Data Governance and Risk Management

Internal Audits Role in Assessing Data Governance and Data Risk Management Maturity

The Institute of Internal Auditors

Cherry Bekaert

Your Guide Forward

Today’s Presenters

Scott Peyton, CPA

Partner, Risk Advisory Practice Leader

Cherry Bekaert Advisory LLC

scott.peyton@cbh.com

Dan Sembler, CPA, CISA

Partner, Information Assurance & Cybersecurity

Cherry Bekaert Advisory LLC

dsembler@cbh.com

Learning Objectives

- Define key data stakeholder groups including their roles, responsibilities, and common stakeholder misconceptions
- Describe effective data governance models including structure, policies, and procedures.
- Describe the stages of data governance and risk management maturity including key milestones.
- Cite examples of data privacy and protection requirements and leading practice compliance programs.
- Identify an internal audit approach to assess the maturity of data governance and risk management leveraging leading frameworks and industry leading practices.

Polling Question 1

What experience do you have with Data Risk Management audits?

A. None
B. Some
C. Significant
D. It is my entire job

The Institute of Internal Auditors

Cherry Bekaert
Your Guide Forward

Data Governance
An Overview

Data Governance Defined

Data governance:
is the system of internal policies, protocols, and procedures used to manage, access, and secure enterprise data.

Goal of Data Governance:
to help people efficiently and securely use the vast amounts of data generated by today's enterprises.

Common Features:
Internal processes, policies, defined roles, metrics, and compliance standards.

Why it Matters:
Secure data governance keeps data organized and consistent, defines who can and cannot access data, and helps organizations handle data—especially customer data— in compliance with relevant standards and regulations.

Key Data Stakeholders and Their Responsibilities

Data Governance Stakeholders

Key roles and responsibilities of the major groups within a data governance framework:

PLAN & MANAGE

KEY ROLES AND RESPONSIBILITIES

Data Owners

These individuals, often at a business level, have ultimate accountability for the data within their domain, ensuring its accuracy, completeness, and security.

Data Stewards

Subject matter experts who work with data owners to implement data governance policies, manage data quality, and resolve data issues.

Data Custodians

Responsible for the technical aspects of data governance, including storage, access, and data integrity.

Data Architects

Design and implement data architectures that support data governance, ensuring data standards are followed.

EXECUTE

KEY INDIVIDUALS / GROUPS

Chief Data Officer (CDO)

The leader of data governance, responsible for defining and implementing data policies, standards, and procedures.

Data Governance Committee

A group that oversees the data governance program, setting policies and standards, and making decisions related to data management.

Executive Sponsors

High-level executives who champion data governance initiatives and secure necessary resources and support.

Common Misconceptions

Data Governance and Stakeholder Responsibilities

Data governance is a one-time project

Most data governance failures are caused by technology shortfalls

Data governance is a burden, not a benefit

Only IT personnel need be concerned with data governance

Data governance is a compliance checkbox

Effective data governance can be achieved through tools and software alone

Polling Question 2

Which of the following have a role in Data Governance?

