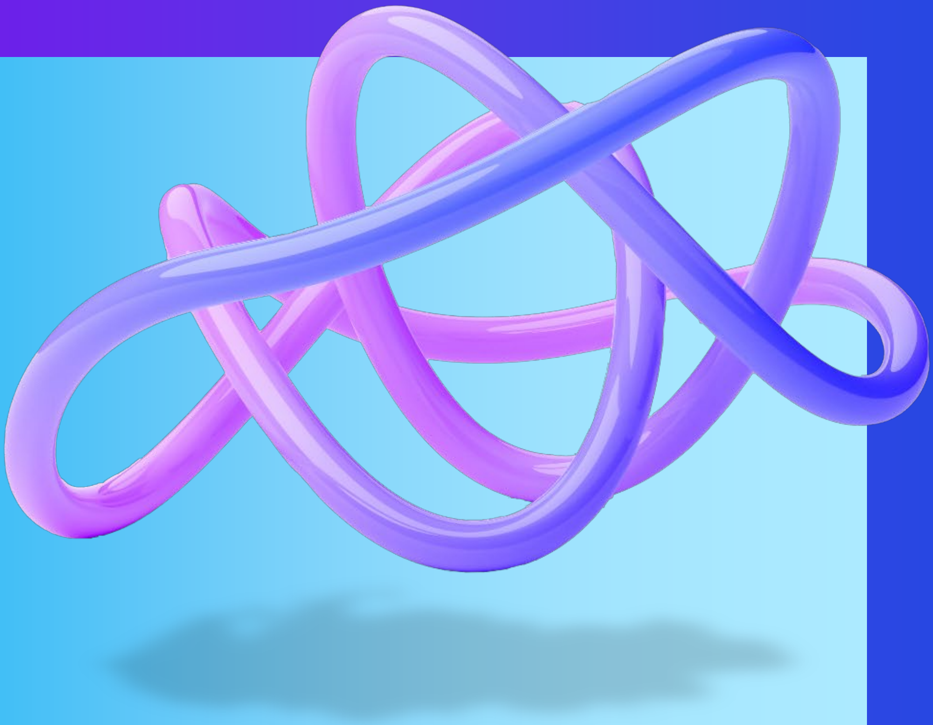


How to secure your data on Cloud

Establish the right blend of proactive and reactive security controls

While organizations continue to reap the benefits of cloud computing, they are also confronted with questions and multiple challenges associated with onboarding data to cloud and redesigning the existing cloud security controls to safeguard from ever-involving data breach and cyber incident patterns.

Today's cloud is much richer and more nuanced than it was at its inception, over ten years ago. Cloud consumers now have more native options, stronger security and privacy tools, and enhanced measures for detecting, responding to, and preventing security breaches. As the processes, regulations and knowledge surrounding the cloud continue to improve, these advances have increased customer confidence and eased the burden for IT functions.

Historically, Data Security has been one of the biggest obstacles to cloud adoption and still many clients hesitate in migrating their entire data landscape to cloud. Further with burgeoning data breach and cyber incidents, clients struggle to establish right-fit data controls across their multi/hybrid cloud environments. Hence, it's important to understand some of the common security concerns to separate them into assumptions vs realities and leverage appropriate cloud controls to ensure data security. In this context, what are the prevailing assumptions which impede data on cloud adoption and how to redesign/evolve existing security controls to enable enterprise data trust on cloud?

Prevailing Assumptions & their Realities

With the continual rapid adoption of cloud due to its obvious benefits, especially with the deliverance of artificial intelligence (AI) services on cloud, it becomes imperative to bring most of the data to cloud in order to yield maximum benefits.

For many enterprises the data migration is hindered due to the following prevailing assumptions / myths:

Assumption

Cloud security is far too difficult to maintain such as implementing 3:2:1 backup rule on multi/hybrid cloud scenarios, etc.

Reality

The same standardization applied to on premise security management can be applied to cloud security management.

Assumption

Cloud security costs more

Reality

Cloud with its automation offerings and feasible infosec integration options helps enterprises withhold 100:10:1 (engineers, ops, infosec resp.) workforce ratio. Thus, balancing people cost and optimizing employee productivity.

Assumption

Cloud is inherently insecure

Reality

A multi-tenant cloud would be more secure, because it makes it difficult to target a particular company or data set.

