Cloud Control

Enabling Cloud Control Traceability

September 2021

INNOVATE. TRANSFORM. SUCCEED.

Adapt to the new business reality.

protiviti®

Face the Future with Confidence

INTRODUCTION – BACKGROUND AND CONTEXT

Rapid growth in the adoption of cloud services has failed to address overarching enterprise vision, risk management and evolving regulatory requirements.

Growth in adoption of cloud services

Cloud adoption is continuing to rapidly grow, due to benefits such as increased agility, reliability and reductions in cost. Each business's cloud journey is unique – migrating IT infrastructure to the cloud, designing serverless applications or increasing the consumption of cloud-based software and services.

However, the rapid adoption of cloud services does not come without cost. It often results in a disconnect between technology and risk functions and an inability to address overarching enterprise vision, effectively manage risk or meet evolving regulatory requirements.

Client challenges that are addressed through the adoption of our 'Cloud Control' framework include:

- **Linkage between risk & compliance, security and technical teams** – Risk and compliance teams traditionally require substantial upskilling to adequately evaluate existing cloud environment compliance requirements, often relying on external third-party support.
- **Disconnect between enterprise risk appetite, tolerance and technical controls implementation** – A range of complex industry standards exist for cloud control deployment, however alignment of specific enterprise drivers and compliance requirements are not typically conducted when deploying these controls.
- **Shared responsibility model requirements** – A lack of understanding of customer responsibilities relating to cloud services, combined with a limited understanding of nuanced differences between cloud services is a common challenge faced by our clients.
- **Cloud Service Provider (CSP) control mapping** – Whilst most large CSPs provide extensive services to secure and control cloud environments, customers are finding it difficult to ensure coverage and completeness across their cloud environment.
- **Cloud skills shortages, training and knowledge transfer** – New technologies require enterprise training and upskilling to truly enable successful adoption and understanding of key services, and how contemporary services can be utilised to secure an organisational cloud environment.
- **Complex, evolving and dynamic landscape** – In addition to the constantly evolving business landscape, organisations face uncertainty around alternate cloud deployment challenges, such as adoption of hybrid cloud deployments or overcoming scalability concerns.

CLOUD CONTROL FRAMEWORK – OVERVIEW

The purpose of the Cloud Control Framework is to enable traceability, design and deployment of cloud controls at pace to meet evolving enterprise risk, regulatory and strategic requirements.

Description

The Framework provides a holistic, structured way to identify and manage your cloud risks within the context of your business drivers and compliance obligations. It provides a mechanism for designing a fit-for-purpose cloud control environment, before architecting, implementing and optimising cloud services to embed and automate control activities.

Benefits provided

The 'Cloud Control' framework results in the rapid deployment of cloud controls and services, the automation of control activities and the agility to adapt to changing regulatory requirements over time. In addition, our framework provides value through each of the following:

Linkage of core enterprise **drivers** (risk appetite, regulation, strategy, etc.) to typical **cloud risks** across **different service types.**

Mapping of common **cloud risks** to **industry-standard controls** for mitigation (including regulated entities).

Tailored **mapping** of **industry standard** cloud control**s** to **platform agnostic controls**, as well as **CSP-specific** controls.

Heightened **connectivity** between enterprise **risk management**, **process** and **technology** business functions.

CLOUD CONTROL FRAMEWORK

Our Cloud Control Framework enables a consistent and repeatable process to achieve risk management and regulatory compliance.

1. Drivers

Key drivers underpin both adoption of cloud and the need for risk management.

- Strategy
- Risk
- Regulation
- Operational Resilience

2. Cloud Risks

Cloud risk management is scaled based on tolerance and ability to deploy effective controls.

Cloud Risks

- IAAS
- PAAS
- SAAS

Risk Levers

Level of Tolerance	Level of Responsibility	
High	High	IAAS
	Med	PAAS
Zero	Low	SAAS

3. Cloud Controls

Effective cloud controls enable mitigation of overriding risks and compliance with regulatory requirements.

Core Cloud Controls

- Customer Specific
- Shared
- Inherited

Cloud Regulatory Controls

e.g. Enhanced data controls required

4. Cloud Services

Mapping cloud controls to specific Cloud Services provides a roadmap for implementation.

Cloud Services	
IAAS	AWS Services e.g. IAM
	Azure Services e.g. Azure AD
	GCP Services
	Alibaba Services
	Oracle Services
PAAS	e.g. AWS RDS
SAAS	e.g. Salesforce

5. Implement & Optimise

The final step is to implement and optimise cloud controls and services within the context of a Well Architected Framework.