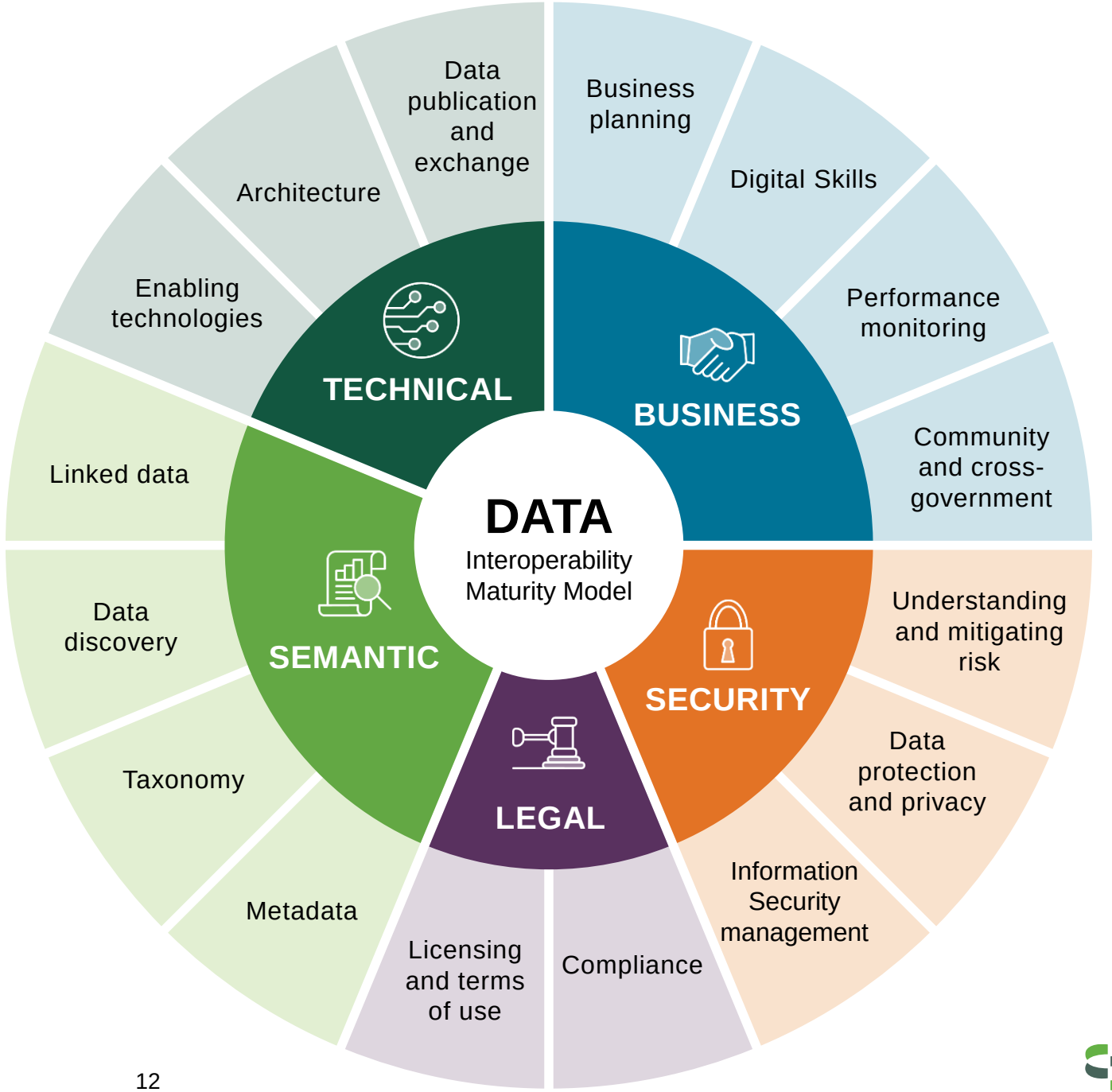
A. Finance
B. IT
C. Legal
D. HR
E. All of the above + more