Assumption

There are more breaches in the cloud

Reality

When the correct security policies for preventing attacks and detecting them are implemented, attacks are no more threatening to the cloud than any other piece of infrastructure.

Assumption

Establishing the security controls is one-time initiative (static process)

Reality

With ever-involving threat patterns / data breach incidents and evolution of cloud security controls, establishing cloud security becomes a dynamic process. It demands iterative approach for improvising security controls and ensuring data sovereignty.

There is no shortcut for devising data security strategy and cutting corners will produce daunting results in the future. Hence, data security is something which needs to be built brick-by-brick and in a standardized manner. Though cloud offerings provide adequate security controls, but there are legitimate residual challenges for security on cloud:

Governance & Compliance

The enterprises require streamlined mechanisms to:

- Comply with government mandates / regulations and enforcement of organizations policies
- Manage data availability and BC/DR in cloud
- Storing the customer records in the required geography with adequate regulatory norms

Digital Identity

- Framing a flexible and centralized Identity and Access Management strategy
- Process to request, authorization, certification, and audit processes
- Extend SSO solution to Cloud Apps and review the security of implementation (APIs)

Data Privacy & Protection

Across multiple industries clients struggle to

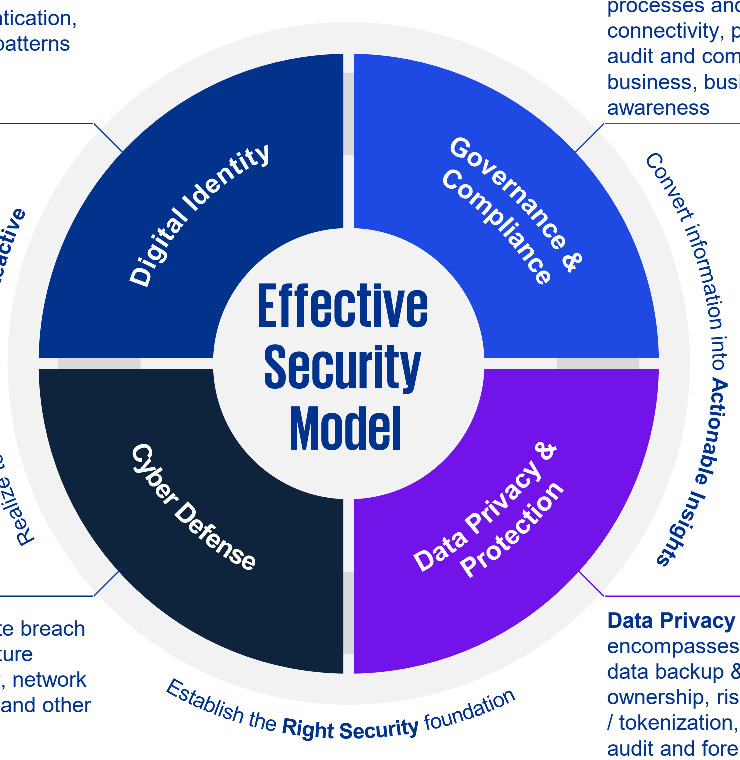
- Migrate sensitive data (personal, health, finance) into the cloud
- Establish adequate data privacy guardrails such as, sole tenancy & data purge mechanism
- Resolve security concerns for the communication channels between the cloud and existing infrastructure

Cyber Defense

- Ensure adequate & in-time knowledge about a security incident or a data breach
- Integration concerns with Cloud Provider security capabilities for monitoring and Incident Response
- Enablement know-how for Advanced Analytics, Advanced Vulnerability Management and Active Defense

The **Digital identity** depicts roles authorization levels and authentication, evaluation / monitoring usage patterns and education

Governance & Compliance Includes processes and policies (ownership, connectivity, privacy, audit / wipe), legal, audit and compliance, service level for business, business continuity, training & awareness


Effective Security Model
Digital Identity
Governance & Compliance
Cyber Defense
Data Privacy & Protection
Realize to be Proactive & Reactive
Convert information into Actionable Insights
Establish the Right Security foundation

Cyber Defense focuses on date breach protection with cloud infrastructure guardrails-security functionality, network configuration, cloud hardening and other operations

Data Privacy & Protection encompasses of data classification, data backup & retention, data ownership, risk assessments, encryption / tokenization, data loss prevention, audit and forensics

Enabling Enterprise Data Security on Cloud (KPMG's Proven Methodology)

Whether the enterprises are in initial stages of their data migration to cloud OR are already living on cloud, the KPMG Data Security on Cloud module furnishes an assessment approach for optimizing the cloud security controls by identifying key data profiles, classification criteria, associated risks along with technology (process and tool) evaluation and detailed architecture design- leading to holistic data security strategy and plan to establish enterprise data trust. The KPMG capability has vast experience in resolving the cloud security challenges for multiple large enterprises delivering tangible results.

