



GLOBAL CONFERENCE 2025

ENTERPRISE RISK MANAGEMENT:
RISING FROM THE ASHES

UNLEASHING YOUR
POTENTIAL AS A SECURITY
AND RISK CHAMPION

DR. USHA BALASUNDARAM
HEAD OF DATA GOVERNANCE
S&P GLOBAL

Data Governance

Unleashing Your Potential as a Security and Risk Champion

GLOBAL
CONFERENCE 2025
ENTERPRISE RISK MANAGEMENT:
RISING FROM THE ASHES

S&P Global

Disclaimer

The views expressed at, or through, this session are those of the individual presenters sharing in their capacities only – not those of their respective employer and research organization, **S&P Global** and **University of Science Malaysia** or committee / task force as a whole. All liability concerning action taken or not taken based on the contents of this presentation is hereby expressly disclaimed. The content on this posting is provided ‘as is’; no representations are made that the content is error-free.

About the Speaker



Dr. Usha
Balasundaram

- 20 + years of industry experience with 12 years in the Data Industry
- Key Projects include data scrubbing, data quality, data visualizations, data governance and predictive analytics data modelling for KPI targets.
- Current Role: Head of Data Governance
- Doctorate Research: **BIG DATA ANALYTICS CAPABILITY AND FIRM PERFORMANCE: THE MEDIATING ROLE OF DYNAMIC, OPERATIONAL, INNOVATIVE CAPABILITIES AND THE MODERATING ROLE OF DATA GOVERNANCE**
@ University of Science Malaysia



Evaluating and improving the performance of
existing governance programs

Strengthening Supply Chain Security



Conducting a Maturity **Assessment**



Framework Development Importance

Establishing a tailored framework based on industry standards is essential for accurately assessing governance maturity and ensuring alignment with organizational objectives and best practices.

Stakeholder Engagement Necessity

Actively involving stakeholders throughout the assessment process enhances the identification of gaps and fosters a collaborative approach to improving governance practices.

Continuous Improvement Focus

Implementing a system for ongoing monitoring and feedback is vital for adapting governance practices, ensuring they evolve in response to changing business needs and regulatory requirements.

Identifying **Gaps** in Roles, Processes, and Technologies



Role Clarity Enhancement

Establishing well-defined roles and responsibilities among data stewards, owners, and IT personnel is critical to eliminate overlaps and ensure accountability, thereby strengthening the overall governance framework.

Importance of Stakeholder Feedback in Governance



Enhancing Governance Frameworks

Integrating stakeholder feedback not only identifies specific challenges within data management but also fosters a culture of collaboration, ensuring that governance frameworks are continuously refined to meet evolving organizational needs and industry standards.

Assessing and Managing **Third-Party Risks**



Security Posture Assessment

Assessing the security posture of third-party vendors is crucial to understanding potential risks they may pose.

Thorough Evaluations

Conducting thorough evaluations of third-party partners helps identify vulnerabilities and areas of concern.

Risk Mitigation Strategies

Implementing risk mitigation strategies can significantly reduce the risks associated with external relationships.

Implementing controls for data use and protection

Becoming a Data-Driven Organization with Data Governance

Ensuring Data Quality and Compliance



Monitoring Data Quality Metrics

Systematic Metric Evaluation

Implementing a systematic evaluation of data quality metrics enables organizations to identify trends and anomalies over time, facilitating proactive management of data integrity and compliance risks.

Implementing Robust Security Protocols



Importance of Security Protocols

Robust security protocols are essential in the supply chain to protect sensitive information and assets.

Adherence to Standards

Enforcing security standards across the supply chain ensures compliance and reduces vulnerabilities to breaches.

Reducing Breach Likelihood

Effective security protocols lower the chances of security breaches by creating multiple layers of defense.



Regulatory Compliance Necessity

Regular updates to data privacy and security policies are essential for compliance with evolving regulations, such as GDPR and CCPA, minimizing legal risks and enhancing organizational credibility.



