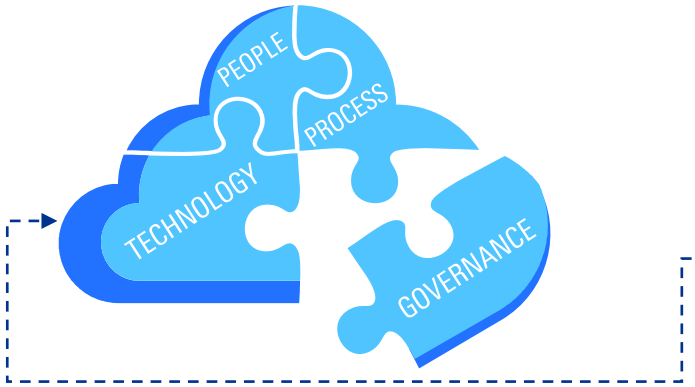
KPMG

Cloud Information Protection & Compliance

Securing Data Across Cloud Services & Integrations

Enterprises are increasing use of cloud applications and infrastructure to reduce costs, increase innovation, and drive efficiencies. At the same time, our clients want to know what data they have in the cloud, who is accessing it, and how to protect it. There are multiple stakeholders within organizations with interests in and responsibilities for securing data in the cloud:

- **Business analysts and system operators** want security of data in the cloud without having to think too much about it.
- **Developers/engineers** need easy-to-use security Application Programming Interfaces (APIs) to perform automated security functions within custom and homegrown applications that leverage both on premise and cloud services.
- **Security operations** require the ability to run one-time discovery and on-going monitoring of cloud services for access, configuration, and data-related events for detection and response.
- **Internal Audit/Risk** must demonstrate regulatory compliance and data protection in alignment with internal policy and external regulations such as SOX, HIPAA, ePHI, and other standards.
- **Legal** is responsible for discovering and placing legal holds on data across complex cloud environments and needs to ensure the organization is properly protecting critical information assets.



> "At the same time, our clients want to know what data they have in the cloud, who is accessing it, and how to protect it."

As stakeholders drive toward securing data across cloud environments, risk identification and mitigation have become paramount concerns. In order to leverage cloud-based services to support business needs, all parties must overcome the following key challenges:

- **Lack of visibility** of what sensitive data is being stored and processed within the cloud applications and knowledge of who has access to it.
- **Adequate detection and protection** of sensitive information, including controlling access and encryption.
- **Compliance** with security requirements mandated by the industry and internal information security policies, procedures and processes.
- **Inability to scale** legacy security tools to support cloud consumption.
- **Lack of standardized cloud policy and integration practices** where security is often bypassed or done in a silo, and configurations and polices are not commonly understood and applied.
- **Enabling effective security monitoring and response** when cloud service logs are not centralized, correlated or configured for alerting and response.

By adopting a strategy that focuses on a combination of people, process, technology and governance, organizations can address these challenges and achieve their cloud data protection goals and requirements.

Security analysts broadly define the category of security solutions that sit between cloud providers and consumers and interject enterprise security policies as Cloud Access Security Brokers (CASBs). CASBs are scalable and comprehensive security solutions that provide multiple types of security policy enforcement, including: data discovery, loss prevention and content classification, access governance, configuration security, encryption management, firewalls and user behavior analytics. Tactically, CASB solutions provide many valuable security services; however, designed and implemented strategically, these services can become part of an organization's common cloud security services layer that can serve the needs of the organization across all cloud environments and platforms. KPMG offers the following cloud data protection services and solutions:

— **Discovery Assessment:** Analyzing our client's current environment to determine their data risk exposure in their cloud environments and providing a practical strategy to address their data protection needs.

— **Use Case and Requirements Definition:** Identification of the client's key drivers and requirements for cloud application data protection, such as enterprise security policies, industry regulations and enterprise risk assessments.

— **Cloud Security Strategy and Architecture:** Defining a strategy for securing all of a client's cloud environments, including SaaS, PaaS and IaaS, in an effort to operationalize security to address risks and help clients identify the role of cloud data protection products and policies in the broader cloud security strategy and architecture.

