relationship between service provider and user organization
- Evaluate the managed security services in the paradigm of cloud

Cloud Security Governance Overview

The proposed framework endeavors to bring together the key elements and components of cloud security governance & assurance to provide better comprehension of the theme

Cloud Security Governance and Assurance Framework



The encapsulate of cloud security governance in the form of a framework can be referred by enterprises looking to implement a comprehensive security governance program for their cloud environments. The top layer lists the various cloud security solutions that are implemented to secure workloads. The second layer enumerates the broad areas that form part of the cloud security governance while the third layer talks about the focus areas of the same. This is followed by the guiding principles which form the essence of the overall governance program and need to be operationalized at an enterprise level.

This encapsulate also captures the key drivers which shall be elaborated in the next section and finally the resources, capabilities and references are being talked about in the right of the diagram. At the center of these different layers and sections is the cloud infrastructure and its various models and elements that need to be secured in accordance with the cloud security governance principles and best practices.

The framework hinges upon four key pillars, first being the key drivers underscoring the importance of cloud security; second being the nature of cloud infrastructure; third talks about the existing references and resources which are being referred while managing security and finally the fourth pillar provides the template to structure and plan the security governance & assurance.

Key Drivers for Security Governance

There is rising expectation from enterprises to proactively manage the security affairs of their cloud setups. This is driven by several intrinsic and extrinsic factors which can have significant implications for businesses and their stakeholders. The key drivers for security governance are outlined below:

Business/Monetary Loss

Business/monetary loss owing to the cloud security breaches have been reinforcing the significance of cloud security governance strategy as there have been numerous instances where enterprises data is exposed owing to poor patch management, misconfiguration, weak access control, etc. The financial effect of a data breach is unquestionably one of the most immediate and severe repercussions that businesses have to face. Compensation for impacted consumers, incident response activities, investigation of the data breach, investment in new security measures, legal fees, and the regulatory fines that can be levied for non-compliance with the data protection rules are just a few examples of monetary loss.

Reputation Loss

Reputational harm from cloud security breaches may be severe for a company since customers would avoid doing business with companies that have been breached. This unfavorable situation, along with a loss of consumer trust, can inflict irreversible reputation damage to the organization that has been breached, as cloud consumers are highly concerned about data security. Reputation loss not only results in losing existing customers, but also impacts an enterprise's ability to attract new customers, as the way an enterprise manages and mitigates its cyber risk is closely related to its brand and reputation. A robust cloud security governance strategy helps enterprises to mitigate the cyber-attack which further helps enterprises to maintain their reputation.

Threats & Attacks

The advances in the threat landscape and the increasing attempts by the malicious elements to target cloud environment is pushing organizations to have sound cloud security practices in place and this is yet another driver from viewpoint of governance. Taking adequate measures to comprehensively address the vulnerabilities, threats and risks on cloud would be absolutely imperative.

Service Disruptions

Continuity of business & operations can be the most pressing concern for most organizations, especially the ones operating in the critical sectors like healthcare, power, manufacturing, et. al cyber intrusions and attacks can result in, among other things, disruption of critical services which can have far-reaching implications. A robust security governance program can preempt these service disruptions and ensure continuity of operations.

Privacy Concerns & Obligations

With the existing data privacy laws across the globe e.g., GDPR, and Indian Data Protection Bill which is underway, the liabilities and obligations pertaining to safeguarding personal data would need to be factored into enterprises' cloud security governance strategies.

Regulation

Obligations emanating from national legislations, regulatory directives form one of the primary drivers for ensuring reasonable and effective security & privacy of data on the cloud. There are several facets to this driver, including but not limited to, creating trust in digital economy, adequate measures around protection of sensitive data of end consumers, extending support for crime investigation and ensuring national security.

Security Governance in Cloud Environment

The underlying guiding principle when it comes to governance is that you take care of even the smallest element as it might lead to larger security ramifications. Hence, robust security assurance & governance framework is imperative for enterprises.

Any governance mechanism essentially comprises of three things, that is - taking every possible step to prevent unwanted instance, capability to identify and remediate any undesirable event, and lmechanism to minimize its impact.