The Institute of Internal Auditors

Cherry Bekaert
Your Guide Forward

Effective Data Governance and Risk Management

Data Governance and Data Risk Management Interoperability



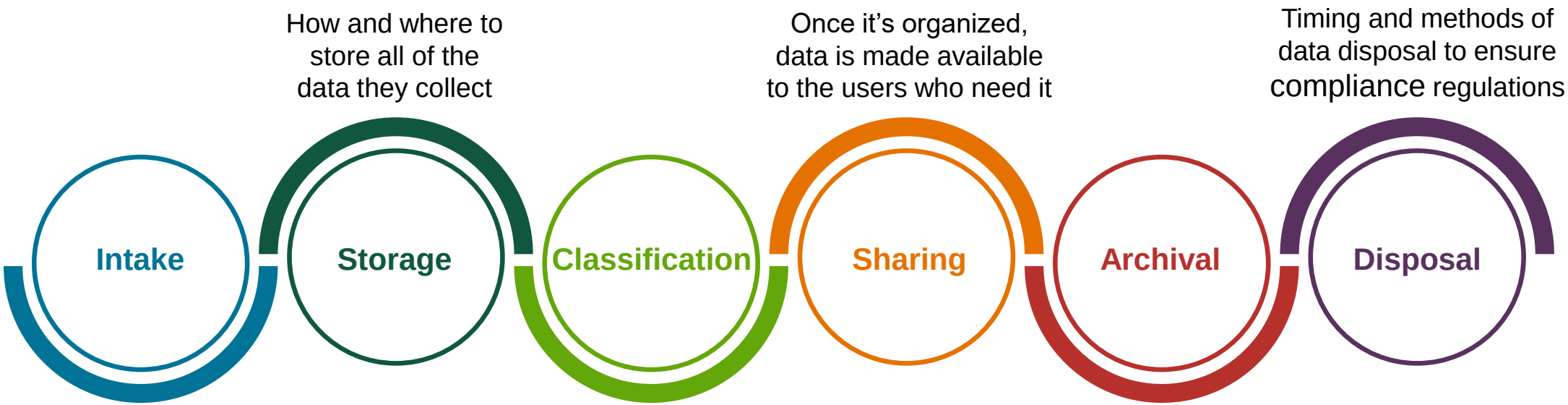
Policies and Procedures

It is critical that data governance and risk management be well defined through data policies and supporting procedures. Following are

- Policies should include clear definitions of data ownership, roles, and quality standards.
- Enterprise polices should be supported with specific capability (e.g., IT, etc.) and business unit criteria.
- Access controls, retention requirements, and regulatory guidelines should be explicitly stated within.
- Specific data privacy and security should be considered within policy requirements such as GDPR, GLBA, HIPAA and others.
- Appropriate methods of sharing data should be established within the policy and enforcement mechanism should be established in the tools that store data and are used to share data.

Data Lifecycle Management

A key part of data governance is managing data from intake to disposal, usually using data governance tools. Details may vary between organizations and use cases, but data lifecycle management typically includes:



Throughout all of these steps, data must remain secure and compliant. A well-designed data governance strategy defines what steps and regulations are needed to maintain compliance and security.

Data Governance Best Practices

Here are examples of best practices that organizations can follow as they develop and implement their data governance systems:

Strategic

Designate an executive data sponsor. Data governance adoption starts with leadership. The sponsor represents the system and advocates for its usage across the organization.

Build a business case. Identify organizational goals and benefits to justify the time and resources required to create a data governance system.

Think big, start small. Set data goals at a high level and then design granular project objectives that build towards those goals.

Data privacy and security by default. Privacy and security are two of the most important things to keep in mind when you think about data.

Tactical

Know your data. All your data. Gather a complete inventory of all data types, structures and locations. All data needs to be considered, including metadata and unstructured data from collaborative tools, SaaS applications, and other shared files.

Data quality management. Establishing data quality requirements as an enterprise mandate helps maximize the potential of your data assets for informed decision-making, competitive positioning, and customer satisfaction.

Build the right toolset. With so much data accessible, its critical to have a suite of tools to identify, inventory, secure, access, and dispose of data efficiently and accurately.

The Data Capability Maturity Model (CMM)

