Please disable pop-up blocking software before viewing this webcast

# **Protecting Data in the Cloud:** The Latest Trend of Security & Privacy in the Cloud

**January 23rd, 2019**
**12:00pm CT**

# Speakers

**Derek Han**
Principal
Grant Thornton LLP

**Victor Chavalit**
Manager
Grant Thornton LLP

# Learning objectives

1. Describe the threat landscape of data in the cloud
2. Identify the latest trends for protecting data in the cloud
3. Demonstrate the key building blocks of a cloud data protection program
4. Define a roadmap to manage data risks in the cloud

Grant Thornton

# Agenda

1. Background
2. Building Blocks
3. Where to Start

Grant Thornton

# Background

Protecting Data in the Cloud

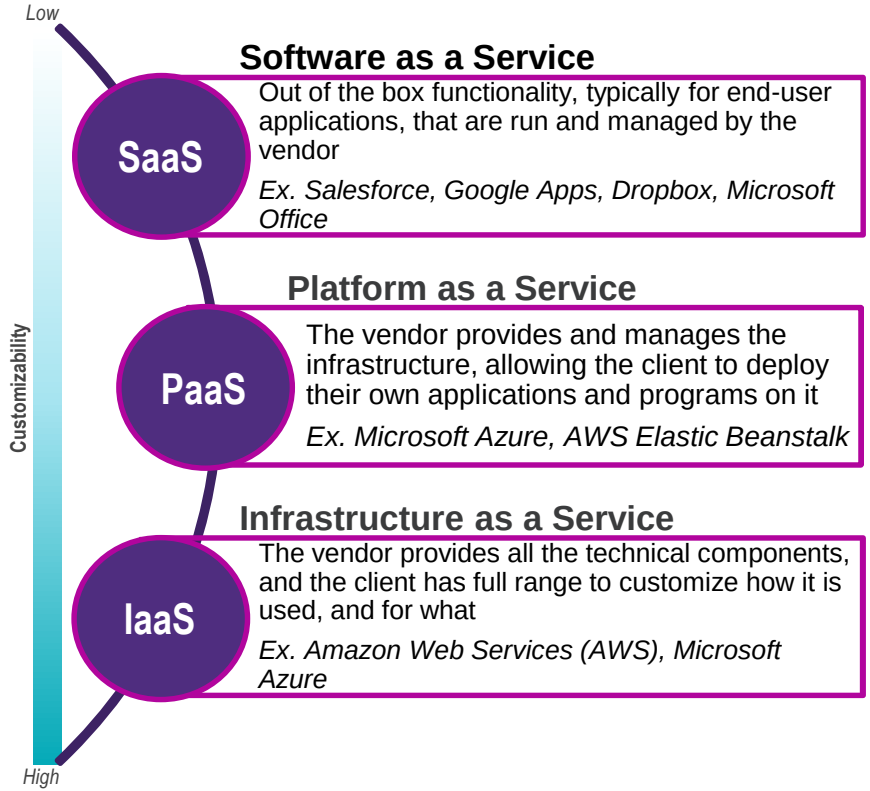
# Understanding data in the cloud

**77%** of organizations have at least one application, or a portion of their computing infrastructure, currently in the cloud. *- Source: Forbes, "State Of Enterprise Cloud Computing, 2018"*

Organizations are leveraging more SaaS applications and shifting IT infrastructure into the cloud.

Although cloud computing can help increase efficiency and reduce cost, organizations are faced with the challenge of properly securing and managing data that is transferred to and stored in the cloud.

Safeguards and controls to protect data in the cloud against threat actors and leakage is necessary to reduce risk to the organization and maintain compliance with applicable laws and regulations.




Grant Thornton

# Identifying the risks and threats

Threats to data security are present for every organization; however, cloud computing introduces new risks that must be considered. By migrating company data into the cloud, these threats can impact the data from numerous avenues – including the methods by which it was stored and uploaded.

**Reduced visibility and control –** By utilizing the cloud, companies lose control over what/where data is stored, and often have difficulty regaining that control. A company may not even be aware of what data employees are storing in the cloud. This opens them up to risk of confidential documents or sensitive data being accessed inappropriately.