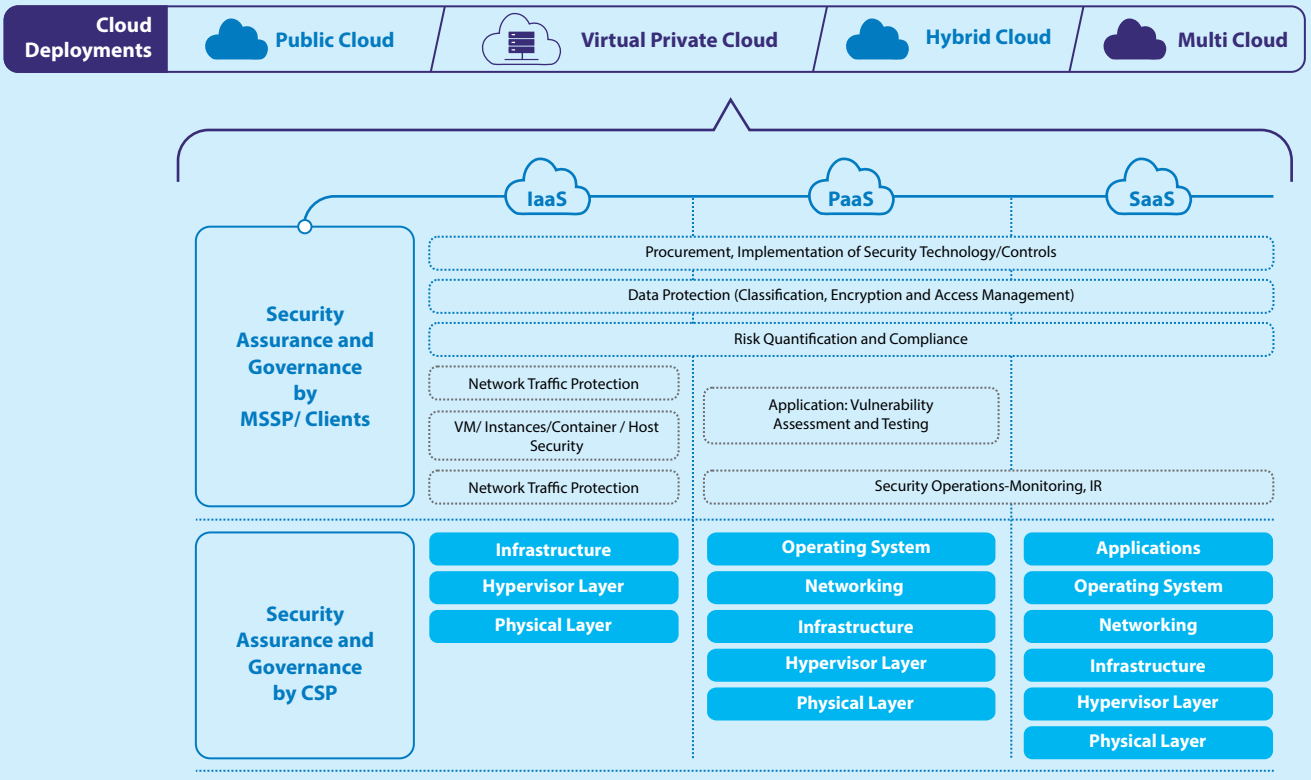
Security governance in cloud environment helps to solve challenges around business outcomes/ objectives, risk management etc. Right planning and procedures around cloud security assurance and governance shall help to answer some of the following questions :

- Are security investments on cloud yielding the desired returns?
- Is there a mechanism available for validation of security controls and their effectiveness against cyber risk in cloud?
- Are enterprises aware of their security risks in cloud and potential business impact?
- Is security risk is getting reduced to an acceptable level?
- Have we established a security-conscious culture within the enterprise?

Security assurance and governance for cloud infrastructure is directly or indirectly associated with service models, cloud deployments, adoption pattern and specific workloads. Security assurance and governance architecture, and responsibilities may change with following

1. Service model and cloud deployments
2. Adoption pattern and specific workload

Service Model and Cloud Deployment



Service Model and Cloud Deployment

Cloud governance in the context of different service models and deployment is based on shared responsibility model of security, in which cloud service providers, client and MSSPs share responsibility of data security and compliance on cloud. Whether in the data center, or using a server-based IaaS instance, serverless system, or a PaaS cloud service, user organizations are responsible for securing what's under direct control.

1. Security Assurance and Governance by CSP

Cloud service provider is responsible for risk quantification, mitigation through applying necessary security controls and protecting the infrastructure that runs all the services offered by CSP. For instance, in IaaS, cloud service provider is mainly responsible for protecting and assuring security of infra, hypervisor and physical whereas In PaaS and SaaS, additional security governance responsibilities around networking, operating systems and applications gets added.

2. Security Assurance and Governance by User Organization / MSSP

User organizations or their managed security service providers are accountable to protect host instances, network traffic, application security, procurement of security controls, active monitoring of incidents – response, data classification- encryption and compliance in IaaS- Infrastructure as service set up. In PaaS and SaaS, user organizations do not govern security of operating systems, applications, but still responsible for vulnerability management, risk quantification and implementations of security controls to ensure confidentiality and integrity of own data. Additionally, organizations maintain responsibility for securing everything in organization that connects with the cloud, including your on-premises infrastructure stack and user devices, owned networks, and applications, and the communication layers that connect users, both internal and external, to the cloud and to each other. Organizations need to set up own monitoring and alerting for security threats, incidents, and responses for those domains that remain under organization's control. These are responsibilities of customer whether running on any cloud service provider, or any other public cloud provider's systems.

Adoption and Workload

Organizations with varying scale, maturity and nature, usually adopt different service models, deployments and services.

