



Data Governance Policies and Procedures

IS465: Data Management and Governance

Outline

- Data Governance Policies
- Data Governance Standards
- Data Governance Procedures
- Data Governance Implementation
- Metrics, Reports, and Risks

Data Governance Policies

Data Governance Policies

- Data governance policies are the rules, procedures, and guidelines that organizations follow to ensure the effective management of their data assets.
- The purpose of data governance policies is to ensure data quality, security, accessibility, and retention.

Data Governance Policy



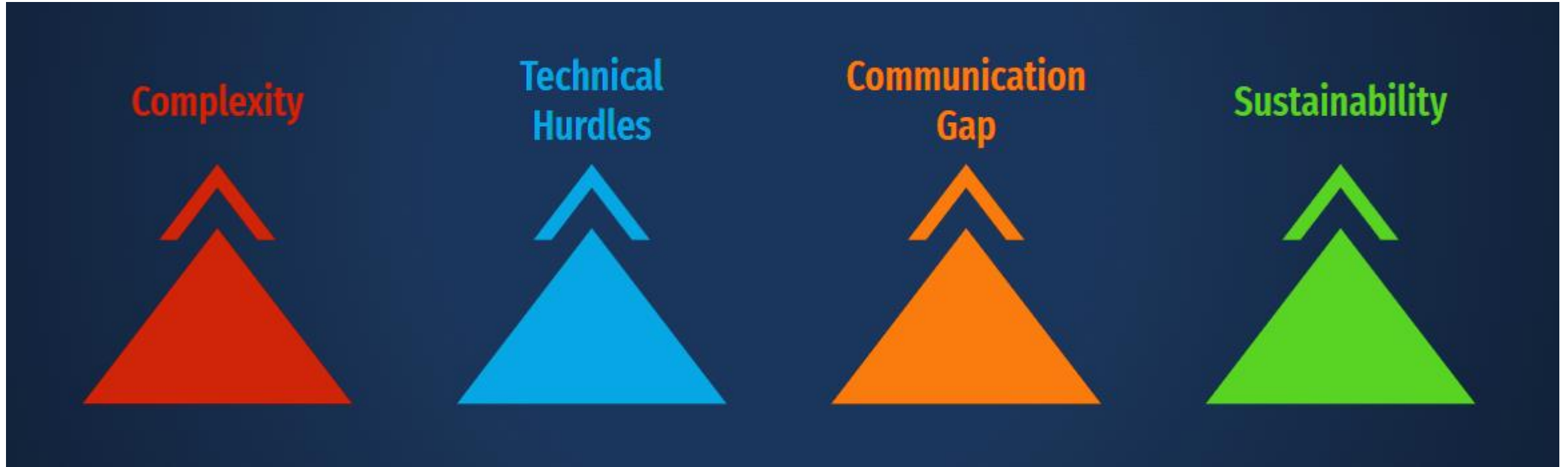
Importance of Data Governance Policies

- Data governance policies are essential for ensuring data quality, security, accessibility, and retention.
- They help organizations comply with legal and regulatory requirements related to data management.
- They promote data sharing and collaboration across different departments and teams.
- They help organizations make informed decisions based on accurate and reliable data.

Why Are Data Governance Policies Important?



Challenges Organizations Face



The Policy Framework



Types of Data Governance Policies

- Data quality policies
- Data security policies
- Data access policies
- Data retention policies
- Data classification policies

Data Quality Policies

- Data quality policies aim to ensure that data is accurate, complete, and consistent.
- Examples of data quality policies include:
 - Data validation rules
 - Data cleansing procedures
 - Data normalization standards

Data Security Policies

- Data security policies aim to protect data from unauthorized access, corruption, or loss.
- Examples of data security policies include:
 - Access controls
 - Encryption protocols
 - Authentication procedures

Data Access Policies

- Data access policies aim to ensure that data is accessible to authorized users and groups.
- Examples of data access policies include:
 - User authentication procedures
 - Authorization protocols
 - Role-based access controls

Data Retention Policies

- Data retention policies aim to ensure that data is properly stored and retained according to organizational policies and legal requirements.
- Examples of data retention policies include:
 - Data backup procedures
 - Data archiving protocols
 - Retention schedules

Data Governance Standards

Data Governance Standards

- Data governance standards are guidelines and frameworks that organizations follow to ensure the effective management of their data assets.
- The purpose of data governance standards is to provide a consistent and repeatable approach to data management, ensuring data quality, security, accessibility, and retention.

Importance of Data Governance Standards

- Data governance standards are essential for ensuring data quality, security, accessibility, and retention.
- They help organizations comply with legal and regulatory requirements related to data management.
- They promote data sharing and collaboration across different departments and teams.
- They help organizations make informed decisions based on accurate and reliable data.