Stakeholder Collaboration Importance

Engaging diverse stakeholders in the policy update process ensures that the revised policies address practical challenges, fostering a culture of accountability and enhancing overall data governance effectiveness.

Continuous Improvement Mechanisms

Establishing feedback loops and utilizing automated tools for monitoring can significantly enhance the adaptability of data privacy policies, ensuring they remain relevant in a rapidly changing digital landscape.

Boosting data literacy throughout the organization

Enhancing Data Protection

Data Encryption and Access Control



Importance of Data Encryption

Data encryption is crucial for protecting sensitive information from unauthorized access and potential breaches.

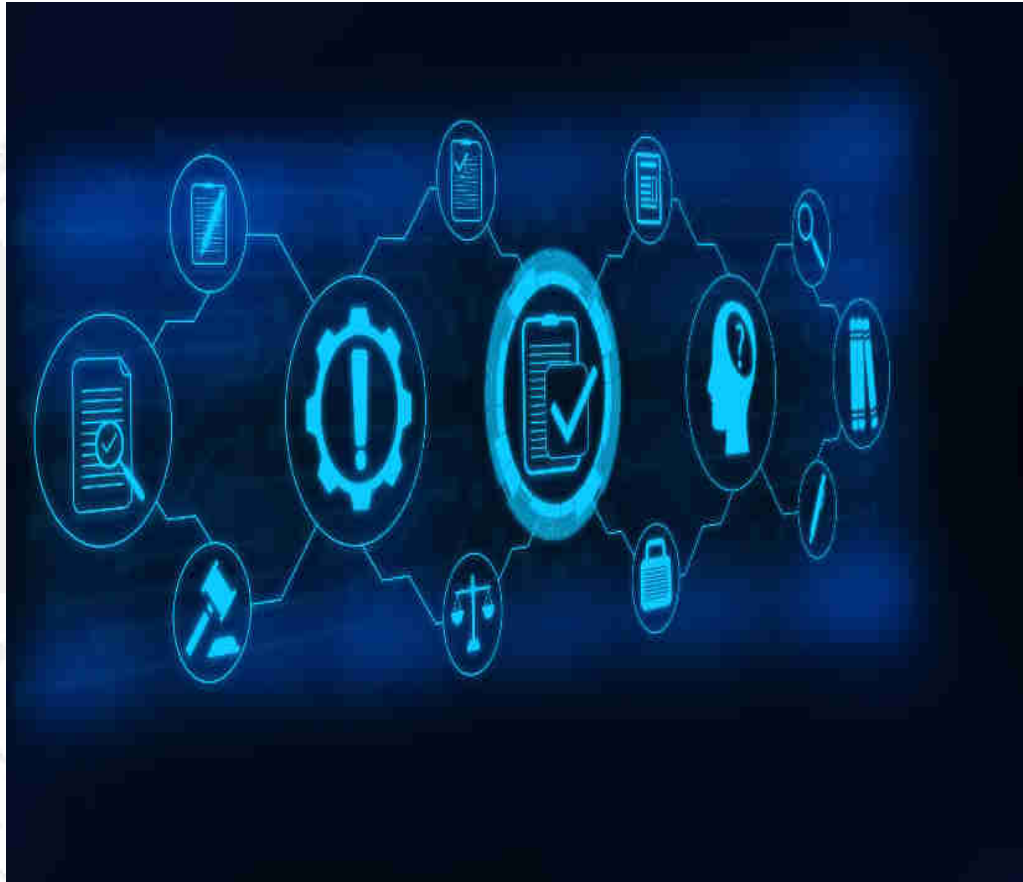
Access Control Measures

Strict access control measures ensure that only authorized users can access sensitive data, enhancing overall security.

Data Security Assurance

Combining encryption with access control provides a robust framework for data security and privacy compliance.

Regular Security Audits and Assessments



Identify Vulnerabilities

Regular security audits allow organizations to spot vulnerabilities in their systems before they can be exploited.

Ensure Compliance

Audits are essential for ensuring compliance with industry standards and regulations, minimizing legal risks.