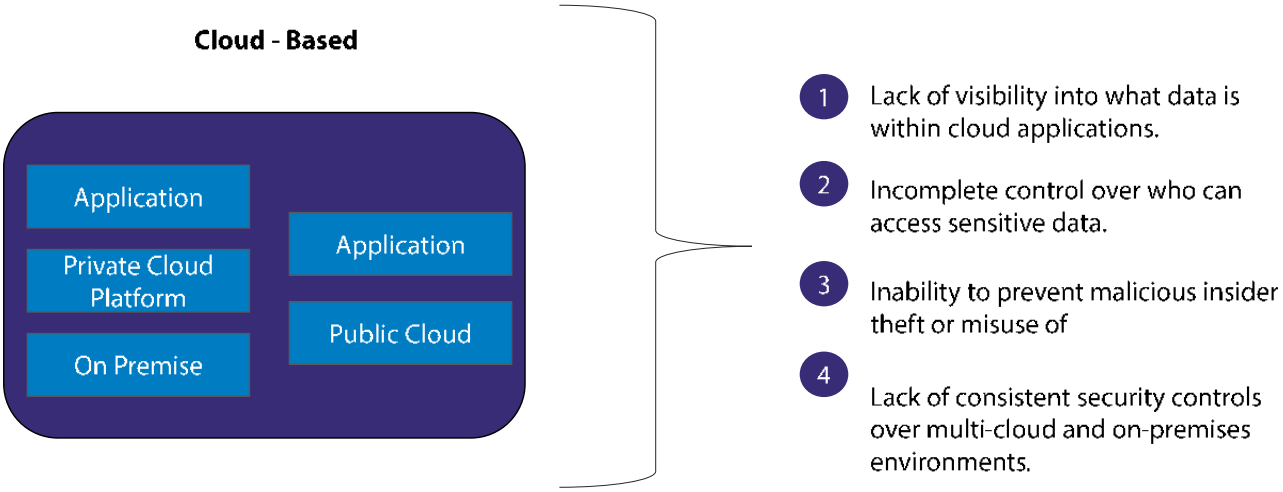
1. Cloud Based

Cloud based approach leverage some of the capabilities of the cloud such as higher availability and scalability but do not completely redesign applications to use cloud services. Once applications moved to cloud provider, user no longer responsible for managing the resources for the application, so there's no need to maintain a server or worry about backup.

A cloud-based applications/ services running in the cloud may include SaaS-based applications, as well as PaaS and IaaS-based. While SaaS-based applications will almost be cloud-based, but cloud-based services may not always be SaaS-based.

Security concerns pertinent to cloud-based applications are as follow :

- Lack of visibility into what data is within cloud applications
- Theft of data from a cloud application by malicious actor
- Incomplete control over who can access sensitive data
- Inability to monitor data in transit to and from cloud applications
- Inability to prevent malicious insider theft or misuse of data
- Lack of consistent security controls over multi-cloud and on-premises environments



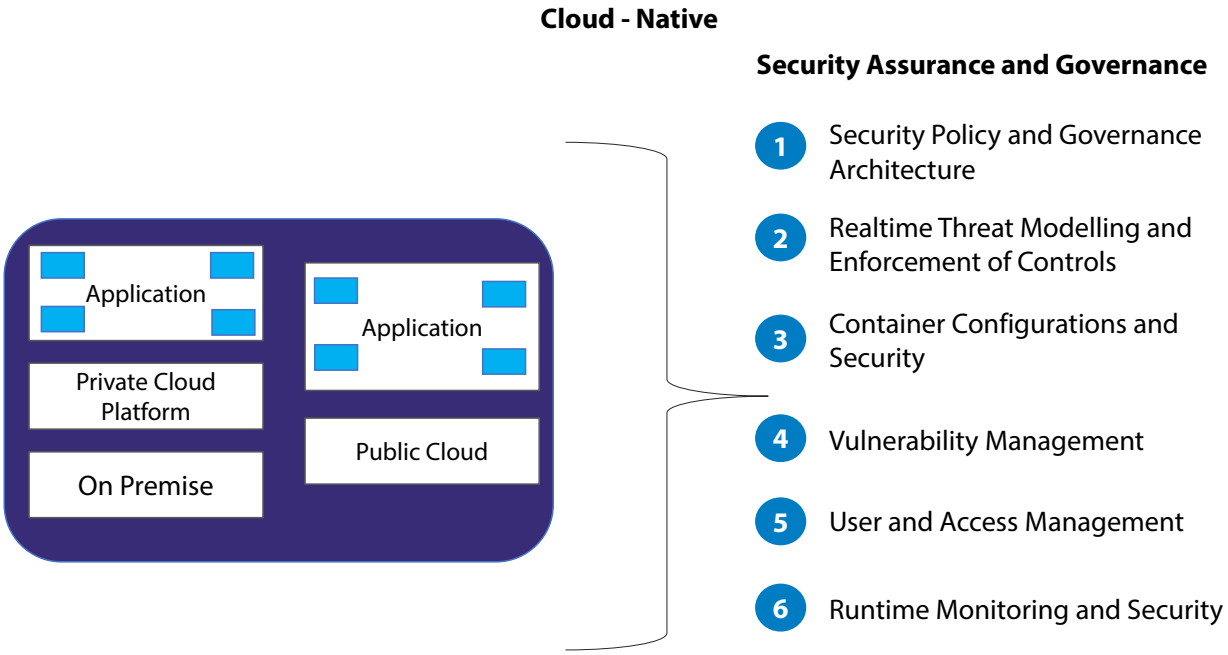
Security assurance and governance view

2. Cloud Enabled

Cloud-enabled applications are traditionally built and migrated to the cloud infrastructure, applications usually get designed in a monolithic fashion and depend on local resources and hardware. In the migration of the application to the cloud, the application is refactored to use virtual resources, but the underlying architecture remains the same. Cloud enabled can be an approach for legacy applications or as the first step towards cloud adoption.