**Targeted attacks/hacking –** A common, and often costly, issue with migration to the cloud is the increased likelihood of being the target for cyberattacks. While data is being migrated into the cloud, it is at its most vulnerable; and neither network nor cloud security can guarantee protection from data breaches during those operations. Even after the data migration, cloud storage will remain a target for cyberattacks.

**Multi-Tenancy –** If the cloud service provider fails to maintain separation between tenants, an attacker can gain access to an organization via a different, but linked tenant. An attacker is able to exploit vulnerabilities in the hypervisor, or subvert logical isolation controls - so multi-tenancy by default leads to an increased attack surface.

**Improper data migration –** Migrating data into the cloud is a complex task, and if not approached with a carefully curated plan can lead to disastrous repercussions. Commonly faced issues during cloud migration include server downtime / loss of data, cyberattacks, interoperability failure between systems, and internal strain with current business processes adapting to using the cloud.

# Why cloud Data Protection is crucial

"Through 2023, at least 99% of cloud security failures will be the *customer's fault*."

*- Gartner, "Magic Quadrant for Cloud Access Security Brokers"*

Cloud files can contain sensitive data such as PII, PHI, payment, and IP information

Sensitive data and files can be accidentally shared with unintended recipients through public links

**65%** of organizations use some form of infrastructure as a service

The average organization now uses **1,935** cloud apps, making cloud data protection essential

**21%** of cloud files contain sensitive data

**23%** increase of sharing sensitive data with a public link over the last 2 years

**2,200** average number of IaaS misconfiguration incidents per organization, per month

**17%** projected cloud growth in 2019

*- Source: McAfee, "Cloud Adoption & Risk Report 2019"*

## Prepare Your Organization

- ❑ What sensitive information do you store in the cloud?
- ❑ How are your end points secured?
- ❑ Who can access content in your cloud?
- ❑ What is your disaster recovery plan?
- ❑ How is your cloud data monitored?
- ❑ What safeguards are in place to protect your sensitive data in the cloud?
- ❑ Are you maintaining compliance with local laws and regulations?

Grant Thornton

# Data Protection: *One part of security*


While Data Protection is a critical area of focus for organizations, it is only one facet of the wider security landscape to consider in determining how to broadly protect your cloud environment. The fundamentals of standard data security should be applied when adopting new cloud platforms or migrating data / applications into the cloud.

It is important to recognize that organizations often cannot solely rely on the cloud service provider to protect its cloud environment, or the data stored within it. The responsibility still lies with the organization itself, which calls for the development of a comprehensive strategy that includes Data Protection as one of many components.

Grant Thornton

# What are the common challenges?

Through our experience performing privacy and data protection work with a variety of organizations across numerous industries, we have seen many challenges that can arise when attempting to implement data safeguards in the cloud environment.

## Adoption strategy

Lack of clear communication, training, and strategy for cloud adoption and data migration

## Regulatory obligations

Inadequate understanding of how the various regulations and mandates apply in the cloud environment, or how to ensure compliance within it

## Data insight

Limited institutional knowledge of sensitive data elements, and the flow of data in / out of the cloud

## Misconfigurations

Human error remains a leading cause for security vulnerability and the cloud is no exception

## Lack of expertise

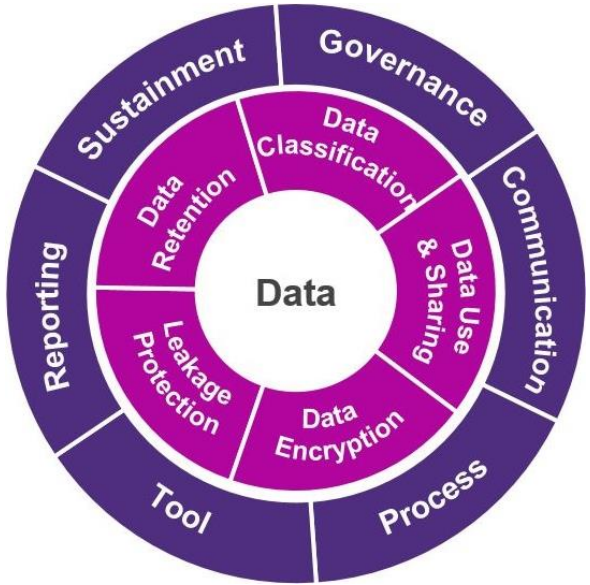
Deficit of cloud security talent coupled with poor understanding of the cloud infrastructure and architecture