The CMM model identifies five stages of data maturity

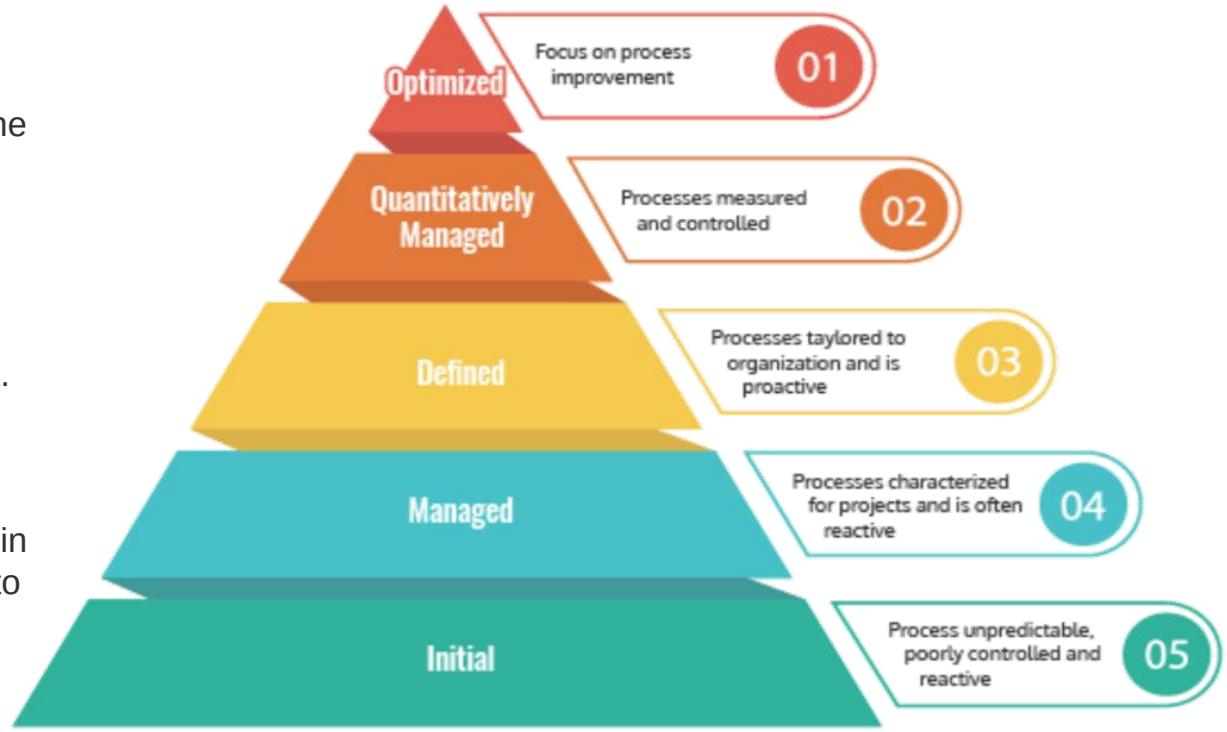
5. Optimized:
The data can be reused cross organizations/communities with a minimum of effort. Data can be maintained throughout time. Usage of data is monitored.

4. Managed:
Data is linked and metadata follows community standards. Organization wide services are available for searching and accessing data sets. Machine accessibility and data linking is fully achieved.

3. Defined:
Data sets can be utilized by other parties with a minimal effort. Organizational and community standards are utilized, variations are documented. Linking data sets can be achieved with some mapping effort. Access and sustainability processes are well defined.

2. Repeatable:
Data usage is limited, only possible with help of experts who are involved in the project and requires manual effort. Domain experts help are required to interpret the data. Data access is governed mostly by the project owners.

1. Initial:
Data reuse is not possible outside of the project or department who produced the data sets. No long-term solutions for data sustainability and access.



Polling Question 3

Which stage of the Data Capability Maturity Model defines itself as having data that can be utilized by other parties with a minimal effort?