Proactive Risk Management

Regular assessments support proactive management of potential risks, enabling timely remediation actions.

Investing in Tools and Talent

Being the true Champion

Training and Retaining Cybersecurity Professionals



Importance of Training

Investing in training helps cybersecurity professionals stay informed about the latest threats and security trends.

Retaining Cybersecurity Talent

Retaining skilled cybersecurity professionals is essential to maintain expertise and security within organizations.

Regular Security Audits and Assessments



Integrating Advanced Technologies

Organizations should leverage advanced technologies like AI and machine learning to enhance their security measures.

Framework Development

Developing comprehensive security frameworks is crucial for anticipating and responding to potential threats effectively.

Threat Anticipation

A proactive security infrastructure allows organizations to predict and prepare for potential security threats before they occur.



Conclusion

Comprehensive Security Approach with Governance

A holistic view of security integrates culture, technology, and strategy for effective management.

Protecting Assets

Prioritizing security and risk management helps safeguard organizational assets and resources from threats.

Driving Growth

Effective risk management not only protects but also facilitates growth in a dynamic business landscape.

Conclusion

Comprehensive Security Approach with Governance

A holistic view of security integrates culture, technology, and strategy for effective management.

Protecting Assets

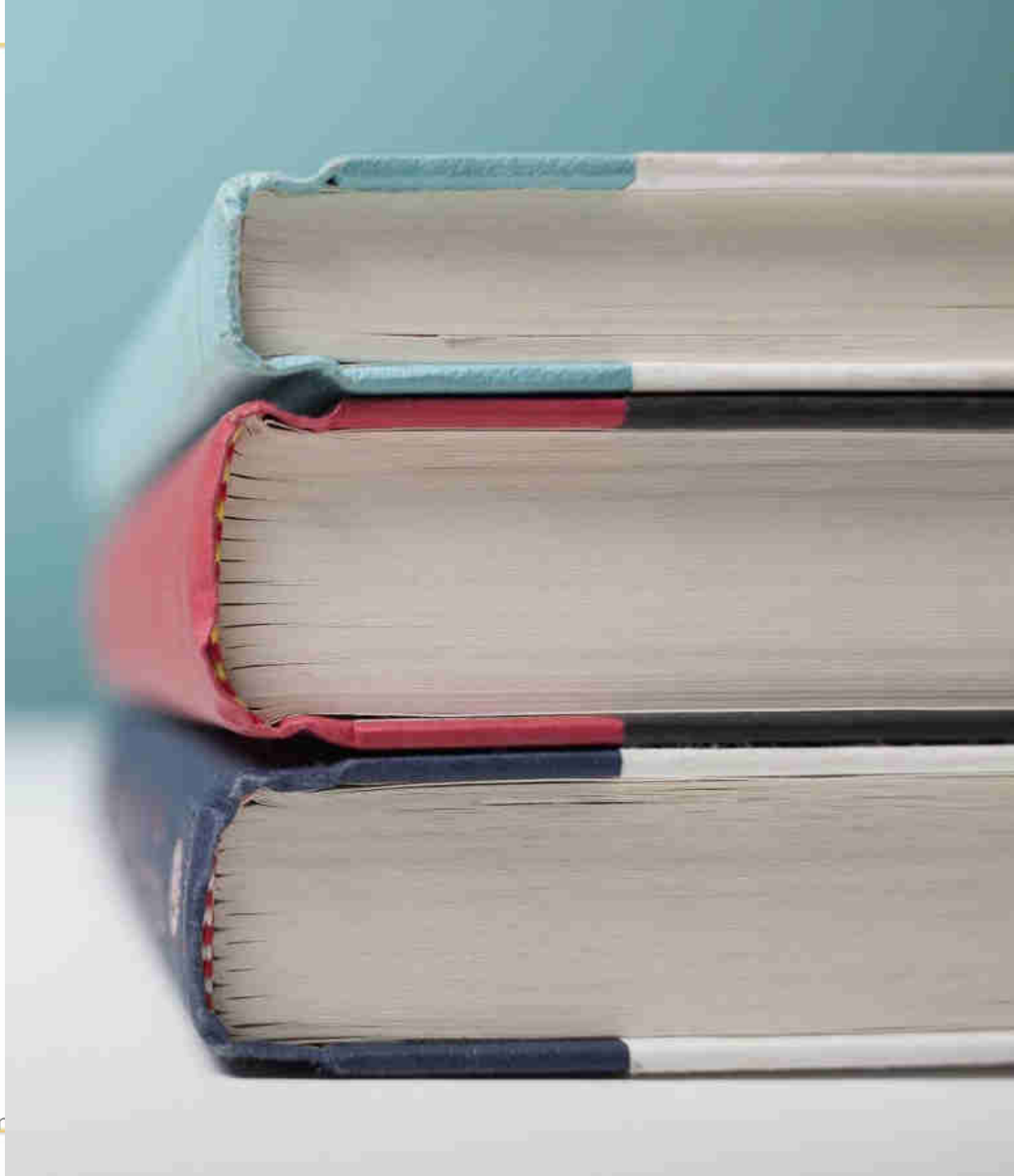
Prioritizing security and risk management helps safeguard organizational assets and resources from threats.

