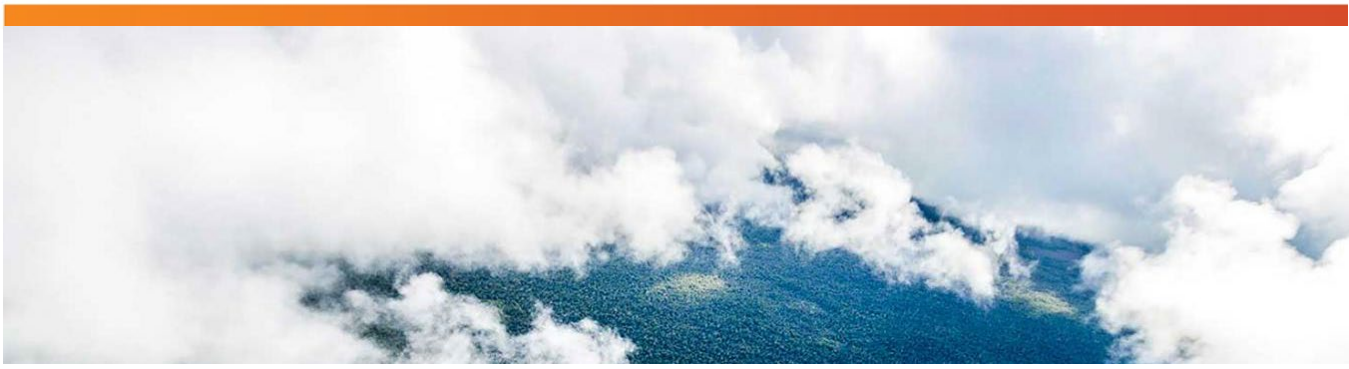
protiviti®
Global Business Consulting



Control the Cloud

Why it's Essential to Manage Security, Risk, and Compliance

Ensuring IT risks are managed, and compliance requirements are met has only intensified with the recent rapid growth in adoption of cloud services. Deployment of production workloads, migration of regulated systems and increasing storage of large volumes of data in the cloud has driven the need for security and controls to be deployed across customer cloud environments.

Within large enterprises, the need to manage security, risk and compliance is essential to maintain customer confidence, minimise system outages and comply with regulatory requirements.

Typical approaches to risk management that we have seen in the cloud have taken a bottom up approach. This is, they have relied on technical teams applying technical controls within the cloud environment, primarily focussing on security, with limited linkage to overarching enterprise risk appetite.

As enterprise cloud adoption continues to accelerate, assisted in part by COVID19, the need to ensure compliance whilst enabling use of innovative new services will be essential for organisations to take advantage of the inherent cloud benefits.

Common Challenges We See

Achieving a balance between security, compliance and service enablement is difficult and we see many common challenges within enterprises:

Shared Responsibility Model Requirements – A lack of understanding of the customer responsibilities for cloud services combined with limited understanding of the nuanced differences between cloud services.

Cloud Service Provider Control Mapping – Whilst most large CSPs provide extensive services to secure and control cloud environments, it is the customer's responsibility to ensure coverage and completeness for their cloud environment.

Cloud Skills Shortages, Training and Knowledge Transfer – New technologies require training and upskilling across the enterprise to truly enable successful adoption and understanding of key services and how they can be utilised to secure a cloud environment.

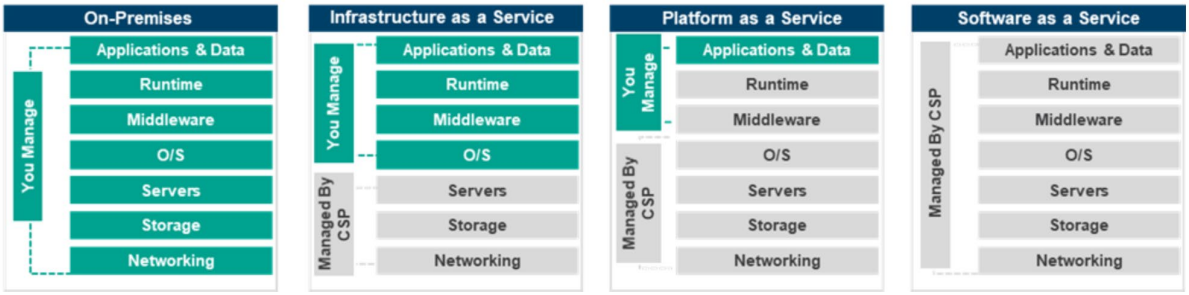
Linkage between Risk & Compliance, Security and Technical Teams – Risk and compliance teams require upskilling to adequately evaluate cloud environments for compliance, typically relying on external third-party support.

Disconnect Between Enterprise Risk Appetite and Technical Controls Implementation – A range of industry standards exist for controls to be deployed into cloud environments, alignment with specific overarching enterprise drivers and compliance requirements is typically not conducted.

Cloud Shared Responsibility Model

The Cloud Shared Responsibility Model outlines the delineation of responsibility for Cloud Services when operating and securing cloud environments.

Ensuring security and compliance 'in the cloud' is a customer's responsibility and needs to be approached in the same manner as existing IT risk management approaches, with cloud specific controls identified and applied.



Customers need to plan for how their existing IT control frameworks need to evolve to support both the shift in responsibility but also the type of controls that can be deployed in cloud environments.