# Data Protection framework

**Cloud Service Category**

- Infrastructure-as-a-Service
- Platform-as-a-Service
- Software-as-a-Service

**Data Protection Framework**

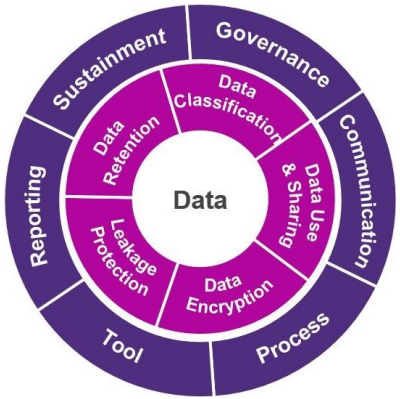



Data Protection technology and supporting processes should be implemented to support a data-centric approach, with consideration towards the type of cloud environment in place.

Implementation of a robust data protection framework focuses on maintaining continued protection as data traverses through its lifecycle – in the cloud and on-premise.

Grant Thornton

# Data Protection capabilities




## Data Classification

- Lays the foundation for how different data types should be handled
- Enhances visibility into where data resides in the cloud and on premise

## Data Encryption

- Allows data to be translated or encoded into a form that can only be accessed by authorized users
- Protects data in the event of theft, or accidental sharing

## Data Retention

- Dictates how long sensitive information should be stored within the organization and when to delete it
- Decreases the threat landscape by continuously removing data that is no longer needed

## Data Use & Sharing

- A policy or guideline dictating how data can be used and shared within and outside the organization
- Provides clear guidance to employees on acceptable use and handling of sensitive information

## Leakage Protection

- Enable organizations to detect and prevent sensitive information from being disclosed to unauthorized parties
- Assist in ensuring compliance with existing data use and sharing policies, to further reduce an organization's risk