3. Cloud Native

Cloud-native applications are architected from the ground up to run in a public cloud using cloud-based technologies. Cloud-native is comprised of continuous integration, orchestrators, and container engines; it's about how applications are created and deployed.



Security assurance and governance view

Resources & References for Cloud Security Governance

The role played by frameworks and standards in the overall security governance architecture and in providing assurance highlights its importance to achieve certain level of security. Cloud security solutions facilitate securing workloads, applications, and data in the cloud. The solutions can be used in public or private clouds and often have features for hybrid or multi cloud deployments.

Cloud Security Standards and Frameworks

Any organization with workloads processing sensitive data should strongly consider compliance with at least ISO-27001, SOC 2 and the CIS AWS Foundations benchmark as a starting point.

Implementing processes and controls for these standards will go a long way to ensuring data security. Taking it to the next level; certification with ISO and attestation with SOC 2 will increase trust in your organization and can gain your organization competitive advantage amongst security-conscious customers. There are other clear business benefits to implementing these frameworks such as avoiding financial loss resulting from a security breach, ensuring data privacy and integrity, regulatory compliance, and defining information-handling roles and responsibilities.

ISO-27001 / ISO-27002

Any organization that has sensitive information can benefit from ISO 27001 implementation. ISO-27001 contains a specification for an Information Security Management System (ISMS). ISO-27002 describes controls that can be put in place for compliance with the ISO-27001 standard. Compliance with ISO-27001 demonstrates to your customers that your organization takes information security seriously and has implemented the best-practice information security methods.

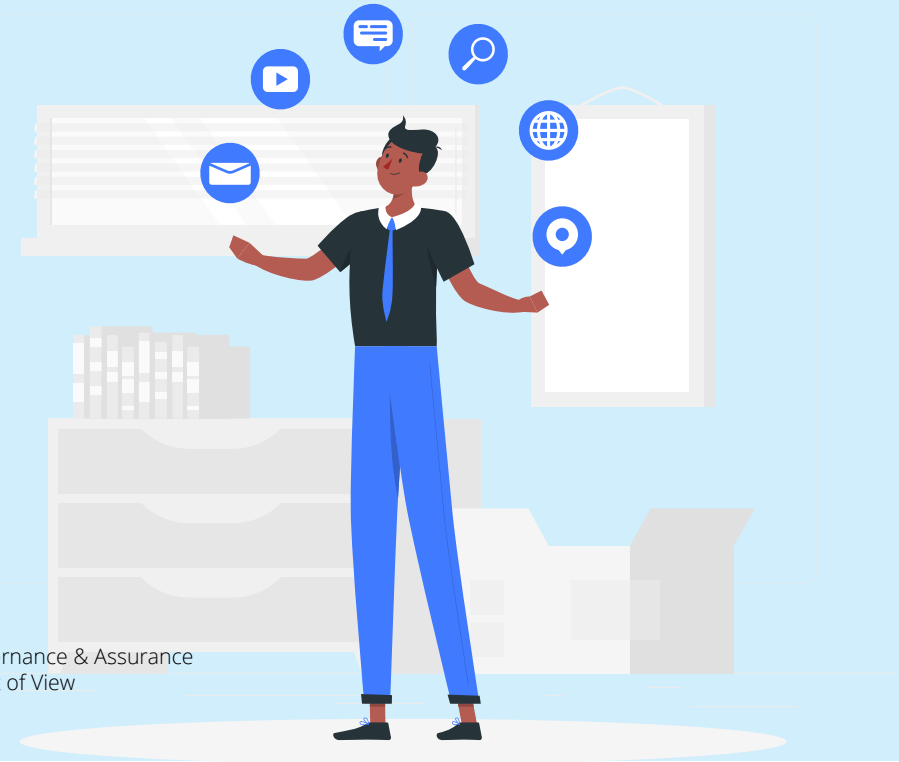
ISO-27017

An extension of ISO-27001 incorporating clauses specific to information security in the context of the cloud. Compliance with ISO-27017 should be considered alongside ISO-27001.

Although the number of standard and control frameworks may seem overwhelming at first, common themes appear across many of the standards. Striving for compliance with one will often get you a long way to achieving compliance with another.

Cloud Security Alliance (CSA) Cloud Controls Matrix

The CSA has published a cloud controls matrix that provides insight into the key security control considerations when assessing cloud provider services. This document is helpful in establishing effective cloud security governance.



