Grant Thornton

Understanding strategies for effective data governance and data protection

June 16, 2025

Speaker

Vik Rai

Grant Thornton

Managing Director

Risk Advisory, Cybersecurity

Vikrant.Rai@us.gt.com

Grant Thornton

Learning Objectives

1. Define current trends in data security and the evolving threat landscape
2. Identify examples of organizations effectively implementing data governance strategies and highlight lessons learned
3. Recognize challenges such as compliance issues, misconfiguration risks, and lack of visibility into cloud data
4. Discuss how technologies impact existing data governance strategies and data protection controls
5. Discuss insights into how technical controls can be used to enhanced data governance and data protection
6. Identify strategies for organizations to continually improve their data governance and data protection controls by taking a data-first approach

Data security trends, opportunities, and challenges

When poll is active respond at **PollEv.com /gtiac713**

Send **gtiac713** and your message to **37607**

What are some of your biggest challenges with data?

Loading...

Nobody has responded yet.

Hang tight! Responses are coming in.

Leading trends suggest data can be an asset and a liability

Enhanced usage of data in analytics and data science programs (improve cost and efficiencies)

High quality data is powering AI solutions providing higher throughput with faster go-to-market solutions

Data boosting transformative trends using advanced analytics, predictive models

AI/ML, IOT, VR/AR, Quantum Computing, Low Code/No-code cloud services

Cloud related data breaches continue to be on the rise due to large volumes of data, limited data governance and data protection controls.

Apr 2025

Increased adoption of cloud and AI/ML services, rich and high-quality data will continue to be an on the rise as organizations continue to harvest data.

Data migration and optimized technology architecture

Fully optimized data structures improve data quality, speed and accuracy

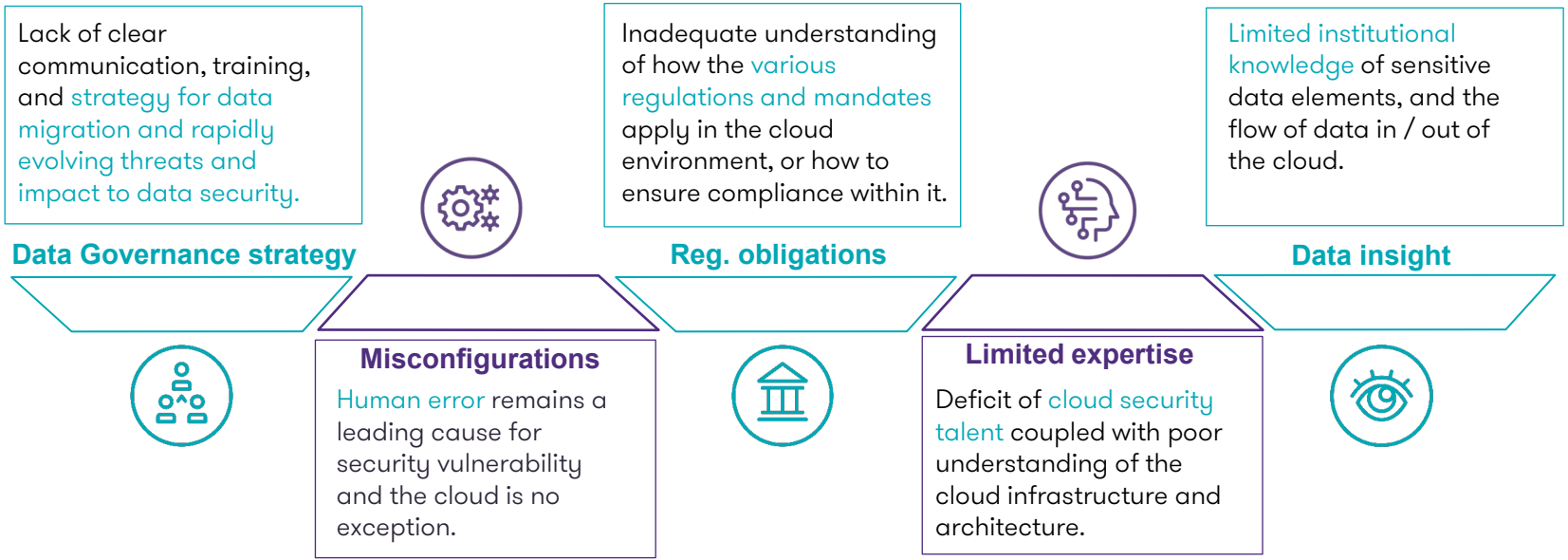
AI infrastructure and Machine Learning enables cost-effective services

Grant Thornton

Challenges with data

Recognizing challenges such as compliance issues, misconfiguration risks, and lack of visibility into data

We've seen common challenges in implementing data safeguards that transcend industry as well as organizational size.