Types of Data Governance Standards

- Industry-specific standards
 - These standards are developed for specific industries, such as healthcare, finance, and retail.
- Generic standards
 - These standards can be applied to any industry and are developed by organizations such as ISO and ITU.
- Framework standards
 - These standards provide a structured approach to data governance, such as the Data Governance Body of Knowledge (DGBOK) and the Information Governance Initiative (IGI).

Industry-Specific Data Governance Standards

- Examples of industry-specific data governance standards include:
 - HIPAA (Health Insurance Portability and Accountability Act) for healthcare
 - GDPR (General Data Protection Regulation) for EU data protection
 - PCI-DSS (Payment Card Industry Data Security Standard) for payment card data
 - FISMA (Federal Information Security Management Act) for US federal government data

Generic Data Governance Standards

- Examples of generic data governance standards include:
 - ISO/IEC 27001:2022
 - Information security, cybersecurity and privacy protection - Information security management systems
 - ITU-T
 - (International Telecommunication Union - Telecommunication standardization sector) recommendations
 - COBIT
 - (Control Objectives for Information and Related Technology) framework

Framework Data Governance Standards

- Examples of framework data governance standards include:
 - Data Governance Body of Knowledge (DGBOK)
 - Information Governance Initiative (IGI)
 - Data Governance Framework (DGF)

Benefits of Implementing Data Governance Standards

- Implementing data governance standards can help organizations:
 - Ensure data quality, security, accessibility, and retention
 - Comply with legal and regulatory requirements
 - Promote data sharing and collaboration
 - Make informed decisions based on accurate and reliable data
 - Reduce data-related risks and costs

Data Governance Procedures

Data Governance Procedures

- Data governance procedures are the specific steps and processes that organizations follow to ensure the effective management of their data assets.
- The purpose of data governance procedures is to provide a structured approach to data management, ensuring data quality, security, accessibility, and retention.

Importance of Data Governance Procedures

- Data governance procedures are essential for ensuring data quality, security, accessibility, and retention.
- They help organizations comply with legal and regulatory requirements related to data management.
- They promote data sharing and collaboration across different departments and teams.
- They help organizations make informed decisions based on accurate and reliable data.

Types of Data Governance Procedures

- Data management procedures
- Data security procedures
- Data quality procedures
- Data retention procedures

Data Management Procedures

- Examples of data management procedures include:
 - Data creation: Ensuring that new data is created and captured accurately and completely.
 - Data modification: Ensuring that data is updated and modified accurately and completely.
 - Data deletion: Ensuring that data is deleted appropriately and securely.
 - Data archiving: Ensuring that data is transferred to long-term storage appropriately and securely.

Data Security Procedures

- Examples of data security procedures include:
 - Encryption: Protecting data from unauthorized access by using encryption techniques.
 - Access controls: Restricting access to data based on user roles and permissions.
 - Authentication: Verifying the identity of users before granting access to data.
 - Authorization: Granting access to data based on user roles and permissions.

Data Quality Procedures

- Examples of data quality procedures include:
 - Data validation: Checking data for accuracy and completeness.
 - Data cleansing: Identifying and correcting errors or inconsistencies in data.
 - Data normalization: Transforming data into a consistent format.

Data Retention Procedures

- Examples of data retention procedures include:
 - Data backups: Creating copies of data to protect against data loss.
 - Data archiving: Transferring data to long-term storage.
 - Data disposal: Disposing of data securely and appropriately.

Data Governance Implementation

Key Data Governance Best Practices

- Define data governance roles and responsibilities.
- Establish data management policies and procedures.
- Implement data security measures.
- Monitor and audit data access and use.
- Provide training and awareness programs.
- Regularly review and update data governance policies and procedures.

Importance of Data Governance Implementation

- Data governance implementation is essential for ensuring data quality, security, accessibility, and retention.
- It helps organizations comply with legal and regulatory requirements related to data management.
- It promotes data sharing and collaboration across different departments and teams.
- It helps organizations make informed decisions based on accurate and reliable data.

Key Steps in Data Governance Implementation

- Step 1: Define data governance roles and responsibilities.
- Step 2: Establish data management policies and procedures.
- Step 3: Implement data security measures.
- Step 4: Monitor and audit data access and use.
- Step 5: Provide training and awareness programs.
- Step 6: Regularly review and update data governance policies and procedures.

Metrics, Reports, and Risks

Importance of Data Governance Metrics

- Data governance metrics are essential for evaluating the effectiveness of data governance practices.
- They help organizations identify areas for improvement and measure progress over time.
- They provide a common language and framework for communication about data governance across different departments and teams.