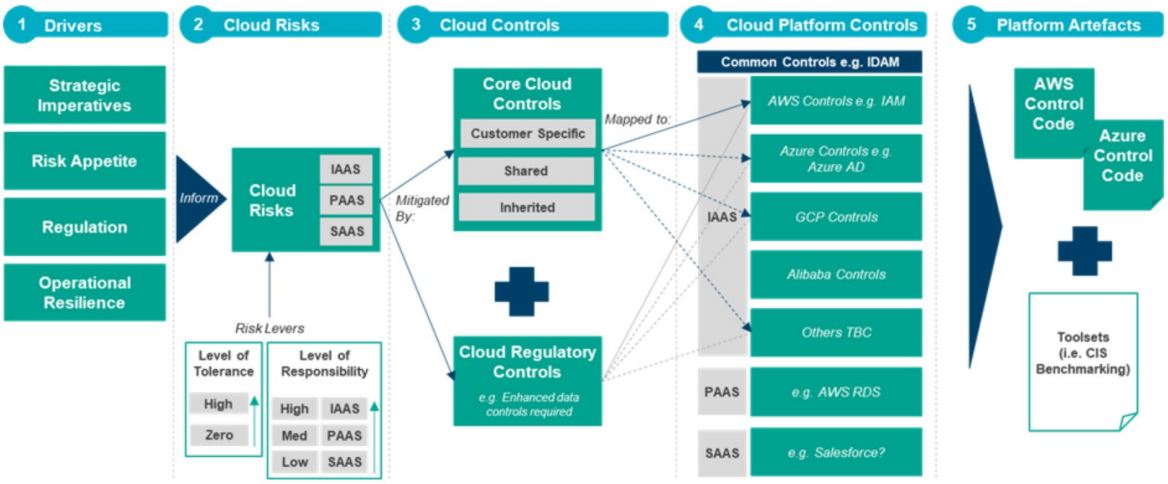
Enabling End-to-End Traceability

Putting in place a holistic Cloud Control Framework enables traceability from business risk drivers and tolerance levels through to technical control implementation within the cloud environment.

This facilitates:

- Streamlined reporting for risk management, compliance, and regulatory requirements.
- Comprehensive and transparent inputs for audits conducted across the cloud environment.
- Supporting to bring non-technical (Risk and Compliance, Audit) and technical teams (IT, Security etc.) together by providing a consistent reference model.

Our Cloud Control Framework has been developed through experience working with a range of global enterprises aiming to balance compliance with their desire to enable broad cloud adoption.



The Protiviti Cloud Control Framework consists of the following key components:

- **Drivers –** A range of typical drivers for cloud adoption but also the areas that would inform cloud risks, whether that be new regulatory drivers requiring implementation of new systems or updates to existing systems; desire to improve operational resilience through adoption of new services or other strategic imperatives important for an enterprise.

- **Cloud Risks –** The overall drivers and type of cloud services being adopted informs the respective cloud risks, with differences arising between the type of cloud platform adopted (Infrastructure-as-a-Service, Platform-as-a-Service or Software-as-a-Service). It should be noted that these risks can be managed using traditional risk levers such as an enterprise risk tolerance and through the Cloud Shared Responsibility Model. *The framework provides an extensive list of typical cloud risks that can be rapidly adapted for each respective enterprise.*

- **Cloud Controls –** Once the drivers and risks are clear for an enterprise adopting cloud then specific controls can be sought to mitigate risk based on the level of responsibility and tolerance levers appropriate for each enterprise. The two types of cloud controls are split between a typical base level and those that may be regulatory specific i.e. only required for regulated enterprises for example in the financial services industry. *The framework provides an exhaustive list of typical cloud controls (based on typical industry frameworks) that can be quickly used by enterprises to review against existing controls and augment where required.*

  It is important to note that there are a range of cloud controls that must be considered:

  1. Customer-specific Controls - those that must be implemented specifically within a customer's environment i.e. access, routing, security.

  2. Shared Controls – those that apply within a customer's environment but must also be cognisant of the underlying infrastructure layer i.e. patching of hosts versus patching of customer applications.

  3. Inherited – those that are adopted because of using a cloud service i.e. physical security controls to cloud facilities.

- **Cloud Platform Controls –** These are specific Cloud Service Provider (CSP) controls that can be deployed within each providers environment to ensure alignment against a customer's cloud control taxonomy. *The framework provides a mapping of cloud controls through to most of the large CSPs offerings to allow enterprises to quickly ensure coverage and alignment with the overarching risk and control position.*

- **Platform Artefacts –** These are artefacts pre-configured in platform agnostic code to allow enterprises to rapidly deploy CSP specific controls into customer managed environments, whilst maintaining lineage back to the overall risk profile.

The Protiviti Cloud Control Framework provides organisations with the following benefits:

- Linkage from enterprise drivers, such as risk appetite, regulation, strategic imperatives, etc., to typical cloud risks across a range of service types (IaaS, PaaS, and SaaS).
- Mapping of typical cloud risks to industry standard cloud controls for mitigation (including additional regulatory controls for highly regulated entities.) Providing linkage from the organisation's enterprise risk appetite through to controls used to mitigate risks.
- Tailored mapping of industry standard cloud controls to a range of platform agnostic controls, as well as cloud service provider-specific controls e.g., Identity and Access Management Service in AWS for identity management and to control system access.
- Rapid deployment of cloud service provider-specific controls through templated control artifacts to provide a quick way for organisations to deploy the controls that are required in their environment and also to adapt as regulatory or compliance requirements change over time.

To learn more about our Cloud Control Framework and Protiviti's cloud, cybersecurity and data privacy capabilities, contact us.

Contacts

David Kissane
Managing Director, Protiviti Australia
david.kissane@protiviti.com.au

Darryn Long
Director, Protiviti Australia
darryn.long@protiviti.com.au

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®