Challenges with Data Governance & Data Protection

An effective data governance depends on a well-defined data governance model that supports a good data security posture. Technological advancement and rapidly changing service automation adds complexity and requires organizations to leverage the advanced technical methods to audit data governance and data protection controls (in the cloud and/or on-prem). Key challenges related to data governance and data security posture are discussed below:

Data Governance

Transparency & Ownership – There is often limited governance which is key to a successful data quality, data stewardship, data protection and compliance.

Data Management – Multiple environments and unmanaged data can spiral quickly out of control due to a distributed data models and how data interacts with other systems/technologies.

Data Protection Strategy and Lifecycle – Data protection strategy and lifecycle are critical for better data protection controls to prevent against malicious actors.

Data Security Posture Management

Limited visibility into data assets– Scalability in cloud environment can make it challenging for organizations to have visibility into data assets (e.g., shadow data stores, forgotten databases).

Inaccurate data flows leading to risk of regulatory non-compliance – Cloud hosted data assets are at a risk of increased exposure as more linked data is migrated to the cloud.

Limited adoption of data management technologies – Third-party DSPM tools can be expensive, difficult to deploy, learn, and manage.

Effective strategies to manage risks with data

How are organizations managing the risk of data

A holistic approach with data governance, data protection strategy

Gaining insight into data sets (structures/unstructured)

Define data classification & applying data protection controls

Reviewing data protection control effectiveness through technical testing

Typical risks associated with data

- Multiple cloud vendors/providers
- Unaccounted data stores
- Structures / Unstructured data sets
- Limited visibility into protected vs., unprotected data stores
- Data tables / columns may store sensitive information
- Limited insight on data flows
- Limited visibility into risk scores with data sets
- Limited visibility into data inventory, and access permissions remain unchecked (internal/external users)
- Limited visibility into compliance posture

How are organizations protecting data in a hybrid/Cloud environment?

It is important to take a 360-degree view of the data environment. This includes evaluating key components including:

- Data Governance – This includes taking a closer look with evaluating your Data Program Governance including program definition, review of data stewardship and data protection responsibilities.
- **Data Security Posture Management (DSPM)** – A data first approach should be adopted to review data assets (structured and un-structured) using cloud scanning platforms to identify where sensitive data may be stored and any potential risks associated with security misconfigurations and excess access.

Leverage industry leading technology platforms to help identify data sets in the cloud, review insecure configurations, access, application vulnerabilities and take a data centric approach to review technical controls to provide deep technical insights that helps evaluate the true effectiveness of data protection controls.

Data protection strategy and lifecycle management

Data strategies should promote a sustainable and repeatable process to protect data.

Data Governance

Designate “Data Champions” in the business that can be a liaison for promoting safe data handling practices

Data Classification

Implement classification or tagging rules based on business context

Data Retention

Establish a repeatable process to dispose data based on rationalized data retention rules

Data Protection

Use leakage protection, encryption, monitoring, and training to protect data

Deliver communication and awareness training to ensure that employees are kept up-to-date on the new policies, procedures, and technical controls on acceptable data handling practices.