- Well Architected Framework
- Implementation
- Operational Management
- Benchmarking

protiviti®

CLOUD CONTROL FRAMEWORK – 1. DRIVERS

The first step of the Framework is to identify business drivers.

1. Drivers

- Strategy
- Risk
- Regulation
- Operational Resilience

Importance:

Analysing core business drivers is fundamental to understanding holistic and enterprise-specific considerations against operational cloud deployments and associated risks.

Description:

Business drivers are the key inputs and activities that drive cloud adoption and value delivery. Typical business drivers relevant to cloud adoption include:

- **Strategy** – Any major strategic objectives that will impact cloud adoption and control.
- **Risk** – The business risks that the organisation has identified.
- **Regulation** – Regulatory landscape and associated requirements the organisation must comply with.
- **Operational Resilience** – The ability of the organisation to provide business services in the face of adverse operational events.

Framework Integration:

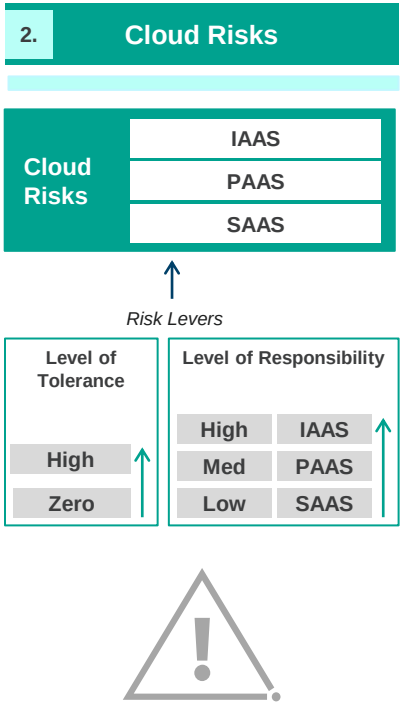
Analysis of business drivers will guide the consideration of relevant cloud risks, corporate legislative obligations and subsequent cloud control requirements.

Consequence of Failing to Address:

Failure to acknowledge and consider core business drivers will lead to a cloud environment configuration that is not fit for purpose, lacks appropriate risk management control, and is misaligned to overall enterprise objectives and vision.

CLOUD CONTROL FRAMEWORK – 2. CLOUD RISKS

The second step of the Framework is to define the organisation's cloud risk environment.



Importance:

Analysis of the cloud risk environment is critical to ensuring organisations identify, assess and prioritise risks associated to core objectives, whilst also relieving existing concerns of enterprise cloud initiatives. The subsequent adoption of a shared, enterprise cloud risk approach is essential for aligning risk management, process and technology functions.

Description:

Cloud risks are informed by business drivers. These are further informed by two risk levers:

- **Level of Tolerance –** The level of risk tolerance associated with specific business and cloud risks.
- **Level of Responsibility –** The degree of responsibility that the organisation has for controlling these risks in addition to the degree of responsibility of the CSP. The level of responsibility varies depending upon the deployed cloud model.

Framework Integration:

Cloud risks will guide the identification of fit-for-purpose cloud control requirements and subsequent implementation of these controls. In addition, this stage will ensure alignment to organisational objectives, confirm that scalable and effective cloud control capabilities exist (for selected deployment method) and validate enterprise capability to deploy effective controls in their cloud environment.

Consequence of Failing to Address:

Failure to adequately analyse the cloud risk environment will result in limited risk and technology function connectivity, creating higher ongoing costs, a more complex business ecosystem and an inability to effectively manage ongoing cloud risks.

CLOUD CONTROL FRAMEWORK – 3. CLOUD CONTROLS

The third step of the Framework is to identify and define required cloud controls.

3. Cloud Controls

Core Cloud Controls

- Customer Specific
- Shared
- Inherited

Cloud Regulatory Controls

e.g. Enhanced data controls required

Importance:

Designing a fit-for-purpose cloud control environment aligned to business drivers, compliance requirements and organisational risks is an integral step before operationalising and automating controls. Effective cloud control enables mitigation of overriding enterprise risks and compliance against regulatory requirements.

Description:

Cloud Controls are mechanisms to secure and optimise customer cloud environments, and are split between a typical base level, and those that are regulatory specific. Base level controls can be delineated between:

- **Customer-Specific Controls –** Those that must be implemented specifically within customer environments (e.g. access, routing and security).
- **Shared Controls –** Those that apply within customer's environment but must also be cognisant of underlying infrastructure (e.g. patching of hosts versus patching of customer applications).
- **Inherited Controls –** Those that are adopted as a result of utilising a cloud service (e.g. physical security controls of cloud facilities).