Grant Thornton

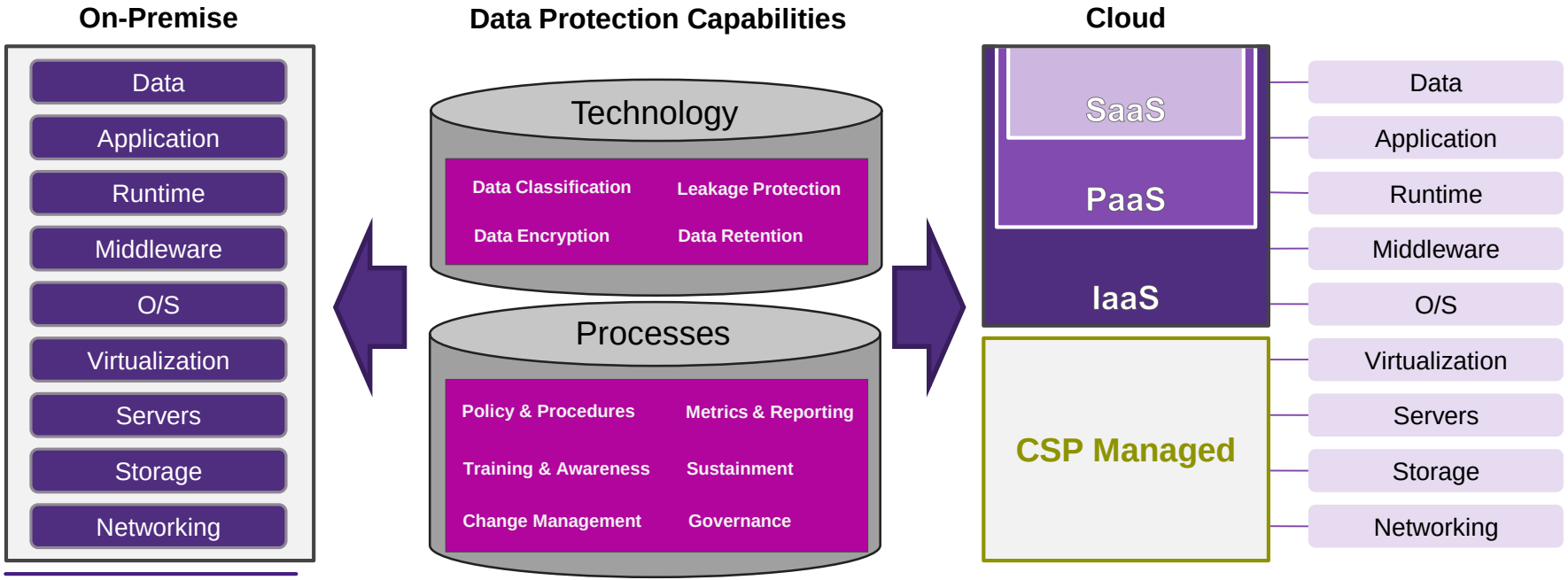
Grant Thornton

# Building Blocks

Protecting Data in the Cloud

# Align Enterprise Security Architecture

Establishing Data Protection in the cloud should align to the organization's existing Enterprise Security Architecture, and leverage existing Data Protection capabilities that are already in place.




Grant Thornton

# Cloud Data Protection technology

Organizations can often leverage existing on-premise Data Protection solutions to protect data in the cloud; however, many CSPs also provide native capabilities. Solutions such as Cloud Access Security Brokers (CASB) can also be used depending on the use cases.

| | |
|---|---|
| **Traditional on-premise solutions** | Data protection tools such as data classification, data-at-rest encryption, or Data Loss Prevention (DLP) that are implemented for on-premise applications and systems can be leveraged to support IaaS and PaaS cloud environments. This can facilitate central management between the on-premise and cloud environment.<br><br>***Examples include:*** *Titus, Bolden James (Classification) ; Safenet, Voltage, Vormetric (Encryption) ; Symantec, McAfee, Trustwave (DLP)* |
| **Native cloud capabilities** | Most cloud service providers offer native data protection capabilities, such as encryption at-rest, encryption in-transit, and access monitoring that organizations can configure/enable within their cloud environment. These native solutions may not have advanced functionality when compared to traditional on-premise capabilities, or those offered by specialized data protection vendors; however, they are guaranteed to be compatible with the environment.<br><br>***Examples include:*** *AWS, Microsoft Azure, Oracle, IBM* |
| **Cloud Access Security Brokers (CASB)** | A unique set of solutions that emerged to address the growing use of SaaS applications are CASBs. These solutions sit between the organization's environment, and the cloud to provide an array of security features such as: activity monitoring, access control, and encryption. Since the solution doesn't require backend integration, it is often considered for SaaS applications; although, it can be used to support IaaS and PaaS models as well.<br><br>***Examples include:*** *Forcepoint, Skyhigh, Cisco, Bitglass, Netskope* |

# More than just technology

Data Protection is not just a technology problem. To successfully implement these capabilities and tools, underlying processes need to be developed to support the execution and maintenance.

Train employees on new data use and handling guidelines and develop data protection awareness campaigns to promote safe activities in the cloud.

Establish management and operational groups that will make decisions and resolve risks and issues.

Develop key risk and performance indicators to measure effectiveness of people, process, and technology.


Develop/update policies, standards, and procedures to support new capabilities and requirements for protecting data in the cloud.