Grant Thornton

Join by Web **PollEv.com/gtiac713** Join by Text Send **gtiac713** to **37607**

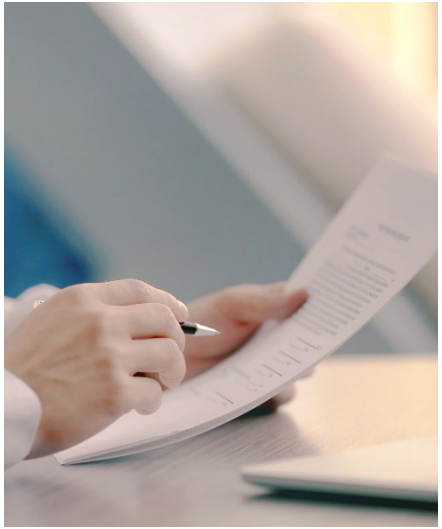
Do you have good visibility into your organization's data protection controls (e.g., inventory, classification, data flow, etc.)?

0%	0%	0%	0%

Data Governance – critical for data protection

Data governance is the authority and control over data assets by managing the quality, consistency, usability, security, and availability of your organization's data.

Why is this a hot topic?



Market	Business
Expectations	• Compliance and risk management – Lack of principles and standards, problems enforcing privacy, security, compliance • Lack of confidence relating to data integrity – multiple versions of the truth
Technology	• Awareness of availability and location of data is limited • Multiple and inconsistent data definitions
Costs	• No clear understanding of data flows between core systems and data repositories • Duplication of data collection / integration processes • Inability to meet 'urgent' internal and external demand for accurate segmental information in a timely manner
ESG	• Multiple stand-alone systems and sources of data – fragmented ownership and control

DAMA-DMBOK2 data management framework

Grant Thornton

Data classification benefits and challenges

Sensitivity Classification

Benefits:

- Automation / technology can enhance classification efforts
- Aligns to most traditional data classification policies and leverages common classification tags (e.g., public, internal, confidential, highly-sensitive)
- Focuses on distinguishing sensitivity of data

Challenges:

- Challenging for users to distinguish in multi-tier classifications (e.g., confidential vs restricted)
- Challenging to leverage additional data protection controls without classification

Business Categorization

Benefits:

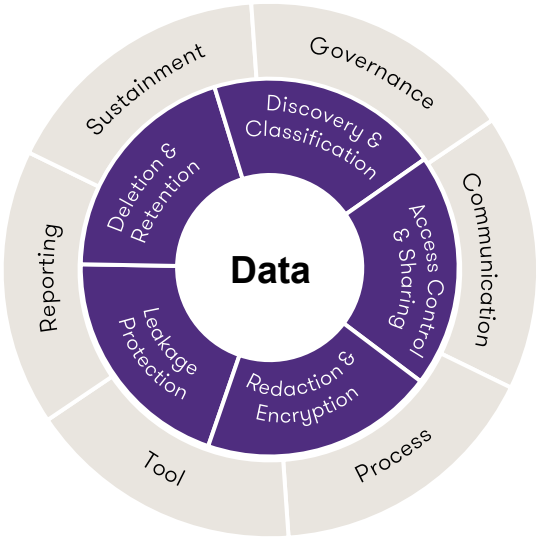
- Categorization tags are based on commonly used terms in the organization
- Easier to setup rulesets for triggering other data protection controls (e.g., DLP, encryption)
- Additional benefit of identifying where different types of information is located in the organization

Challenges:

- Does not provide sensitivity level
- May require a larger number of tags to cover the whole business

Data protection framework

To consistently establish controls for protecting data, both structured and unstructured, a data protection framework is used to evaluate the existing data protection environment. This framework addresses the data governance program structure and capabilities as well as specific data protection controls.



Controls	Definitions
Discovery & Classification	Information is discovered and classified in terms of its business value and nature of the information, legal and regulatory requirements, and criticality to company.
Access Control & Sharing	Data use, access and handling policies and guidance are established and implemented to control the data use, access, and sharing within company and with external parties.
Redaction & Encryption	Data redaction and encryption solutions are in place and enforced to protect sensitive information during data at rest and data in motion per company's data classification policy.
Leakage Protection	Using Data Leakage Protection (DLP) technology and rulesets to detect and prevent sensitive information from being disclosed to unauthorized parties.
Deletion & Retention	Retain and purge data based on company's data retention schedule to address regulatory mandate, internal policy, and reduce storage cost.

Grant Thornton

Key assessment elements

Data protection is an enterprise responsibility. Some key elements that should be assessed are:

Train employees on data protection responsibilities including awareness campaigns to data protection throughout the organization.