Gaps/ Challenges in Cloud Security Assurance and Governance

Resources, references, and standards shall help organizations to achieve certain level of security governance and assurance. However, due to the surge in number of business transactions, multi-stakeholder environment and complex scenarios, there is a possibility that organizations may lag behind with regard to certain security gaps and challenges. These challenges or gaps may not be limited to the following:

1. Lack of understanding about dynamic and sophisticated cloud-based threats
2. Non-alignment of businesses objectives/ values with risk mitigation plan
3. Insufficient or fragmented cloud assurance and governance framework
4. Multi/hybrid cloud makes assurance and governance complex
5. Implementation inappropriate security controls with no validation
6. Weak cloud security policies with limited coverage
7. Inability to comply with multiple regulations and legislations
8. Lack of third party or vendor risk management strategy/ plan

Cloud Security Assurance and Governance Framework

1. Principle

Cloud security governance principle may differ from organization to organization but there are seven cloud assurance and governance principles used to monitor cloud environments. By taking these principles into account, organizations will be able to better manage compliance, governance, business goals, cost and data security.

Principles				
	Visibility	Transparency	Continuity	Discipline
	Orchestration	Business Aligned	Policy Driven	

I. Visibility

According to the Oracle and KPMG Cloud Threat Report, 82% of cloud users have experienced security events due to not having enough visibility on shared security responsibility model and the lack of clarity on this foundational cloud security construct.

When it comes to creating visibility on cloud, many user organizations are not fully aware about cloud infra, running assets, applications, and necessary security controls. Enterprises are also skeptical and have certain questions such as

- What happens to data if organization leave a service provider?
- What if organization do a Proof of Concept (POC) with a cloud service provider and I put up data up there?
- What if we decide not to renew after two years, then what is the disposition of that data in the cloud and who will erase it?
- Does it get erased? This can become a big problem, especially around compliance and an issue around some of the visibility.

Creating good visibility over data, assets, applications, processes, and procedures on cloud is one of the key principles of cloud security assurance and governance.

II. Transparency

Today, organizations are almost ready than ever to embrace the cloud, whereas many remain concerned about having transparency over data security readiness of cloud service providers. Organizations are also remained worried about their ability to enforce security requirements at the cloud services.

Transparency over cloud service providers capabilities, own security controls, traffic, data and processes shall ensure better governance on cloud. This includes:

- Mitigating security concerns, through several practices, such as allowing onsite audits, adopting industry standards, conducting background checks on employees, or maintaining interoperability with existing enterprise security controls.
- Transparency over dense data transactions, network traffic, and processes through continuous monitoring and automation.

Organizations seeing security as critical to cloud adoption, greater transparency is one of the key components and become a competitive differentiator.

III. Continuity

Continuity remains a strategic imperative, growing in importance as business sees

challenges from uncertain events, and highly targeted cyber-attacks. However, there is need of the hour to examine gaps in existing security programs and cyber resiliency plans which shall stay sustained in years to come.

Moving to cloud systems can make business more efficient, more adaptive, and ultimately more profitable but it requires careful planning, especially when it comes to thinking about business continuity in the cloud. Sometimes businesses/ user organizations are forgetting about critical aspects of their business continuity planning and assuming their cloud provider will be handling them. In the context of different cloud adoption patterns and service models, understanding continuity/recovery principles and ownerships are key elements of cloud governance.

IV. Orchestration

Orchestration enables the creation and execution of predictable, repeatable processes of security compliance, monitoring and governance which can be automated. Not only does this help in terms of establishing a consistent, reliable IT environment, but it also eliminates costly human error, security gaps and non-compliance which ultimately improves the organization's business efficiency on cloud.

- Managing security policies is an arduous task that requires automation, and Security policy, compliance orchestration has emerged in response to numerous factors happening in tandem.
- Security policy orchestration helps to alleviate that pressure, enabling operation teams to keep up with the demands of the business while ensuring security and preventing an outage or data breach.

V. Business Aligned

Risk and security should partner with leadership and the board to create good security assurance and governance across the organizations – People, Process and Technologies that aligns with the business objective.

Business understands the value of security assurance and governance on cloud and sees it as a component of managing business risk, whether it be operational, regulatory, or reputational. In cloud environment cyber risks are discussed in line with the enterprise risk management function and the discussion of those risks is shifting from a qualitative to quantitative view of potential impacts to the business.

VI. Policy Driven

A cloud security policies and governance are pivotal to the success of a business's operations in the cloud. Policy driven cloud security can be combination of people, processes, technology, working together—the people being stakeholders and the executive level, the processes being the procedures for amending policies when necessary, and the technology being the mechanisms that monitor compliance with the policies.

2. Focus

Data breaches, system vulnerabilities, insufficient identity, and credential and access management are some of the typical security challenges in the cloud environment that enterprises must address as a priority. An enterprise may lack adequate focus on operationalization and enforcement of policies, procedures, a formal operating model, or even a properly constituted organizational function to effectively manage security in the cloud, close focus around following seven areas adds good value to cloud security governance.

Focus	Ownership	Policies & Procedure	Processes	Technologies
	Configuration	Monitoring	Assurance	

Ownership is listed as one of the important focus areas as part of the proposed governance framework in order to address the critical concern of users around control of the data residing on the cloud. The real ownership may be incumbent upon the nature of data stored as well as the fact as to where it was created. Thus, it is important to appreciate the specific meaning of data ownership in context of cloud.