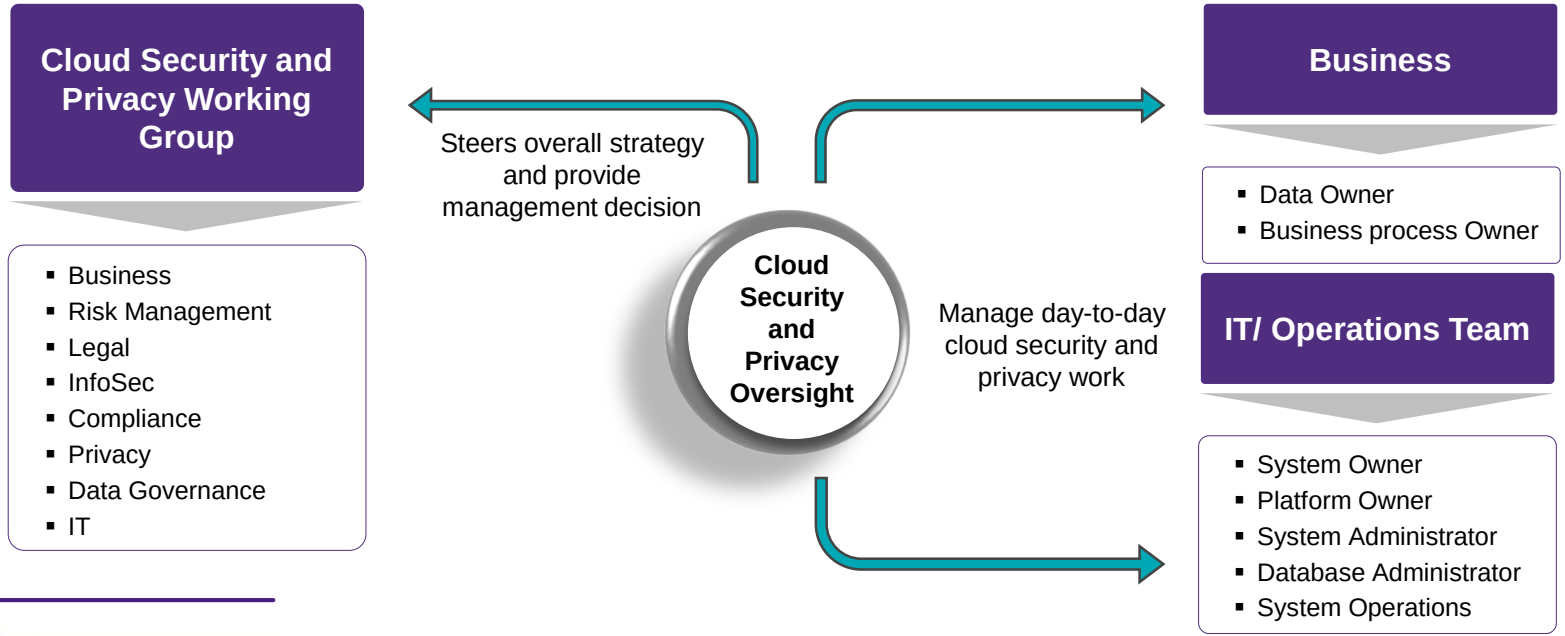
Communicate new processes and technology capabilities to the employees, and ensure there is seamless transition of people, processes, and technology.

Identify teams and develop processes to maintain ongoing operations of new technology capabilities.