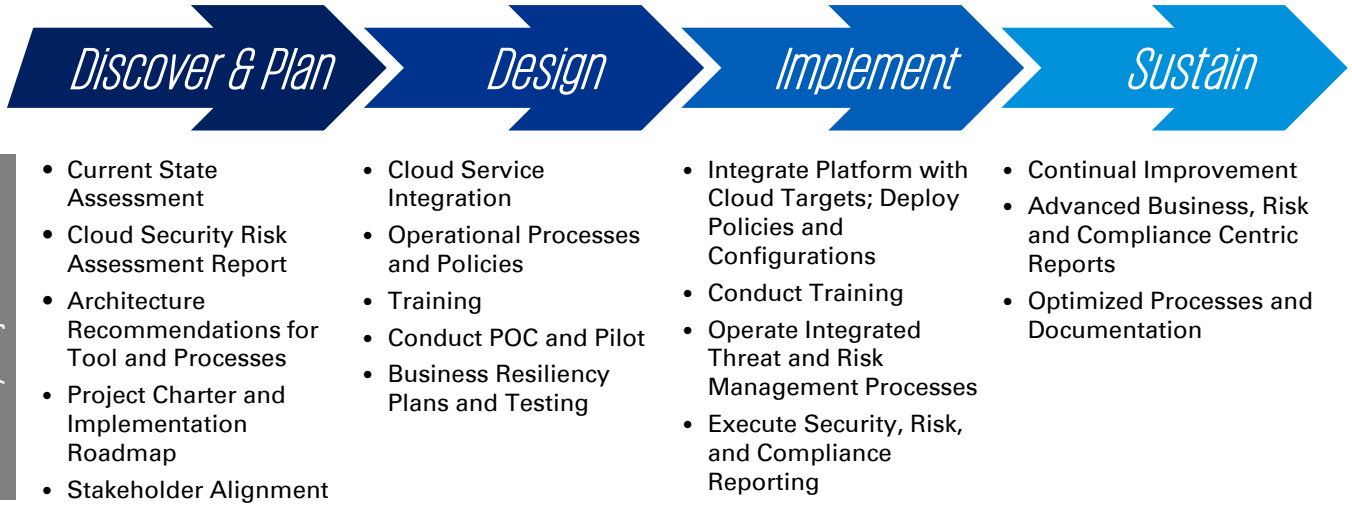
— **Product Selection Assistance:** Evaluating cloud data protection products that help clients achieve security and privacy goals such as continuous monitoring, data loss prevention, configuration security, encryption management, user behavior analytics and application firewalls.

— **Solution Design and Implementation Assistance:** Designing and implementing cloud solutions, including cloud data protection products and policies, that integrate with existing security processes and technologies and drive understanding and adoption.

The KPMG approach for Cloud Data Protection consists of the following four phases: Discovery & Plan, Design, Implement and Sustain. This approach is designed to help cloud service consumers define what cloud security components and services are required for their environment and implement a strategy for delivering those components. The diagram below provides a high-level overview of our four phase approach.

As part of the Discover & Plan phase, a current state assessment of key security risks, people, processes and technology is performed to help ~~our~~ clients define a risk-based approach and roadmap for achieving their security goals. After defining a clear roadmap, we work with clients during the Design Phase to develop a plan for integrating cloud services and defining operational processes, policies, training, business resiliency plans and testing processes for cloud products. We then help clients implement the roadmap and cloud service integration design plans and execute security, risk, and compliance reporting as part of the Implement Phase. Finally, in the Sustain Phase, we help ~~our~~ clients continually improve and strengthen the security processes and technology developed in prior phases.

By following this approach, the client can benefit from having operational security controls in cloud environments, which are integrated with other security operations, processes, teams and technologies.