Key Data Governance Metrics

- Metric 1: Data Quality Index (DQI) - measures the accuracy, completeness, and consistency of data.
- Metric 2: Data Security Index (DSI) - measures the effectiveness of data security measures.
- Metric 3: Data Accessibility Index (DAI) - measures the ease of access to data for authorized users.
- Metric 4: Data Retention Index (DRI) - measures the effectiveness of data retention policies and procedures.
- Metric 5: Data Governance Maturity Index (DGMI) - measures the overall maturity of data governance practices.

Data Quality Index (DQI)

- The Data Quality Index (DQI) measures the accuracy, completeness, and consistency of data.
- Calculation: $DQI = (Accuracy + Completeness + Consistency) / 3$
- Example: A DQI score of 0.8 indicates that data is 80% accurate, complete, and consistent.

Data Security Index (DSI)

- The Data Security Index (DSI) measures the effectiveness of data security measures.
- Calculation: $DSI = (Data\ Encryption + Access\ Controls + Incident\ Response) / 3$
- Example: A DSI score of 0.9 indicates that data security measures are 90% effective.

Importance of Data Governance Monitoring and Reporting

- Data governance monitoring and reporting are essential for ensuring data quality, security, accessibility, and retention.
- They help organizations comply with legal and regulatory requirements related to data management.
- They promote data sharing and collaboration across different departments and teams.
- They help organizations make informed decisions based on accurate and reliable data.

Key Data Governance Monitoring and Reporting Tools

- Tool 1: Data Governance Dashboards - provide real-time visibility into data quality, security, accessibility, and retention.
- Tool 2: Data Quality Reports - measure data accuracy, completeness, and consistency.
- Tool 3: Data Security Reports - measure data security controls and incident response.
- Tool 4: Data Accessibility Reports - measure data availability and usability.
- Tool 5: Data Retention Reports - measure data retention and disposal practices.

Data Governance Dashboards

- Data governance dashboards are interactive tools that provide real-time visibility into data quality, security, accessibility, and retention.
- Features:
 - Data quality metrics (e.g., accuracy, completeness, consistency)
 - Data security metrics (e.g., encryption, access controls, incident response)
 - Data accessibility metrics (e.g., data availability, usability)
 - Data retention metrics (e.g., data retention schedules, disposal practices)
- Benefits:
 - Real-time visibility into data governance practices
 - Easy-to-understand metrics and reports
 - Identification of areas for improvement

Data Quality Reports

- Data quality reports measure data accuracy, completeness, and consistency.
- Metrics:
 - Data accuracy (e.g., percentage of accurate data)
 - Data completeness (e.g., percentage of complete data)
 - Data consistency (e.g., percentage of consistent data)
- Benefits:
 - Identification of data quality issues
 - Tracking of data quality over time
 - Improvement of data quality practices

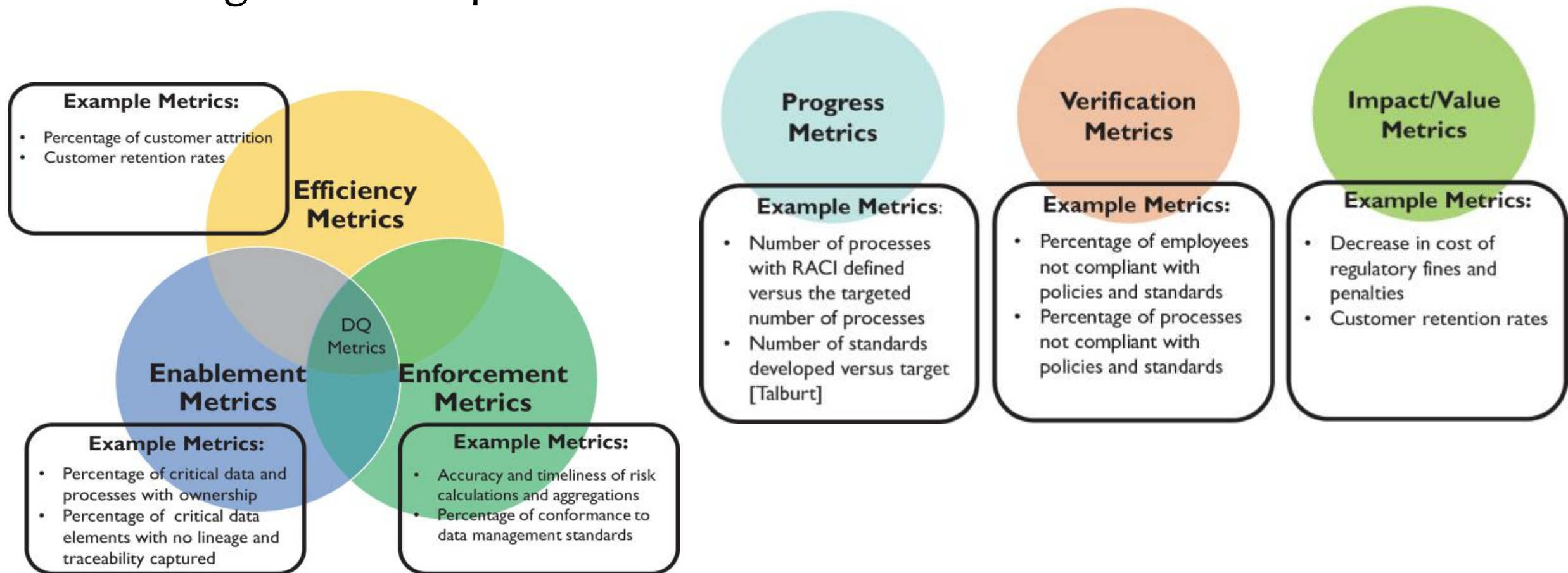
Importance of Data Governance Training and Awareness