Data protection holistic program including defined roles and responsibilities across the enterprise – its not just an IT effort.

Key risk and performance indicators to measure effectiveness data protection processes and controls.

Policies, procedures, and controls to support proper data protection including compliance with data protection regulations.

Change management process and technology capabilities to properly secure data throughout the data management lifecycle.

Processes to maintain ongoing operations including introduction of new technology capabilities.

Data protection and privacy regulations should be evaluated and mapped to the data protection scope such as FFIEC, GLBA, and NYDFS.

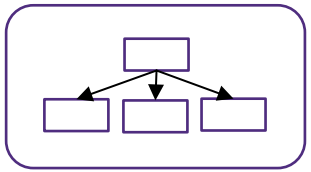
How to address data protection challenges in a cloud environment and generation of synthetic data

Grant Thornton

Types of data structures and data attributes

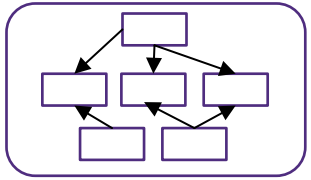
To understand the risks, you need to understand your data including how it is collected, processed and stored. Examples of data structures including how it interacts over distributed network is shown below.

Hierarchical

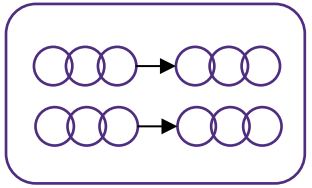


Array

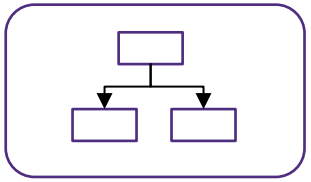
Networked



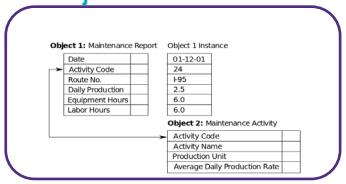
Linked List



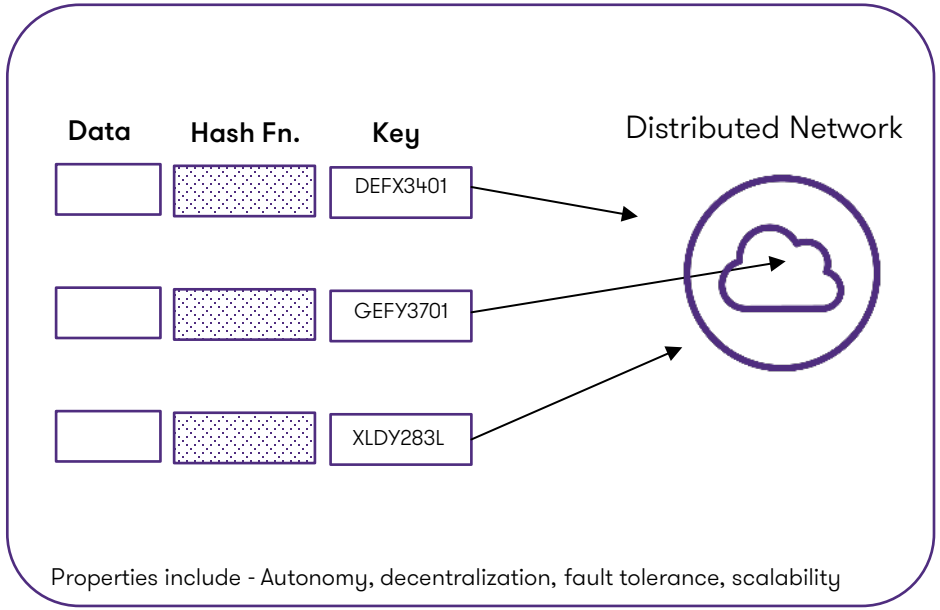
Tree



Object Oriented DB



Distributed Hash Table



Data structures and data attributes

Data category

Categorization of data that are representative of inherent business processes

Data Subject

Such as, employee, vendors, customers, affiliates or combination of users

Data structure type

Such as, relational, non-relational data structures, data lakes, data clusters, cubes etc.