A. Repeatable
B. Managed
C. Defined
D. Optimized

The Institute of Internal Auditors

Cherry Bekaert
Your Guide Forward

Data Privacy and Protection Considerations

Data Privacy Considerations

US Data Privacy Regulation

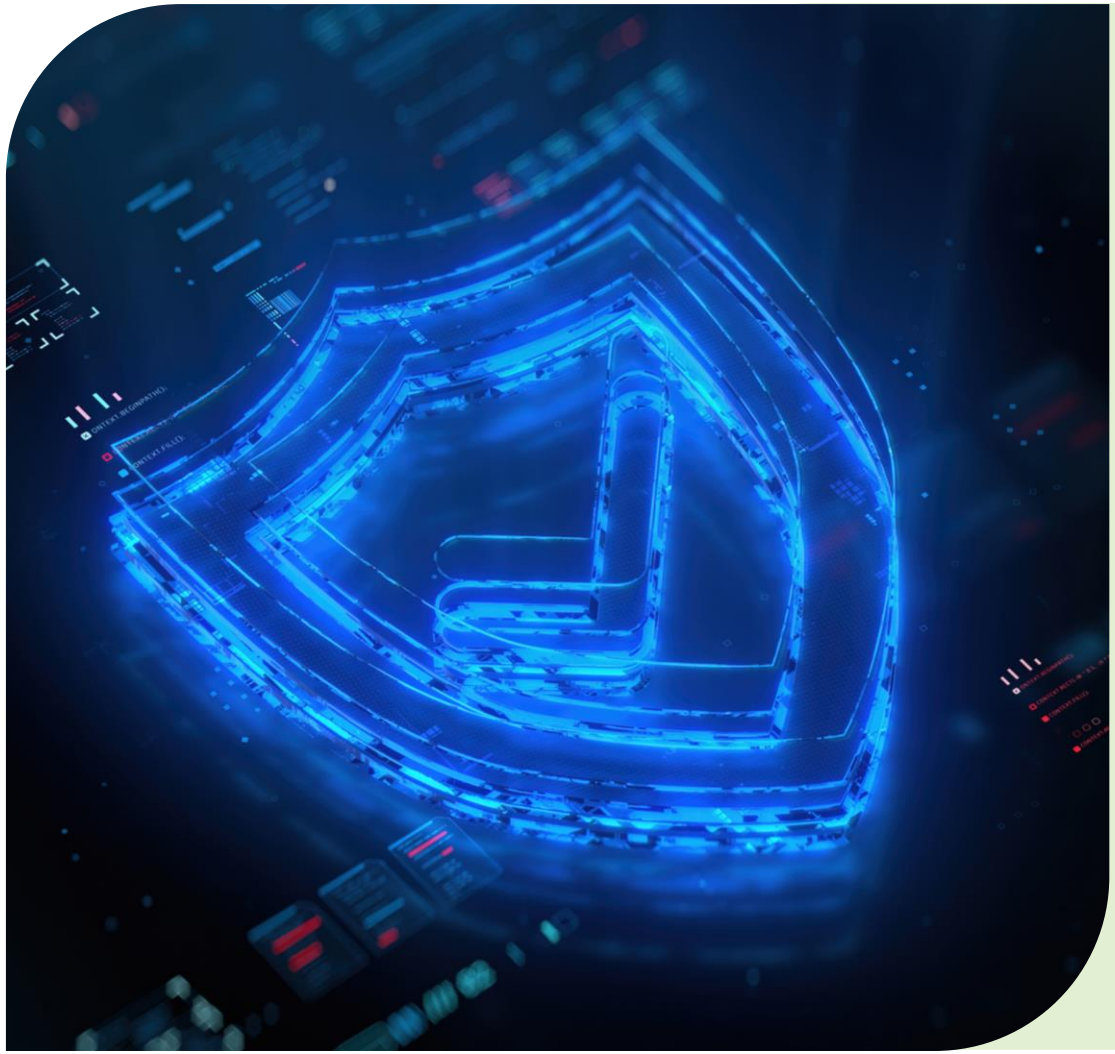
- Although no single law exists for all data in the U.S., there are still sector specific requirements and best practices.
- Regulations such as the Children's Online Privacy Protection Act (COPPA) for child data, the Gramm-Leach-Bliley Act (GLBA) for financial information are examples of these.

International Data Privacy Regulation

- In the EU, the General Data Protection Regulation (GDPR) requires all businesses to comply with privacy and protection requires for data belonging to its citizens.
- In Asia, data privacy laws are quickly emerging and are continuously updated. For example, the Malaysian Personal Data Protection Act, which mimics the EU's GDPR.
- If your company conducts business internationally, businesses are typically required to comply with the strictest laws in which it is operating for all customer data.

