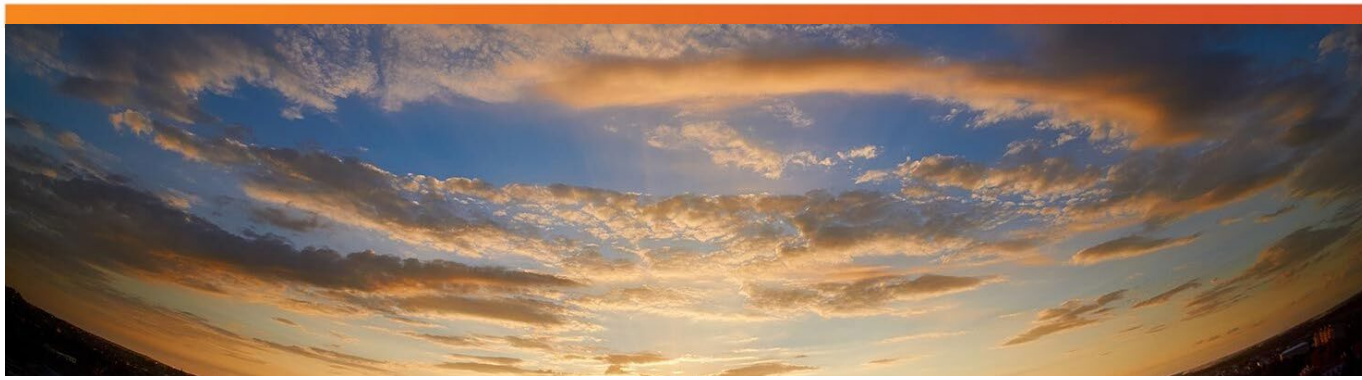
protiviti®
Global Business Consulting



Enable Transformation, Manage Risk with a Cloud Control Framework

Businesses are experiencing increased agility and reliability – and cost reductions – through cloud transformation but adopting cloud solutions can result in new risks. Sometimes, they impede enterprise vision and regulatory compliance. Applying an appropriate framework to help manage the risk of cloud adoption can mitigate or even eliminate these hazards. In an earlier blog, we introduced the cloud control framework concept. In this post, we'll use an example to illustrate how our cloud control framework provides the structure within which organisations can manage risk while giving proper consideration to business drivers and cloud technologies themselves.

Is your organisation leveraging cloud to reduce cost, enhance agility or improve system reliability? An effective cloud control framework integrates risk, compliance and security with technical implementation matters by considering enterprise drivers and compliance concerns in implementation planning and delineating customer and provider roles. Our framework bridges the gap between business risk expectations with the technology expertise that drive the business and seeks to improve through adoption of better cloud services. The framework provides flexibility to design cloud environments suited to each organisation's unique needs. The result? Rapid and effective deployment of cloud controls and services and new-found agility to respond to business imperatives, changing regulatory environments, and ever-accelerating technological opportunities.

Analyse drivers

Analysing drivers like strategic objectives, business risks, regulations and operational resilience factors at the outset ensures informed consideration of business strategy, cloud risks, compliance obligations — and ultimately, cloud control requirements — in subsequent steps.

The first step in our example considers enterprise-specific concerns. Each of the following drivers should be considered to result in a cloud solution uniquely suited to an organisation:

- Strategic objectives – What are your strategic objectives? What drivers underpin your strategic objectives? How does technology enable you to achieve these?
- Risk management – What are your business risks? What is your business risk appetite? How is technology enabling you?
- Regulatory environment – What are your regulatory and compliance requirements? What is the impact of non-compliance? How is technology enabling you in achieving compliance?
- Operational resilience – What are your operational resilience requirements? How are you achieving operational resilience? How are you leveraging technology to enable operational resilience?

Define the cloud risk environment

Sharing a single cloud risk approach across the enterprise is essential to align risk management and technology functions. Considering cloud risks starts with exploring organisational risk tolerance and assigning responsibility for risk management efforts. This step prompts stakeholders to identify, assess and prioritise the risks associated with identified drivers.

In our example, we focus on sensitive data loss, a risk clients often cite. Losing sensitive, protected or confidential data results in fines and reputational damage, among other penalties.

First, we consider sensitive data loss in conjunction with business drivers:

- Strategy: Are improving trust, customer confidence or reputation elements of enterprise objectives?

- Risk: Is sensitive data loss an identified business risk?
- Regulation: Are there regulatory requirements to protect sensitive data?
- Operational resilience: How will sensitive data be protected in a service disruption event?