Data ageing

Earliest date of a record stored in a system (including production, non-production, and offline backups)

Data lineage

Referential integrity across data that is shared between systems

Nature/ type of purge

Such as, master record deletion, disparate metadata deletion, manual vs. automated purge

How and where to start

It is important that organizations understand their critical assets and data prior to implementing any data protection solutions or controls. This helps maximize the value obtained from the investment and minimize risk within the organization.

Not dependent; can run in parallel

Confirm in-scope data types that draw the greatest concern with respect to data protection from the business and regulatory perspective. Once completed, identify the critical processes, systems, and vendors.

Define a classification scheme that aligns with the organization's values and determine the best methodology for applying classification to the inventoried data.

Provide the business with a solution to apply data classification.

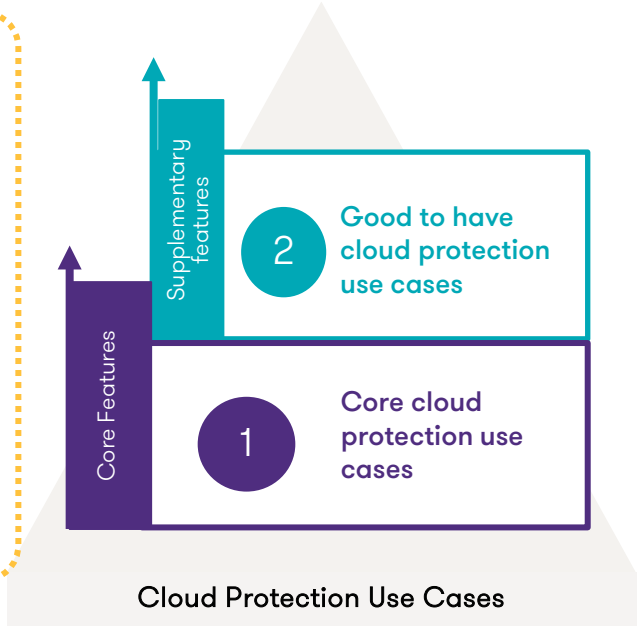
Define data retention and leakage protection requirements.

Develop data purge scripts, approval, archival, and retrieval processes along with purge schedules based on age of system / data and the organization's retention schedule

Select the preferred DSPM tool for testing controls and configure based on in-scope data type, environments, and applications

Define use cases for data protection in a cloud environment

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

Loading...

Poll Everywhere

Data governance and data protection

Activities

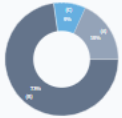
Visual settings

Edit

When poll is active respond at **PollEv.com/gtiac713** Send **gtiac713** to **37607**

What's your level of confidence that your organization has strong data governance practices in place?

Low Medium High



Powered by Poll Everywhere

Testing strategies for data governance and data protection

Technical controls in the cloud can be challenging to audit when new instances can be created at a click of button. Internal audit needs to focus on security-by-design that helps enable secure business operations.

Data Governance

- Policies and procedures for including data management roles and responsibilities, etc.,
- Data Management and review level of **access in line with data storage, backup, recovery, data classification, data retention standards and data protection requirements**
- **Data protection controls identification, and operationalization of ownership & responsibilities**

Data Inventory & Classification

- **Review design and development of data inventory and data storage,** (data type, data structure, data security practices)
- Data classification, data tagging, data quality review, and testing strategy
- **Application of data protection controls** (risk exceptions)