Key Benefits

Data Discovery

Analyze the underlying data subject areas, systems of insight to determine current level of risks associated and redundancies within security. To understand the gaps and for analysis, leverage **KPMG's Cloud Data Security Controls Framework**.

Data Security

Characterization Determine the Data Security requirements – **Data classification, data store protection, data loss prevention, data compliance with infrastructure controls** and design technology guardrails for detailed security design and pilot implementation, with **KPMG's Cloud Data Security Cartridges**.

Strategy & Actionable Roadmap

Define enterprise strategy for data security rollout, implementation plan and feedback procedures for remediation.

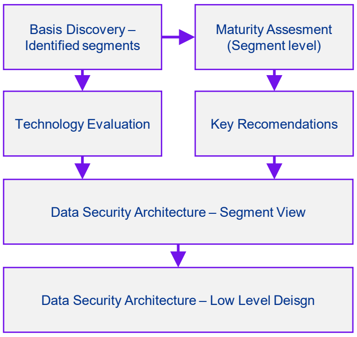
DOC Security Phases

	Data Discovery Workshop	Data Security Characterization	Data Security Strategy & Roadmap
Key Objectives	Analyze the underlying data subject areas, systems of insight to determine current level of risks associated and redundancies withing security	Determine the Data Security requirements – Data classification, data protection and data loss prevention and establish technology guardrails for detailed security design and pilot implementation	Define enterprise strategy for data security rollout, implementation plan and feedback procedures for remediation

Key Level Activities

- Identify critical business functions, critical applications and corresponding data repositories
- Define Business Roles
- Identify the data security subsegments
- Identify the data ownership design

Asses / Architect


Basis Discovery – Identified segments

Maturity Assesment (Segment level)

Technology Evaluation

Key Recomendations

Data Security Architecture – Segment View

Data Security Architecture – Low Level Deisgn

Roll-out & POC plan

- Build roll-out plant for enterprise data security as per data subject areas
- Build standard operating procedures
- Define mechanism for periodical data discovery
- Build change management plan and user awareness mechanism
- Determine remediation mechanism to handle data security exceptions

Organizations that are committed to digital transformation, will develop, and implement data security strategies that reduce risks and continue to do so in a sustained manner as security is an evolving landscape. Once these principles for data security have been established the rest of the transformation journey involves collaboration between business users, IT, technology, and the data community to be clear on the objectives for the data usage and how the tools will become embedded within day-to-day operations and decision making. This collaboration is essential to ensure successful adoption of new tools and ideas, but also essential to progress on your journey to become a data driven organization.

For more information on how KPMG can help you drive maximum value from your data security journey, please get in touch.

Contact our author(s) for assistance

Achinto Sengupta

Associate Director Cloud Advisory | Lead – Cloud Strategy

achintosengupta@kpmg.com

Achinto has 15+ years of professional experience in leading complex Cloud & IT Transformation programs. He has expertise in driving IT mandate around Cloud Transformation Strategy , Cloud Op Model, Enterprise Agility. He has worked across BFSI, Retail, Healthcare, Utilities, Travel and CMT industries helping organizations compete and win in ecosystem powered by emerging technologies & evolving culture globally.

Balvinder Singh Saluja

Senior Consultant | Enterprise Cloud & Data Security SME

balvindersaluja@kpmg.com

Balvinder is a Cloud Advisor within our Cloud practice with 5+ years of experience in Cloud Solutioning & Architecture. He has strong experience in Cloud Strategy, Data Modernization & IT Services Management. He has managed multi-geographic, multi-cultural teams and has a broad range of experience from concept to implementation. His recent focus has been in Consulting and CIO advisory services for Cloud Strategy & Data Transformation capability and acting as a strategic trusted advisor to several of our clients.

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

CREATE: CRT143124A