Next, we consider:

- Risk tolerance: What is the business' tolerance for disruption (to its business operations, customers or trading partners, for example)?
- Responsibilities: How will responsibilities for cloud controls be divided between the business and its CSP? (Typically, the CSP is responsible for securing the host infrastructure while the client secures the workloads and data — such as data classification and access management controls.)

Examining risks guides subsequent definition of cloud controls to ensure alignment to objectives, confirms required control capabilities are available and validates the organisation's capability to implement the controls.

Identify and define cloud controls

Analysing business drivers and risk is foundational to designing fit-for-purpose cloud controls: mechanisms to secure and optimise customer cloud environments while providing the foundation for automation and better compliance. Controls mitigate risk, make operations resilient and enable regulatory compliance. They encompass:

- Customer-specific controls: implemented specifically within customer environments (like access, routing and security).
- Shared controls: reside in the customer's environment, but cognizant of underlying infrastructure (like patching hosts versus patching customer applications).
- Inherited controls: intrinsic to a cloud service (like cloud facilities' physical security controls).

Continuing our example, the risk of sensitive data loss can be mitigated through some of the following controls:

- Data classification: Classify data by value, sensitivity, and criticality.

- Data ownership and stewardship: Assign ownership and stewardship of personal and sensitive data.
- Data encryption: Protect data using cryptographic libraries certified to approved standards.
- User access provisioning: Authorise, document and communicate user access changes to data and assets.
- Segregation of privileged access roles: Ensure access to data, encryption and key management and logging capabilities are distinct and separated.

Map cloud controls to cloud services

Once cloud controls are designed and evaluated, they're mapped to the cloud services via which they'll be implemented. Mapping cloud controls to specific cloud services ensures alignment to enterprise risk and control positions and significantly improves awareness, reporting, protection and governance.

In our example, we'll use Amazon Web Services (AWS) as the cloud service provider (CSP) to show how cloud services can implement and automate a data classification control, focusing on the sub-control "discover and catalogue" in particular. In support of "discover and catalogue," AWS makes these services available:

- Amazon Macie uses machine learning to automate discovery, classification and labelling of data.
- AWS Glue discovers and catalogues data and metadata to assist with classification.
- Amazon Neptune analyses metadata to develop insights about relationships between datasets.

Implement and optimise cloud controls

Evaluating cloud services ensures the cloud control implementation is effective, scalable and aligned with drivers we established in our first step. Importantly, specific services and controls should be implemented within the context of a broader plan aligned to business drivers and risk and compliance requirements. Optimising these services with toolsets and benchmarking supports continual improvement.

One specific example of a cloud service we may implement is Amazon Macie, which we've already identified as a service to help discover, monitor and protect sensitive data in the future-state architecture. Amazon Macie uses machine learning and pattern matching to automate the discovery, classification and labelling of data. Now, we'll create and schedule AWS Macie jobs and analyse our results:

- Create jobs: we'll create sensitive data discovery jobs. These jobs may use predefined criteria to identify sensitive data. We'll also use Macie to create custom identifiers that detect sensitive data specific to this customer's business.
- Schedule jobs: we'll schedule the jobs to run periodically to ensure sensitive data is identified continually as the use of the system creates and modifies data.
- Analyse results: the Macie jobs will identify where sensitive data is stored and assess sensitivity on a severity scale. We'll analyse job results to determine whether security controls are appropriate relative to the sensitivity of the data.
- Integrate findings: our analysis of Macie results will help determine which additional cloud services could expand our holistic approach to data classification. Integration with the AWS Security Hub service, for instance, could enable incorporation of Macie's findings into a broader analysis of cloud security — to help us identify further measures to harden this cloud implementation.

Implement and optimise cloud controls

Organisations that want to implement new cloud platforms or improve existing implementations will benefit from a framework that considers strategic drivers and links them to cloud risks and subsequently to cloud services. This approach achieves broad, traceable consideration of business imperatives, risk management and regulatory compliance.

The ideal framework also offers mechanisms to enable continual analysis and optimisation of cloud control and services, while benchmarking and tools support continual improvement of the cloud control environment. Frameworks like the one described here bridge gaps between business and technology, while ensuring effective risk management, operational resilience and regulatory compliance.

By David Kissane and Samuel Hoare

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.

Get in touch with the authors

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

Samuel Hoare
Senior Consultant
Protiviti Australia
samuel.hoare@protiviti.com.au

protiviti®
Global Business Consulting