Putting in place policies and enforcing them in a meaningful way would be vital part of cloud security governance strategy. Making complete sense of data and classifying it so that the appropriate security measures can be implemented according to the varying levels of data sensitivity. Also, developing policies to facilitate security practices can't be a siloed exercise. The business objectives have to necessarily be considered and this in turn necessitates involvement of various business areas and the senior management.

Monitoring compliance with the cloud security governance policies can be effectively accomplished by leveraging technological tools.

Cloud configurations can be intricate in nature and even a single misconfiguration in any of the services may have serious security ramifications by leaving applications vulnerable to intrusions. Proactively identifying and remediating misconfigurations to reduce risk and ensure compliance is critical to maintaining a robust cloud security posture.

3. Areas & Solutions

Solutions	Posture Management	Workload Protection	Managed Detection & Response	Intelligent Compliance	Zero Trust Architectures

Areas	Identity & Access	Data	DevOps & Container	Infra Sec	Vulnerability Management	Threat Management	Resiliency

Identity & Access

As more companies migrate to the cloud, companies search for security measures to authorize and authenticate internal and external users, but they do not want to negatively impact the user journey with troublesome authentication methods. Identity-as-a-service is expected to grow aggressively over the next few years as more businesses look to reap the benefits of cloud computing. The goal for companies is to validate the identities of both consumers and employees from the cloud, but in a seamless and

painless manner for users. One component of a strong security posture takes on a particularly critical role in the cloud – identity. Public cloud providers offer a rich portfolio of services, and the only way to govern and secure many of them is through identity and access management. IAM is a cloud service that controls the permissions and access for users and cloud resources. IAM policies are sets of permission policies that can be attached to either users or cloud resources to authorize what they access and what they can do with it. IAM is a crucial, aspect of cloud security. Businesses must look at IAM as a part of their overall security posture and add an integrated layer of security across their application lifecycle. Beyond identity, how to enterprises are governing & reconciling the identities, roles and access management policies is key aspect of cloud IAM.

DevOps & Container

Container users need to ensure they have purpose-built, full stack security to address vulnerability management, compliance, runtime protection, and network security requirements of their containerized applications. the container security solutions that organizations can rely on have grown in terms of both capabilities and sophistication. Regardless of what level of DevSecOps maturity has been attained, container security tools are now more accessible than ever. The shift left approach of security where, security solutions are embedded as part of the infrastructure and application provisioning through codification ensures that cloud security governance and assurance is built in from day zero.

Vulnerability Management

Vulnerability management plays an essential role in cybersecurity. Traditional vulnerability management of on-premises hosts (physical or virtual machines) cannot scale to cloud environments. To cope with rapidly-changing cloud environments, vulnerability management needs a new approach. Vulnerabilities of workloads are not only the key challenges but also the cloud control plane which includes security misconfigurations needs to be addressed well to ensure cyber resilient cloud environment.

Resiliency

The right decisions on cloud are critical for organizations to reduce the overall spending and increase the ability to respond to cloud related risks, threats, and opportunities. Yet however necessary, identifying requirements, risks, prioritizing them and allocating funds to address them is not always easy. In order to do this, organizations need to gather and analyze the right information to make value-driven decisions regarding the cost-effective management of risks related to resiliency. Whether migrating workloads to cloud-based platforms or pursuing a Disaster Recovery as a Service (DRaaS) model, cloud requires a fundamental shift in thinking about integrated enterprise risk management. While there is a pervasive lack of resiliency planning in most cloud implementations today, better up- front assessment and planning can help organizations realize the enormous potential cloud offers for improved, more agile resiliency and strike the right balance between business service availability requirements and tolerance for risk.

Intelligent Compliance

The expectations and obligations arising from the increasingly complex compliance and regulatory landscape merit meticulous attention from governance standpoint. Vis-à-vis cloud environment, complying with various legislations pertaining to protection of sensitive personal information and data becomes critical for enterprises. When moving to the cloud it is important to know in which countries your data will be processed, what laws will apply, what impact they will have, and then follow a risk-based approach to comply with them. Financial institutions must confront the reality of dramatically increasing costs while also keeping pace with the legislative and regulatory changes arising from numerous regulatory bodies. Global organizations have the added burden of even more international and nation-specific regulations. Noncompliance has costs. Regulatory violations involving data protection, privacy and disaster recovery can have severe and unintended consequences

Cloud security governance through automation e.g. auto remediation, auto scaling to ensure no business disruption happens

Integration of automation with the cloud security governance strategy enables organizations to ensure to have continuity in business operations. Automation tools and governance policies help enterprises to achieve consistency and control over the cloud environment and also it alerts stakeholders of policy infractions and automates corrective procedures so that change may be implemented to ensure cloud security. Implementing auto-remediation in a cloud environment helps enterprises to build a cloud management platform that supports policy-driven automation to enhance the business's cloud governance by automatically remedying the event that caused the policy violation. On a similar hand, enabling auto-scaling with cloud computing supports users with an automated approach to increase or decrease the compute, network service, and storage and to meet the workload demand to ensure business continuity with no disruption.

Disaster recovery and business continuity through right design can ensure the assurance of the cloud environment.