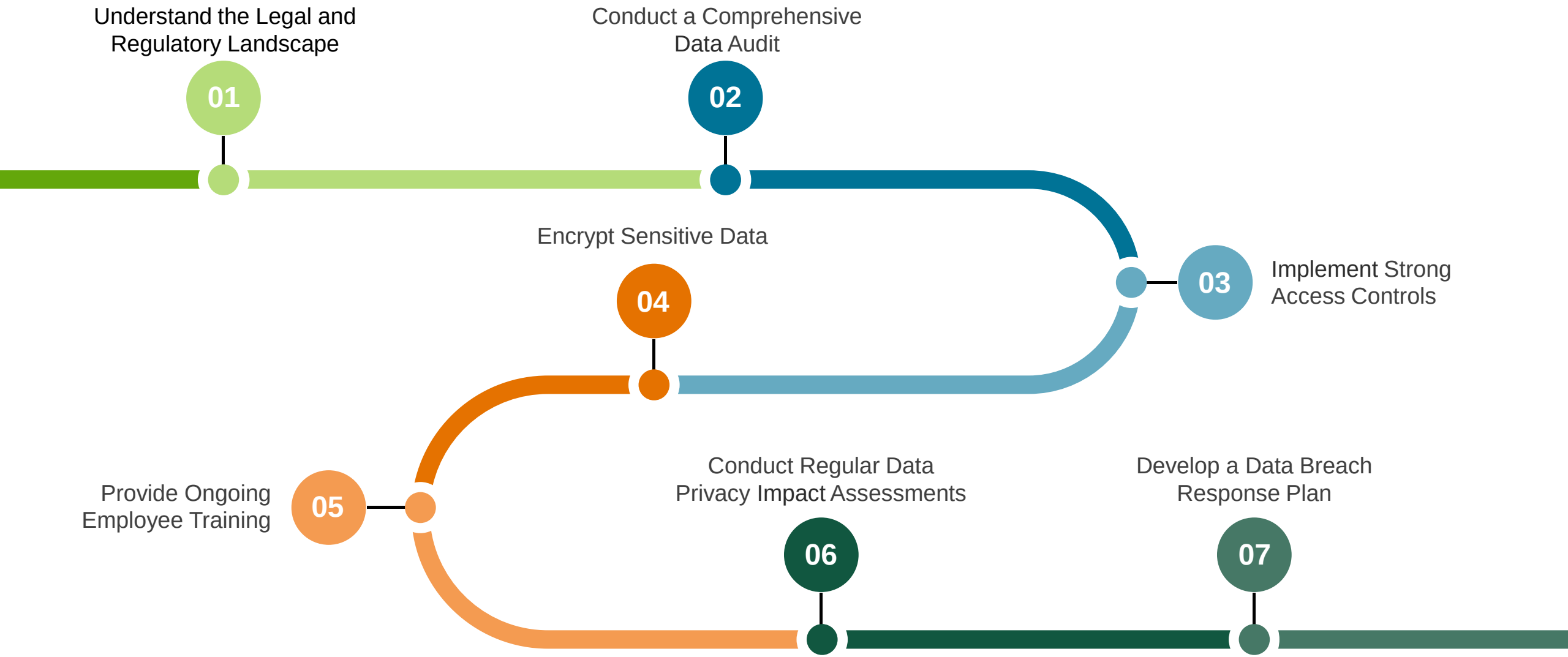
Internal audit programs are generally developed based off one of these specific requirements.

Key Components To A Data Privacy Program



- Consent
- Restriction
- Monitoring
- Communication
- Governance
- Classification
- Retention
- Inventory
- Documentation
- Remediation
- Third parties
- Management
- Compliance
- Assessment
- Training
- Identity

Best Practices for Data Privacy Management



Data Privacy vs. Data Security

Governing how data is collected, shared and used

Protecting data from internal and external attackers/unauthorized access

Data Privacy vs. Data Security

Aspects	Data Privacy	Data Security
Focus	Responsible handling of personal data, individuals' control	Protecting data from illegal access, breaches, cyber threats
Goal	Protect privacy, promote transparency, informed consent	Safeguard data assets, prevent cyber threats, ensure security
Scope	User permission, defining personal data, data sharing guidelines	Encryption, access controls, intrusion detection, network security
Components	Data anonymization, consent systems, privacy policies	Firewalls, antivirus, intrusion detection, secure authentication
Legal Framework	GDPR (EU), HIPAA (US), individuals' rights	ISO 27001, international standards, best practices

Data Governance and Risk Management

An Internal Audit Approach

Key Data Assessment Elements

An effective internal audit of data governance and risk management should consider each of the following key elements:

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

Train employees on the data classification policy and solution; and develop awareness campaigns to promote the importance of classifying their files and documents.

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

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

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

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

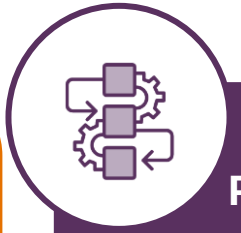
Data Governance Scoping Considerations

Inventory And Geography

- Understand the full inventory of in-scope data types and sources
- Evaluate data hosting and geographic locations
- Consider structure of data sources
- Verify data inventory processes, controls and technology solutions

Governance

- Data governance Charter and Data Steering Committee
- Policies, runbook, procedures and standards
- Roles and responsibilities
- Data management framework and strategy
- Compliance and risk framework
- KPIs and KRIs



Processes

- Business and data processes i.e. Data flow process and diagrams defined, developed
- Security, privacy & regulatory compliance
- Measurement & monitoring
- Communication & change management
- Technology mapping to key processes and controls