Data Access & Data Flows

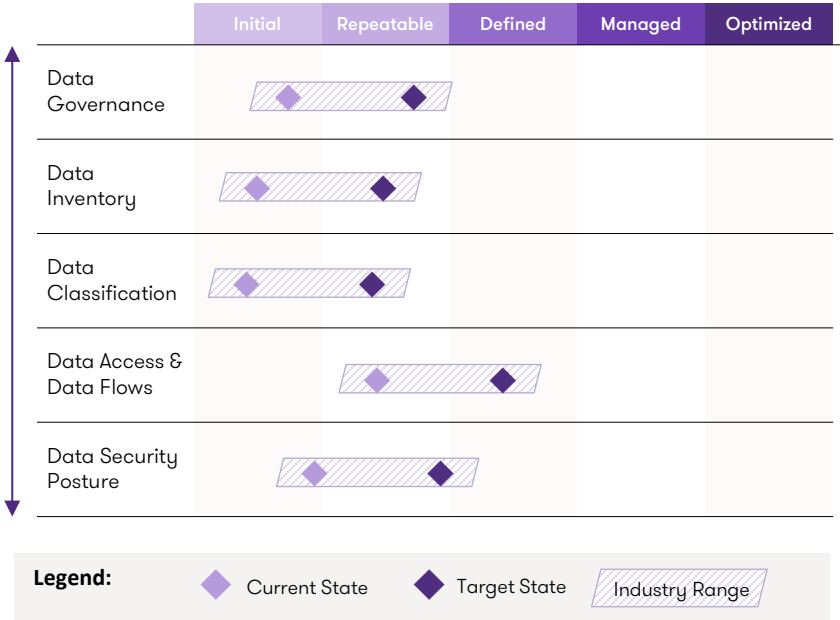
- **Data access, data flow documentation** (data processed, stored or transmitted)
- Data ownership and stewardship of all relevant personal and sensitive data (including location)
- Data privacy – DPIA, protection of data during transmission, data access, reversal, rectification and deletion, data disclosure, limited use, retention, deletion, disclosure

Data Security Posture

- Encryption and key management policies, procedures, roles and responsibilities
- Data encryption requirements on classified data and using encryption technology
- **Encryption and key management** (e.g., key generation, revocation, restoration, destruction etc.,)

Data management maturity analysis

Knowing where the greatest risks and opportunities are within the organization is critical, however, being able to determine the best path forward is equally as important. This will help "right-size" the desired future state considering strategic goals, operational objectives and available investment resources using our own experience and leading practice frameworks such as CCM/CIS.



MATURITY LEVELS

1 Initial	Limited program components, with ad-hoc processes and limited reporting. Lack of consistency in documented policies and procedures, and supporting technologies are not implemented/configured appropriately.
2 Repeatable	Stakeholders are established and given ownership over specific tasks; high level documentation is available but may not be consistently utilized. Process is planned and performed, but not routinely assessed.
3 Defined	Process is well defined and are described in standards, procedures, tools and methods. Periodic testing occurs and is used to measure and evaluate process.
4 Managed	Process is measured using defined metrics that demonstrate how the process is beneficial to business operation. Process has been repeatedly tested, refined and adapted in multiple conditions across the organization.
5 Optimized	Process is continuously monitored and improved as needed. Process is flexible enough to accommodate new technology and innovation in the organization.

CMMI MATURITY CAPABILITY DIMENSIONS *

Governance & oversight	Risk metrics & dashboards	Policies & Standards	Management processes	Tools & technologies

** The maturity definition is based on the Capability Maturity Model Integration (CMMI) maturity model. The maturity is evaluated based on the CMMI capability dimensions.*

Grant Thornton

Data security maturity roadmap

1

Define a data security program governance and operating model

2

Identify business use cases and define data classification, labeling and handling processes

3

Operationalize data protection controls based on a defined strategy

4

Review data protection controls through Data Security Posture Management (DSPM) audit

5

Perform testing, identify control gaps, prioritize and remediate findings through a risk mitigation strategy

6

Monitor and report, assign accountability and continuously evaluate data security posture, perform assurance review to ensure sustainability

Grant Thornton

Recap

Recap

1. We discussed data trends and the evolving threat landscape

2. We discussed examples of how organizations are effectively implementing data governance strategies and lessons learned

3. We discussed compliance challenges, and risks related to misconfiguration, and limited visibility into data sets/structures

4. We discussed how technologies impact existing data governance strategies and data protection controls

5. We discussed about how technical controls can be used to enhanced data governance with a data protection framework

6. We identified and discussed strategies for organizations to continually improve their data governance and data protection controls by taking a data-first approach

Questions?

Vik Rai

Grant Thornton
Managing Director,
Risk Advisory, Cybersecurity
Vikrant.Rai@us.gt.com

Grant Thornton

Thank you for attending

www.gt.com

twitter.com/GrantThorntonUS

linkd.in/GrantThorntonUS

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

Grant Thornton