Disaster Recovery (DR) is an important aspect of business continuity and to ensure the assurance of the cloud environment. After a disaster over a cloud or data loss in cloud, DR lets organization to swiftly restore important systems/data/files and provide remote access to systems in a secure virtual environment. Disaster Recovery as a Service (DRaaS) by security service providers allow enterprises to backup and store data to regain access and functionality to IT infrastructure after a disaster. Disaster in cloud or data loss in cloud can happen owing to the natural disaster, technical glitch/ hardware failure, power loss/interruption, accidental data deletion, cyberattack on cloud, etc. To mitigate data loss, to reestablish business-critical directories and to prevent costly service outages organizations are adopting DR tools/service.

One of the key governance issues is related to Data whether it is data ownership , data life cycle management secure disposal of data etc.

Cloud Security Solutions

There are an increasing number of cloud security solutions available from both cloud vendors and third parties. While cloud providers offer many clouds native security features and services, supplementary third-party solutions are essential to achieve enterprise-grade cloud workload protection from breaches, data leaks, and targeted attacks in the cloud environment. Only an integrated cloud-native/ third-party security stack provides the centralized visibility and policy-based granular control necessary to deliver the following industry best practices.

Cloud Security Posture Management

Lack of visibility may turn out to be the greatest vulnerability. In environments as complex and fluid as the typical enterprise cloud, there are hundreds of thousands of instances and accounts, and knowing what or who is running where and doing what is only possible through sophisticated automation. Without this support, vulnerabilities arising from misconfigurations can remain undetected for days, or weeks, or until there is a breach.

Cloud security posture management addresses these issues by continuously monitoring risk in the cloud through prevention, detection, response, and prediction of where risk may appear next.

Zero Trust for Cloud Security

The basic principle of zero trust in cloud security is not to automatically trust anyone or anything within or outside of the network—and verify (i.e., authorize, inspect and secure) everything. Zero trust, for example, promotes a least privilege governance strategy whereby users are only given access to the resources they need to perform their duties. Similarly, it calls upon developers to ensure that web-facing applications are properly secured. For example, if the developer has not blocked ports consistently or has not implemented permissions on an "as needed" basis, a hacker who takes over the application will have privileges to retrieve and modify data from the database.

Recommendations

Governing security affairs of your cloud environment is no longer a choice, and it requires a focused approach that is contextualized to cloud setup and is in accordance with the principles outlined in the framework being proposed by this POV. This section enumerates a few suggested pointers that could be construed as recommendations by enterprises that are looking to bolster their cloud security posture.

Leveraging Frameworks, Standards, Best Practices, and other References

Developing a contextualized and comprehensive cloud security governance framework should certainly be the first step in this endeavor. Standards and frameworks could play a vital role in guiding the organizations in planning and executing their governance & assurance journey. The POV has also tried to come up with a holistic approach towards governance of Security on the cloud.

Coming Up with Ownership and Accountability for Critical Cloud Assets and Services

Effective governance on cloud can be accomplished by working towards a shared responsibility matrix that clearly delineates the responsibilities of the organization and the CSP when it comes to implementing cloud security controls. The cloud, assets, services business objectives and processes and policies must be documented along with their operational relationships.

Use of Cloud Security & Governance Policies

Cloud services providers have developed security frameworks which establishes security and governance policies through cloud guardrails therefore ensures the efficacy and efficiency of cloud security controls are from day zero. These security and governance policies designs the boundaries of enterprises cloud security policies, processes, controls and compliance adherence.

Conducting a Comprehensive Evaluation and Assessment of the Cloud Threat & Risk Landscape

A thorough evaluation of the cloud threat landscape and associated risks for the organization should be undertaken with the object of having meaningful security governance and effective assurance. This assessment would pave the way for safeguarding the stakeholders involved from any potential exposure.

Governance of SLAs and Performance

Given the fact that SLAs play an exceedingly important role in overall cloud service delivery, they need to be carefully looked at and should find a place in the overall cloud security governance and assurance framework. It is imperative to establish a common understanding on the services to be provided and enforce guarantees around performance, transparency, conformance, and data protection.

Managing Change Management Processes on the Cloud

Leveraging proper tools for configuration and change management process on the cloud is an important element of the recommendations for better security governance. These tools help them capture information like cloud resources currently being used, what has changed, how the relationships between cloud resources have changed and so on.

Building a Robust Cloud Security Architecture

In accordance with its business needs, obligations and risks, an organization should embark on the task of building a robust cloud security architevcture which suitably incorporates the shared responsibility model along with the cloud security best practices and the technologies including but not limited to container security, infrastructure as a code, CI/CD tools and frameworks, CASB et. al.

Continuous Discovery of Assets and improvement of Asset Security Posture

For a dynamic environment such as cloud, inventory management is a dynamic discipline. Organizations must put in place provisions for continuous discovery of assets that will allow the governance team to keep up with the pace of change.

Regular Review of the Cloud Security Governance Strategy

While its essential to build a comprehensive strategy for governing the security affairs on the cloud, periodically reviewing the same would be critical from relevance standpoint. This will ensure effectiveness as the review would provide the scope for revisiting the threat landscape for cloud environment which would indeed be dynamic

Frequently Asked Questions

Q1: What are the key tenets of cloud governance enterprises should ensure to consider while creating the cloud security strategy?