Systems

- Systems that store data (e.g., ERPs etc.)
- Master Data Management (MDM) tools
- Systems that are used for security of data
- Data quality & lineage tools
- Tools used for management and monitoring of data

Data Governance Project Approach

	1. Planning and Kickoff	2. Assessment	3. Report and Roadmap
Key Activities	► Confirm project scope, requirements, approach, deliverables, and resources ► Develop full scope of data types, hosting, and geo location ► Gain understanding of data governance structure and key data stakeholders ► Release the document request list and obtain relevant documentation ► Provide interview schedules for confirmed data governance stakeholders ► Decide on meeting cadence with project sponsor for status briefings on any project issues, milestones, and accomplishments ► Agree on risk-ranking criteria and final report with the project sponsor	► Review past internal audit findings along with data governance documentation to leverage existing findings and identify gaps ► Review data governance, risk management and data inventory documentation and map against the risk assessment toolkit ► Conduct workshops to evaluate data governance structure, data lifecycle management, and data privacy and protection ► Work with stakeholders to identify target maturity level ► Record identified gaps in the toolkit ► Perform risk analysis to risk-rank the identified gaps and develop risk mitigation or reduction recommendations	► Socialize and finalize the audit findings and conclusions with the key stakeholders ► Develop a detailed assessment report to include: • Executive Summary • Data governance structure, roles and responsibilities • Logically grouped assessment results and recommendations ► Develop a prioritized transformation blueprint with high level estimates on resource and timeline for different projects, keeping in mind constraints and in-flight projects ► Present the executive summary and transformation roadmap to senior or executive leadership and gather feedback to adjust recommendations
Deliverables	► Kick-off presentation ► Project plan ► Tailored assessment toolkit ► Interview schedule	► Data governance and risk management assessment results ► Assessment overview and maturity score ► Initial recommendations	► Final assessment report including: • Executive summary • Detailed assessment results • Transformation blueprint for the suggested enhancements

Consider Key Data Governance Elements

As you build your audit program, consider aligning the various data governance and risk management elements across the core data management domains.

Proposed Audit Objectives

#	Sub Process	Focus	Strategic	Operational	Compliance
1.1	Strategy	Evaluate the data governance strategy and key objectives for the following: • Definition of data governance vision and mission • Evaluate the goal of data governance strategy, how it is being implemented and helping organization achieve their goal • Evaluate alignment of the data governance strategy with corporate objectives and business alignment • Evaluate the guiding principles to achieve the data strategy • Evaluate reports from any prior data related strategic or risk assessments	✓		
1.2	Policies, Procedures & Standards				
1.3	Organization Model	Evaluate the organization operating model to: • Ensure it aligns to the business and IT objectives, strategy • Ensure decision makers and escalation points are documented and clearly identified, trained • Data governance organization members, steering committee have been defined and implemented • Roles and responsibilities are defined and implemented for data governance / data management • Data ownership and accountability are defined and in line with best practices	✓	✓	
1.4	Security, Privacy & Regulatory Compliance				
1.6	Technology	Assess data governance technology controls in the organization to ensure: • Technology controls are effective for data governance, data management in line with defined strategy e.g. data quality and lineage tools, ERP (SAP etc.).. • A data mastering and sharing process exists and is in line with industry standards • A framework exists for privacy, compliance requirements and if the organization has assessed and tracks its data process and flow against these requirements • Data and stewardship workflows are defined and documented for a data governance program and in line with organization policy	✓	✓	✓
1.5	Measurement & Monitoring				
1.7	Communication	Assess the data governance communication plan to evaluate • If it is in line with the wider organization communication plan and controls are defined for training user in relation to data quality, use of data, security of data etc. • Communication plan is shared with the right stakeholders in the organization, thus making them aware of their responsibilities	✓	✓	

Polling Question 4

Do you have your Data Governance in your 2025 audit plan?

A. Yes
B. No
C. Elements of Data Governance, but not the enterprise program

The Institute of Internal Auditors

Cherry Bekaert
Your Guide Forward

Questions?

Scott Peyton, CPA

scott.peyton@cbh.com

Dan Sembler, CPA, CISA

dsembler@cbh.com

cbh.com

Cherry Bekaert
Your Guide Forward