Grant Thornton

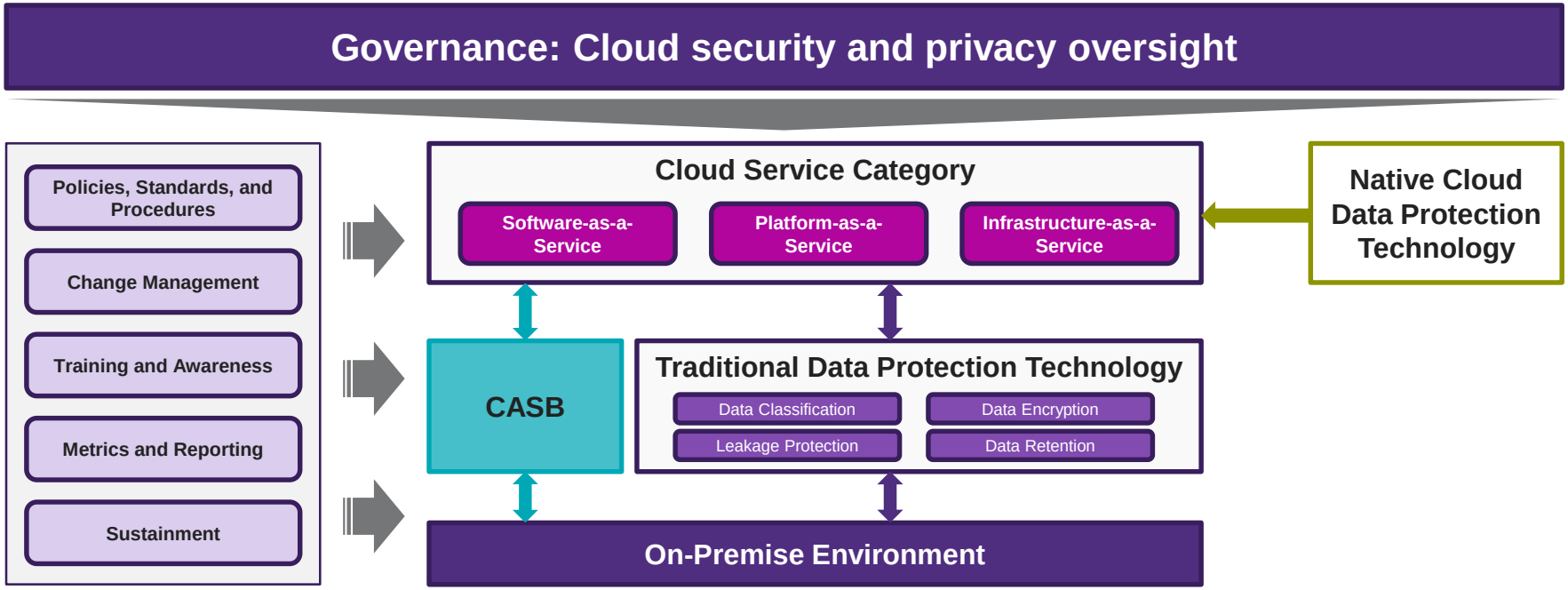
# Integrated oversight

Protection of data in the cloud should be part of a broader cloud security strategy with collaboration between all relevant stakeholder groups. Oversight shouldn't be done in a silo, and instead be an extended arm of traditional security, privacy, and data protection governance.



# How everything ties together

A successful initiative for Cloud Data Protection incorporates governance, process, and technology.



Grant Thornton

# Where to Start

Protecting Data in the Cloud

# Know your cloud environment

Before designing or implementing any capabilities, it is important for organizations to understand all the components that the data is interacting with. To do this, a proper discovery exercise should be performed.

### Types of applications and systems

Identify what applications, API connections, databases, backup and recovery servers, and other systems that are part of or connect to your cloud environment. It is also important to distinguish the different types of cloud services being used (e.g., different SaaS platforms).

### Data types and format

Inventory sensitive data categories and elements stored, or processed in your cloud environment and the format that it's stored in (e.g., relational databases, unstructured files).

### Existing security and data protection controls

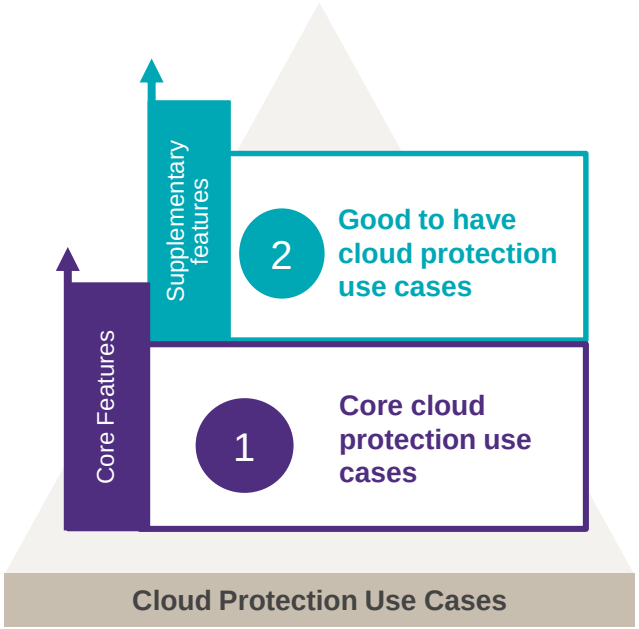
Many cloud service providers offer native security capabilities that organizations can enable in their environment. For remaining security needs, consider expanding existing on-premise solutions to support cloud environments before seeking new tools.