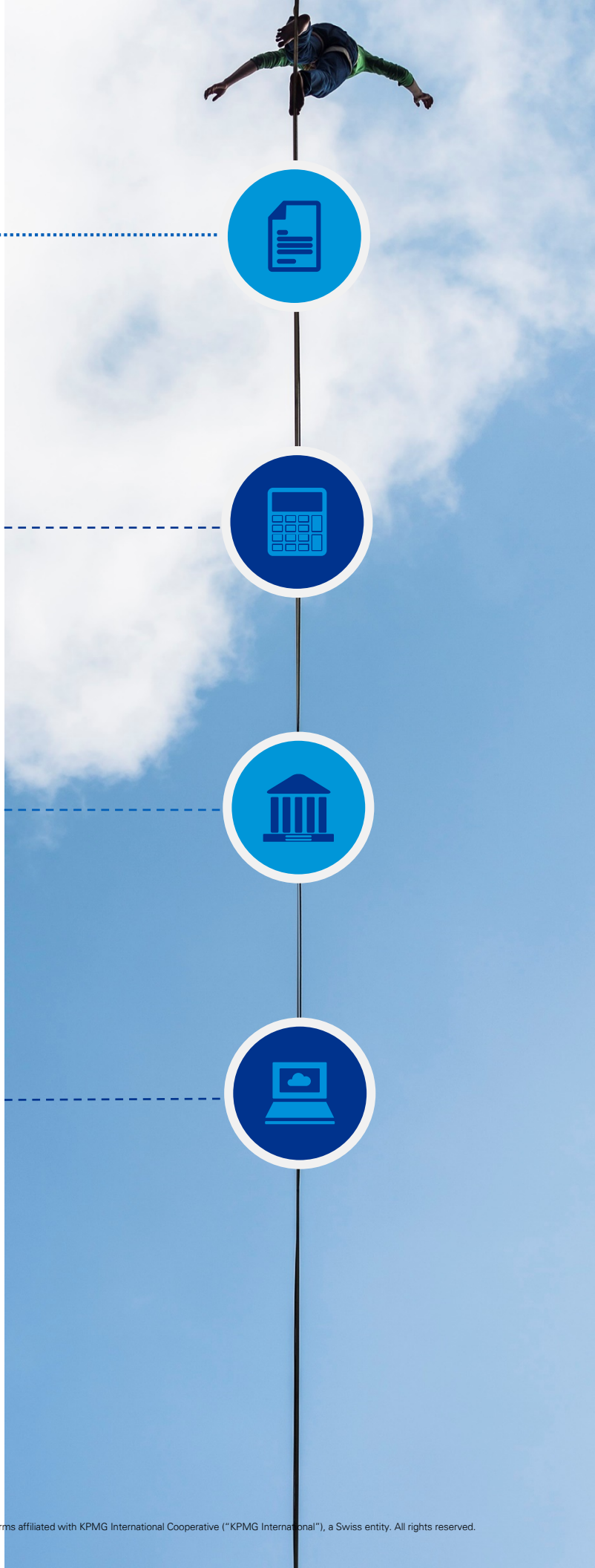
Of the wide array of organizations that can benefit from KPMG's services, the following illustrates a few example scenarios where KPMG can help enable businesses through the Cloud Data Protection service:

— **Sensitive Data Discovery and Protection:**
A pharmaceutical company wants to identify sensitive data related to intellectual property across multiple cloud-based applications and assess whether sufficient security controls at the application level have been implemented to protect this sensitive data. A CASB's data loss prevention and classification capabilities can be used to support the identification of sensitive data across multiple applications, and can provide security policies for access governance, logging and monitoring to support data protection.

— **Security Operations and Forensics:**
A financial services organization that utilizes homegrown cloud applications for financial analytics is concerned about the risk exposure of the data stored and processed by its cloud applications and the ability of its current security tools to identify unauthorized access to the data by users within its organization. As part of the Cloud Data Protection service, our team would assist the organization in defining an intelligent cloud incident and breach response strategy and identify cloud security solutions that can help support this strategy.

— **Regulatory Compliance:**
A health insurance company that leverages cloud applications for insurance claim processes is required to meet standards set forth by HIPAA and other industry regulations to protect the privacy of patients. As part of the Cloud Data Protection service, our team would assist the organization in defining its key drivers and requirements, defining a cloud security strategy and architecture, and integrating cloud security solutions that can help the organization comply with its regulatory requirements.

— **Monitoring Cloud Usage and Environments:**
A national retailer wishes to gather data to analyze the use of an organization-wide SaaS application. As part of the Cloud Data Protection service, our team can design and deploy a cloud security architecture that incorporates user behavior and analytics capabilities, providing the retail client with the capability to make data-driven decisions.



Contact Us

Hartaj Nijjar
Partner
Cyber Security Services
T: 416-228-7007
E: hnijjar@kpmg.ca

kpmg.com/socialmedia

kpmg.com/app