- Data governance training and awareness are essential for ensuring effective data management practices.
- They help employees understand data governance policies, procedures, and best practices.
- They promote major data governance goals such as data quality, security, accessibility, and retention.



Data Governance Metrics and Performance Indicators

- Metrics and performance indicators are used to measure the effectiveness of data governance practices.



Data Governance Risk Management

- Data governance risk management involves identifying, assessing, and mitigating risks associated with data management.
- The purpose of data governance risk management is to ensure that data is accurate, complete, and protected from unauthorized access or misuse.

Importance of Data Governance Risk Management

- Data governance risk management is essential for ensuring the integrity and security of data.
- It helps organizations comply with legal and regulatory requirements related to data management.
- It promotes data sharing and collaboration across different departments and teams.
- It helps organizations make informed decisions based on accurate and reliable data.

Key Data Governance Risk Management Strategies

- Strategy 1: Data Classification
- Strategy 2: Access Control
- Strategy 3: Data Encryption
- Strategy 4: Data Backup and Recovery
- Strategy 5: Data Quality Control

Data Governance Risk Management Framework

- Framework:
 - Identify risks
 - Assess risks
 - Mitigate risks
 - Monitor risks
- Risk management process:
 - Risk identification
 - Risk assessment
 - Risk mitigation
 - Risk monitoring



Data Governance Risk Identification

- Identifying risks involves analyzing data management practices and identifying potential risks.
- Risks can include data breaches, data corruption, data loss, and non-compliance with regulations.
- Techniques for identifying risks include risk assessments, security audits, and compliance audits.

Data Governance Risk Assessment

- Risk assessment involves evaluating the likelihood and impact of identified risks.
- The likelihood of a risk occurring is determined by analyzing factors such as the probability of a security breach or data corruption.
- The impact of a risk occurring is determined by analyzing factors such as the potential financial loss or reputational damage.
- Risk assessment tools include risk matrices and risk heat maps.

Data Governance Risk Mitigation

- Risk mitigation involves implementing measures to reduce the likelihood or impact of identified risks.
- Measures can include implementing security controls, enforcing data access controls, and creating data backup and recovery plans.
- Risk mitigation strategies should be tailored to the specific risk and the organization's needs.

Data Governance Risk Monitoring

- Risk monitoring involves regularly reviewing and updating risk assessments and risk mitigation measures.
- Monitoring helps ensure that risk mitigation measures are effective and that new risks are identified and addressed.
- Risk monitoring tools include risk management software and dashboards.

Key Data Governance Future Trends

- Trend 1: Artificial Intelligence and Machine Learning
- Trend 2: Cloud Computing
- Trend 3: Blockchain
- Trend 4: Internet of Things (IoT)
- Trend 5: Data Privacy and Ethics

Preparing for Data Governance Future Trends

- Organizations should stay informed and proactive in adopting new technologies and practices.
- Develop a data governance strategy that accommodates emerging trends.
- Invest in employee training and upskilling to address future data management challenges.
- Foster a culture of data-driven decision-making and ethical data management.

Summary of Key Takeaways

- Data governance is a critical aspect of data management.
- Data governance roles and responsibilities are essential for ensuring data quality, security, accessibility, and retention.
- Data governance roles include data owners, data custodians, data users, and data stewards.
- Data governance responsibilities include data management, data security, data quality, data accessibility, and data retention.
- Effective data governance requires clear roles and responsibilities, data governance policies and procedures, and regular monitoring and reporting.

Final Thoughts and Call to Action

- Data governance is a continuous process that requires ongoing efforts and commitment.
- Implementing data governance can seem daunting, but it's essential for ensuring data integrity, security, and compliance.
- Start by identifying your organization's data governance needs and developing a data governance strategy.
- Assign clear roles and responsibilities, develop policies and procedures, and establish regular monitoring and reporting processes.
- Don't wait – start implementing data governance today to ensure your organization's data is accurate, secure, and compliant.