Framework Integration:

Design of cloud controls will flow into the Cloud Services stage, where controls can be implemented across cloud platforms.

Consequence of Failing to Address:

Failure to consider, implement and optimise cloud controls may lead to regulatory or industry compliance requirement breaches, increased security and privacy concerns, heightened vulnerability to attacks, and less overall control of enterprise cloud environments.

CLOUD CONTROL FRAMEWORK – 4. CLOUD SERVICES

The fourth step of the Framework is to map cloud controls to specific cloud services provided by the CSP.

4. Cloud Services

Cloud Services	
IAAS	AWS Services
	Azure Services
	GCP Services
	Alibaba Services
	Oracle Services
PAAS	e.g. AWS RDS
SAAS	e.g. Salesforce

Importance:

Once overarching Cloud Controls are designed and evaluated, these controls need to be aligned to the applicable CSP platforms and services to ensure they can be effectively implemented.

Description:

Each CSP has their own specific configurations and controls which can be implemented across their platforms. This requires a mapping of cloud controls to specific cloud services, allowing enterprises to ensure platform provider coverage and alignment with the overarching enterprise risk and control position.

Framework Integration:

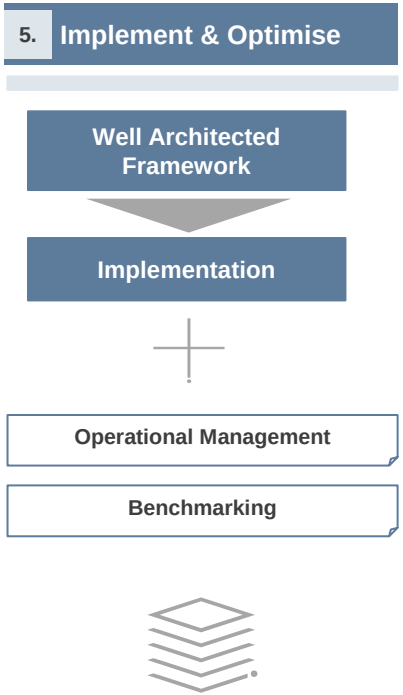
Once cloud controls have been mapped to cloud services, these services flow into the Implement & Optimise phase, where they are architected and subsequently implemented.

Consequence of Failing to Address:

Failure to consider and align required controls to cloud services will lead to a misconfiguration of unique cloud environments, misalignment of effective risk management and regulatory practices, and result in limited feasibility in implementing and automating control activities.

CLOUD CONTROL FRAMEWORK – 5. IMPLEMENT & OPTIMISE

The fifth step of the Framework is to ensure controls are successfully implemented within the context of a wholistic Well Architected Framework.



Importance:

The implementation of Cloud Services needs to be considered within a Well Architected Framework to ensure that control design is effective, scalable and aligns with best practice. The implementation of Cloud Services should be aligned with business drivers to ensure risk mitigation and cost optimisation. The Cloud Control Environment should be optimised by identifying and embedding toolsets and benchmarking to aid continual improvement.

Description:

1. **Well Architected Framework -** Design the Future State Architecture and Implementation Plan within the context of a Well Architected Framework to ensure that control design is effective, scalable and aligns with best practice.
2. **Implementation –** Implement cloud services in accordance with the Implementation Plan to operationalise and automate control activities.
3. **Operational Management –** Identify and configure relevant cloud toolsets to aid in the continual analysis and optimisation of the cloud control environment
4. **Benchmarking –** Identify relevant benchmarking and assessment tools and establish periodic reviews to ensure the continual improvement of the cloud control environment

Consequence of Failing to Address:

Failure to implement and optimise Cloud Controls will result in a continued disconnect between technology and risk functions and an inability to manage risks and compliance obligations.

Appendix

Cloud Control Framework in Practice

CLOUD CONTROL FRAMEWORK IN PRACTICE

This appendix provides an overview of the Cloud Control Framework in practice to illustrate how the framework can be implemented.

Purpose

The purpose of this appendix is to demonstrate how the Cloud Control Framework can be used in practice.

Contents

This is achieved by providing specific examples of each step of the framework and illustrating how drivers flow to cloud risks, through to controls, cloud services and the subsequent implementation and optimisation of cloud services.

This appendix uses the example risk of sensitive data loss to illustrate how risks can be informed by drivers, how required cloud controls and specific cloud services can be identified and how these services can be implemented to ensure the ongoing mitigation of identified risks.