Cloud infrastructure is very dynamic and agile because of the speed & nature of cloud assets provisioning and de provisioning & availability of huge number of services and lack of skilled administrators. Due to this very fluid nature of the cloud platform, it is essential to have real time visibility of cloud assets & any security mis configurations present. The cost effectiveness, cloud security policies or guardrails, access reviews and security baselining for every cloud environment (prod., non-prod, test etc.) are some of the other tenet's enterprise should look at. Regulatory, compliance & risk management are some of the regulatory compulsions enterprises will have to adhere while embarking on their cloud journey. Infosys cloud security posture and compliance management service offering ensures to provide effective cloud governances & compliance management services covering all facet of it.

Q2: What are different solutions and tooling required for enterprises to strengthen their cloud governance approach.

Most of the Cloud Services Providers (CSPs) have multiple built-in solutions which can ensure the basic hygiene for cloud governance. Setting up the cloud security policies & guardrails from day zero through azure, AWS and GCP service control policies are the foundational steps to secure and adhere to compliance requirements. In multi-cloud environments implementing Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), micro-segmentation, entitlement management, access reviews, and network rule analyzers are some of the advanced security controls which can provide effective cloud security governance.

Q3. Can we have comprehensive cloud strategy in the context of using single, multi or hybrid cloud?

Yes, comprehensive cloud strategy in multi/ hybrid cloud environment can help to mitigate larger risk. Standardized/uniform security across hybrid or multi cloud can ensure "single identity", extension of on-premises controls to the cloud & ensure single view security management, administration, and governance.

Q4. How to ensure security assurance and governance with dynamic nature cloud?

Automated cloud governance that includes API based integration with cloud platforms which provides visibility of security misconfigure, asset inventory, compliance score & auto remediation helps to keep pace with dynamic nature of cloud. Cloud Security Posture Management (CSPM) capabilities can be beneficial to ensure good cloud governance.

Q5. What can be the good strategy to implement security controls on the cloud?

Native security controls + 3rd Party next gen controls. Maximum use of native security controls which are tightly integrated with cloud infrastructure & has better understanding of cloud platforms. Complementing native and 3rd party controls ensures fool proof security on cloud.

Q6. In shared cloud security responsibility model, who is responsible for 'in cloud assurance and governance'?

Security and compliance in the cloud is a shared responsibility between the Cloud Service Providers (CSP) and their customers. Under the Shared Responsibility Model, the CSP is responsible for **"security of the cloud"** which includes the hardware, software,

networking, and facilities that run the cloud services. Organizations, on the other hand, are responsible for **"security in the cloud"** which includes how they configure and use the resources provided by the CSP.

Governance over configurations, vulnerability management, identities and access management and visibility across data/ application, cloud infrastructure and compliance remain key responsibility of customers.

Index

1. BFSI – Banking Financial Services and Insurance
2. IaaS – Infrastructure as a Service
3. PaaS – Platform as a Service
4. SaaS – Software as a Service
5. API – Application Programming Interface
6. GDPR- General Data Protection Regulation
7. PDPB- Personal Data Protection Bill
8. CCPA- California Consumer Privacy Act
9. CSP – Cloud Service Provider
10. MSSP – Managed Security Service Provider
11. SOC- Security Operation Centre
12. ISO – International Organization for Standardization

AUTHORS

Infosys

Vishal Salvi
CISO & Head of Cyber Security
Infosys Limited

Darshan Singh
Head of Cloud Security &
Emerging Technologies Security
Infosys Limited

Data Security Council of India

Vinayak Godse
Senior Vice President
DSCI

Aditya Bhatia
Senior Consultant
DSCI

Vivek Sarkale
Senior Consultant
DSCI

Infosys cobalt

Infosys Cyber Security practice has over 5,000 professionals serving 2000 global clients with end-to-end security services in consulting, transformation and managed services. We believe in assuring digital trust by driving a mindset towards "Secure by Design", building a resilient cybersecurity program to "Secure by Scale" and adopting newer technologies to "Secure the Future". We build robust and holistic cybersecurity programs by following our four-dimensional approach of Diagnose-Design-Deliver-Defend. This defines the Infosys Cyber Security philosophy - Digital–trust. Assured.

Infosys Cobalt is a set of services, solutions and platforms for enterprises to accelerate their cloud journey. It offers 35,000 cloud assets and over 300 industry cloud solution blueprints. Cobalt acts as a force multiplier for cloud-powered enterprise transformation. Infosys Cobalt helps businesses redesign the enterprise, from the core, and also build new cloud-first capabilities to create seamless experiences in public, private and hybrid cloud, across PaaS, SaaS, and IaaS landscapes. With Infosys Cobalt's community leverage, enterprises can rapidly launch solutions and create business models to meet changing market needs while complying with the most stringent global, regional and industry regulatory and security standards.

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURUTY COUNCIL OF INDIA

NASSCOM CAMPUS, 4 Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries contact

+91-120-4990253 | research@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect

data-security-council-of-india dscivideo