### User types and roles

Organizations often extend their active directory into the cloud environment to avoid any impact to users; however, it is still beneficial to identify the different user types and roles that will be accessing the cloud environment to allow for more granular or segregated control if necessary.

# Define the use cases

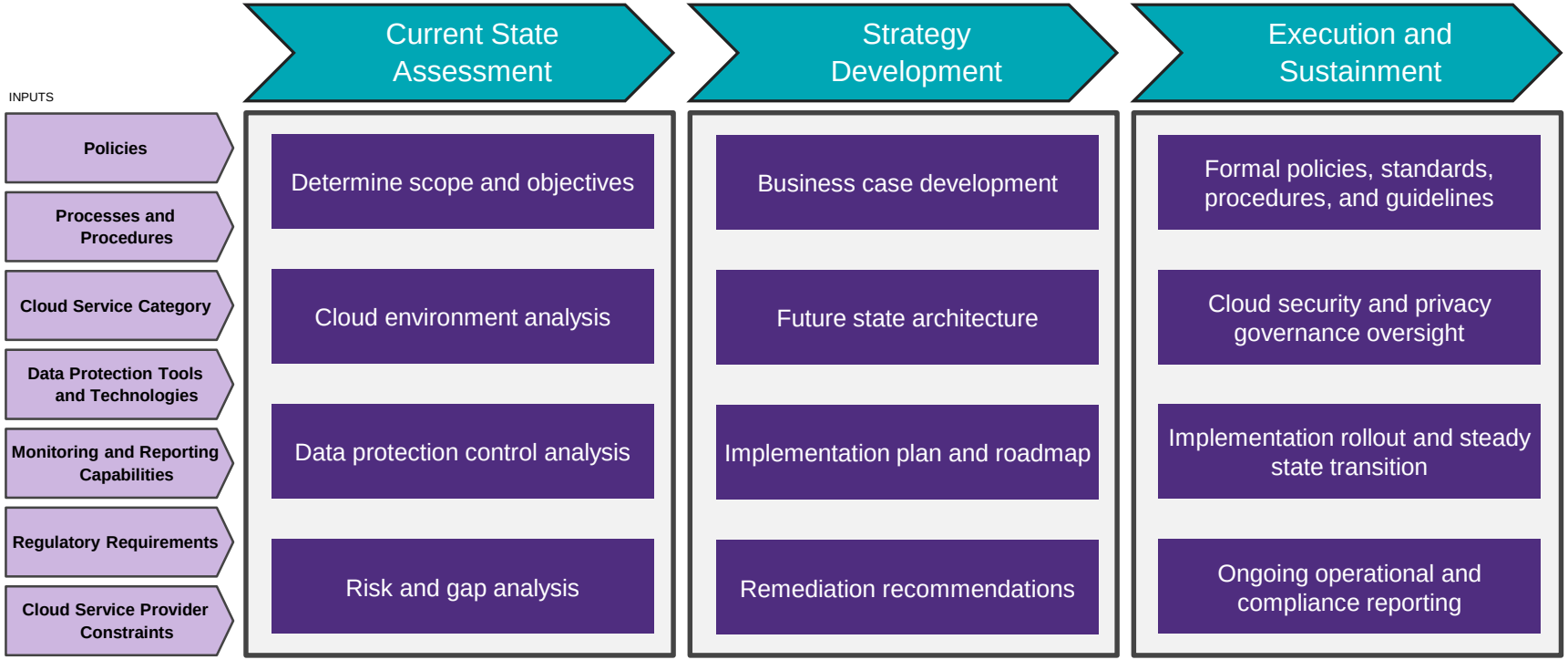
| | |
|---|---|
| Data discovery / classification | Ability to identify sensitive information that is being stored in the cloud |
| Data-at-rest protection | Ability to obfuscate sensitive data elements being stored in the cloud. |
| Activity monitoring | Ability to detect when a large volume of sensitive data is being accessed or downloaded. |
| Data destruction | Ability to remove data that is no longer needed from the cloud. |