1. Drivers

Outlines common questions to assist in the identification and analysis of business drivers.

2. Cloud Risks

Demonstrates how business drivers link to cloud risks through the specific example of the risk of sensitive data loss.

3. Cloud Controls

Maps the risk of sensitive data loss to an extract of mitigating cloud controls.

4. Cloud Services

Provides an example mapping of data classification controls to specific AWS cloud services.

5. Implement & Optimise

Provides an example of how one of the data classification services, AWS Macie, could be implemented in a customer environment.

CLOUD CONTROL FRAMEWORK IN PRACTICE – 1. BUSINESS DRIVERS

The first step of the Framework is to identify business drivers which will inform cloud risks, legislative obligations and cloud control requirements.

1. Drivers

- Strategy
- Risk
- Regulation
- Operational Resilience

In practice, it's valuable to ask some of the below questions to help determine our client's business drivers.

Strategy

- What are your strategic objectives?
- What drivers underpin your strategic objectives?
- How are you going to achieve your strategic objectives?
- How does technology enable you in achieving your strategic objectives?

Risk

- What are your business risks?
- What is your business risk appetite?
- How do you currently manage your risks?
- How is technology enabling you to manage your risks?

Regulation

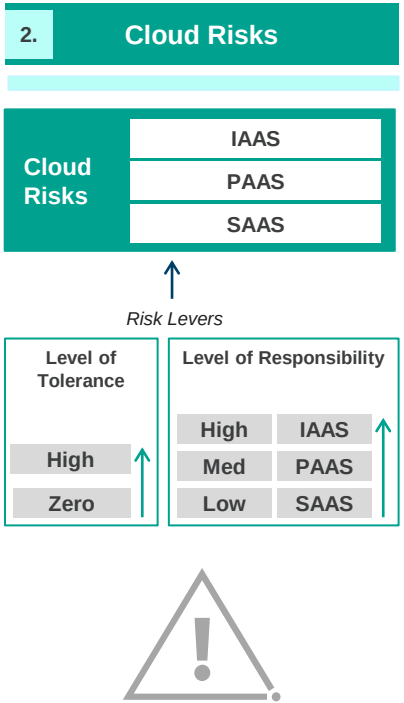
- What are your regulatory and compliance requirements?
- What is the impact of non-compliance with regulatory requirements?
- How are you currently ensuring compliance with regulatory requirements?
- How is technology enabling you to ensure compliance?

Operational Resilience

- What are your operational resilience requirements?
- Why do you need operational resilience?
- How are you achieving operational resilience?
- How are you leveraging technology to enable operational resilience?

CLOUD CONTROL FRAMEWORK IN PRACTICE – 2. CLOUD RISKS

After the analysis of Business Drivers, the Protiviti Cloud Risk Library is leveraged to create a custom-tailored cloud risk environment.



Example Risk – Sensitive Data Loss

A large number of our clients identify Sensitive Data Loss as one of their key risks. Specifically, that the breach of sensitive, protected or confidential customer data may erode customer confidence and result in significant legal costs, regulatory fines and a reduction in share value.

Business Drivers & Risks

This risk is informed by business drivers by asking the following questions:

- **Strategy –** Is improving trust, customer confidence or reputation an element of your strategic objectives?
- **Risk –** Have you already identified sensitive data loss as a business risk?
- **Regulation –** Do you have regulatory or compliance requirements related to the protection of sensitive data?
- **Operational Resilience –** Can you ensure the confidentiality, integrity and availability of sensitive data in the event of service disruption?

Risk Levers

- **Level of Tolerance**: Clients operating in a strict regulatory environment tend to have an extremely low level of tolerance for the loss of confidential customer data.
- **Level of Responsibility:** For clients hosting sensitive data on cloud managed infrastructure (IaaS), the below table shows the breakdown of customer and CSP responsibility for data management.

CSP Responsibility	Customer Responsibility
The CSP is responsible for physical and environmental controls – in this case, securing the infrastructure that customer data is hosted on.	The client is responsible for securing the workloads that run on the infrastructure and data hosted on these workloads, including: • Data encryption • Data classification • Access management

CLOUD CONTROL FRAMEWORK IN PRACTICE – 3. CLOUD CONTROLS

The client's risk environment is then mapped against Protiviti's Cloud Control Library to design a fit-for-purpose cloud control environment.

3. Cloud Controls

Core Cloud Controls

- Customer Specific
- Shared
- Inherited

Cloud Regulatory Controls

e.g. Enhanced data controls required

Example – Mitigating Controls for Sensitive Data Loss

To continue the previous example, below is an extract of controls mapped against the risk of Sensitive Data Loss.

Control Title	Control Description
Data Classification	Data and objects containing data shall be classified by the data owner based on value, sensitivity, and criticality to the organisation.
Data Ownership and Stewardship	All relevant personal and sensitive data shall be assigned ownership and stewardship of all relevant documented personal and sensitive data. Data ownership and stewardship should be reviewed at least annually.
Data Encryption	Data-at-rest and data-in-transit shall be protected using cryptographic libraries certified to approved standards.
User Access Provisioning	Define and implement user access provisioning processes to authorise, document and communicate access changes to data and assets.
Segregation of Privileged Access Roles	Define and implement procedures and technical measures for the segregation of privileged access roles to ensure that access to data, encryption and key management capabilities and logging capabilities are distinct and separated

CLOUD CONTROL FRAMEWORK IN PRACTICE – 4. CLOUD SERVICES

Required controls are then mapped to cloud services provided by the client's CSP.

4. Cloud Platform Controls

Common Controls e.g. IDAM	
IAAS	AWS Controls e.g. IAM
	Azure Controls e.g. Azure AD
	GCP Controls
	Alibaba Controls
	Oracle Controls
PAAS	e.g. AWS RDS
SAAS	e.g. Salesforce

Example – AWS Services to Enable Data Classification

In relation to Sensitive Data Loss, each of the required controls must be mapped to specific cloud services.

Effective identification and classification of data is one of the first steps in securing against the risk of sensitive data loss. The below table provides an extract of AWS services that can be used to implement and automate data classification.

Control Title	Sub-Control	AWS Service	Description
Data Classification	Discover & Catalogue	Amazon Macie	Leverage machine learning to automate the discovery, classification and labelling of data.
		AWS Glue	Discover and catalogue data and associated metadata to assist with data classification.
		Amazon Neptune	Develop insights into relationships between datasets, assisting with identifying and classifying sensitive data through metadata analysis.
	Catalogue	Tagging	Use resource tagging to classify the data stored within information assets and assist with implementing policies to protect sensitive and critical data.
	Protect	AWS Identity and Access Management (IAM)	Manage and control who has the ability to apply and edit classification of data.
	Log	AWS CloudTrail	Extensively log and track the creation, access, classification, modification and deletion of data.

CLOUD CONTROL FRAMEWORK IN PRACTICE – 5. IMPLEMENT AND OPTIMISE

Future State Architecture and an Implementation Plan are developed before implementing and optimising cloud services.

5. Implement & Optimise

- Well Architected Framework
- Implementation
- Operational Management
- Benchmarking

Well Architected Framework

The implementation of Cloud Services is considered within the context of a Well-Architected Framework by developing a Future State Architecture and Implementation Plan.

Control Implementation Example – Amazon Macie

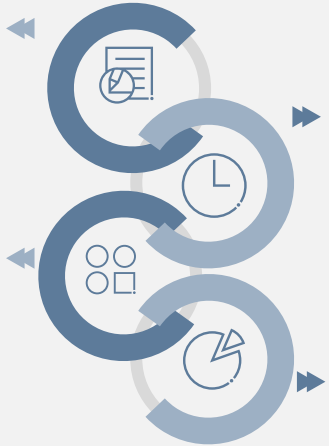
To continue the example risk of sensitive data loss and the associated requirement for data classification, below is an example of how the AWS Cloud Service, Amazon Macie, could be implemented. Amazon Macie uses machine learning and pattern matching to assist with the discovery, monitoring and subsequent protection of sensitive data within AWS.

1. Job Creation

The first step is to create sensitive data discovery jobs to analyse data in Amazon S3 buckets. These jobs can leverage off-the-shelf criteria to identify data such as PII, PHI and financial data. Additionally, its possible to create custom data identifiers to detect sensitive data specific to the context of your business.

3. Analysis

Data discovery jobs identify where sensitive data is stored and assess the sensitivity of this data on a severity scale. The results of these jobs can be analysed to assess security controls on S3 buckets relative to the sensitivity of data stored within.



2. Job Scheduling

Data discovery jobs should be scheduled to run at regular intervals, to ensure that sensitive data is continually identified as data is created and modified.

4. Integration

Findings from AWS Macie can be integrated with other services, such as Amazon Event Bridge or AWS Security Hub, to ensure a wholistic approach is taken to data classification and subsequent protection. For example, integration with AWS Security Hub allows you to incorporate the Amazon Macie findings into a broader analysis of your security posture and prioritise remediation activities accordingly.

Face the Future with Confidence

protiviti®