| | |
|---|---|
| Compliance monitoring | Ability to review the degree of alignment of the cloud environment through assessments and audits |
| Process integration | Ability to integrate business rules, including enterprise hierarchy, change management, and other security domains. |
| Metrics and reporting | Ability to develop metrics based on key risk and performance indicators |
| Advanced automation | Ability to automate data protection capabilities based on pre-defined rulesets, data activity, and other input factors. |

Grant Thornton

# Develop an action plan



# Leading practices to reference

Leading practices and guidance from industry standards can be leveraged as baselines when building your cloud data protection capabilities. No standard is perfect; organizations need to tailor the content to align to their environment, operations, and culture.


Provides a cloud computing standards roadmap


Provides cloud-specific information security controls


Provides security techniques for the protection of personally identifiable information (PII) in public clouds


Provides guidelines for establishing effective cloud security and privacy governance

Grant Thornton

# Lessons learned from the field

1. **Define your requirements –** Implementing Data Protection controls in the cloud can be a daunting task given the various technology solutions available. Having clearly defined requirements can help scope the work needed and even assist with limiting the number of technology solutions you need to consider. This will also allow you to avoid any unnecessary complex implementation efforts.

2. **Implement process, not just technology –** Data Protection solutions are only as strong as the supporting people and processes. Developing strong policies, procedures, and training can be the difference between the solution gathering dust and a successful adoption.

3. **Bring-Your-Own-Key (BYOK) –** If you're leveraging native encryption solutions offered by the CSP, leverage third party solutions or hardware security modules to generate and store the encryption key. This ensures you have full control over your data and reduces the risk of data leakage through the CSP.

4. **Take ownership of protecting your data –** Many organizations assume that CSPs are completely secured and compliant with core regulations. Although that might be true for infrastructure level security and ongoing patching/maintenance, protection of data put in the cloud by organizations are their own responsibility; not the CSP's.

# Path to success

The most successful implementations are those where the business has embraced security and embed it into their strategic objectives and culture. The following aspects can help guide organizations toward the finish line:

## Integrated Approach

Cloud security is integrated into the enterprise architecture and considered as part of the organization's environment.

## Making it Real

Focus on practical solutions in the cloud rather than finding a perfect solution.

## Business Aligned

Business users are trained on company policies and safe practices for handling sensitive information in the cloud.

## Incremental Progress

Design milestones that can provide value to the organization vs pinning success at the very end.

Grant Thornton

# Any final questions?

# Speakers

**Derek Han**
Principal
Grant Thornton LLP

**Victor Chavalit**
Manager
Grant Thornton LLP

# Disclaimer

This Grant Thornton LLP presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered

For additional information on matters covered in this presentation, contact your Grant Thornton LLP adviser.

# Thank you for attending

## To retrieve your CPE certificate

- Respond to the online evaluation form. Please note, you may need to disable pop-up blocking software to complete this evaluation.
- Print your CPE certificate and retain for your records. Participants are responsible to maintain CPE completion records.
- Those receiving CPE will also receive the certificate at the email address used to register for the webcast.
- We are unable to grant CPE credit in cases where technical difficulties preclude eligibility. CPE program sponsorship guidelines prohibit us from issuing credit to those not verified by the technology to have satisfied the minimum requirements in monitoring response and viewing time.

If you experience any technical difficulties, please contact 877.398.9939 or email GTWebcast@centurylink.com

Grant Thornton

# Thank you for attending

www.grantthornton.com

twitter.com/GrantThorntonUS

linkd.in/GrantThorntonUS

Visit us online.
For questions regarding your CPE certificate, contact
CPEEvents@us.gt.com

Grant Thornton