Driving Growth

Effective risk management not only protects but also facilitates growth in a dynamic business landscape.

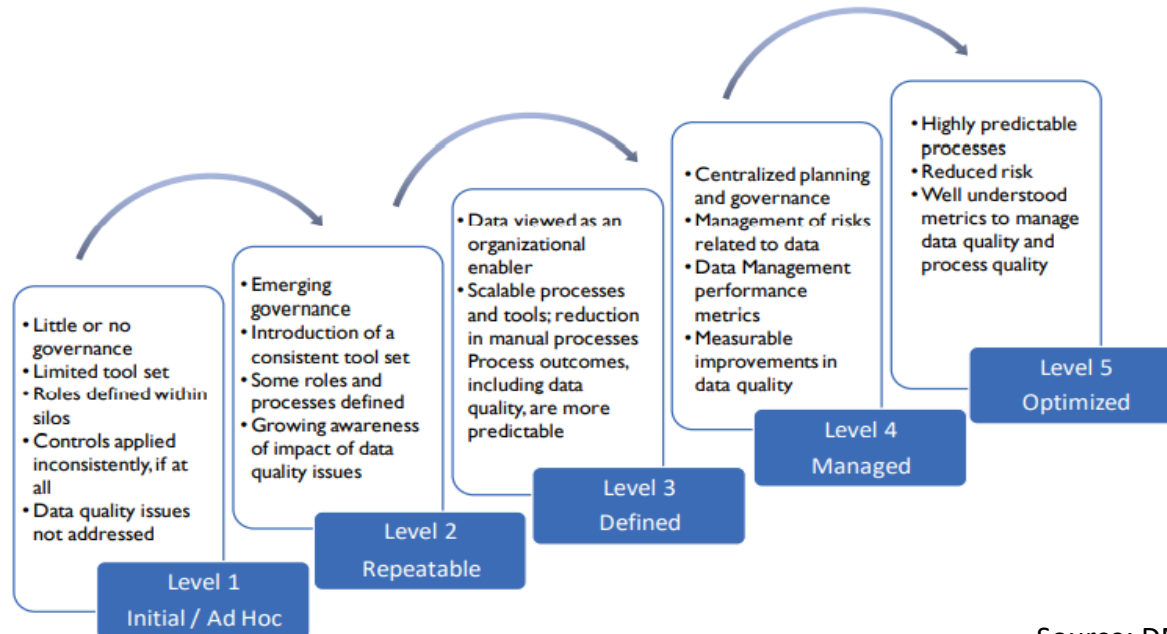
Appendix

5 Step Data Governance



Data Governance Implementation – Step 1

1. Understand current state of data management by conducting the Data Management Maturity Assessment. (DMMA) similar to CMM (Capability Maturity Model)



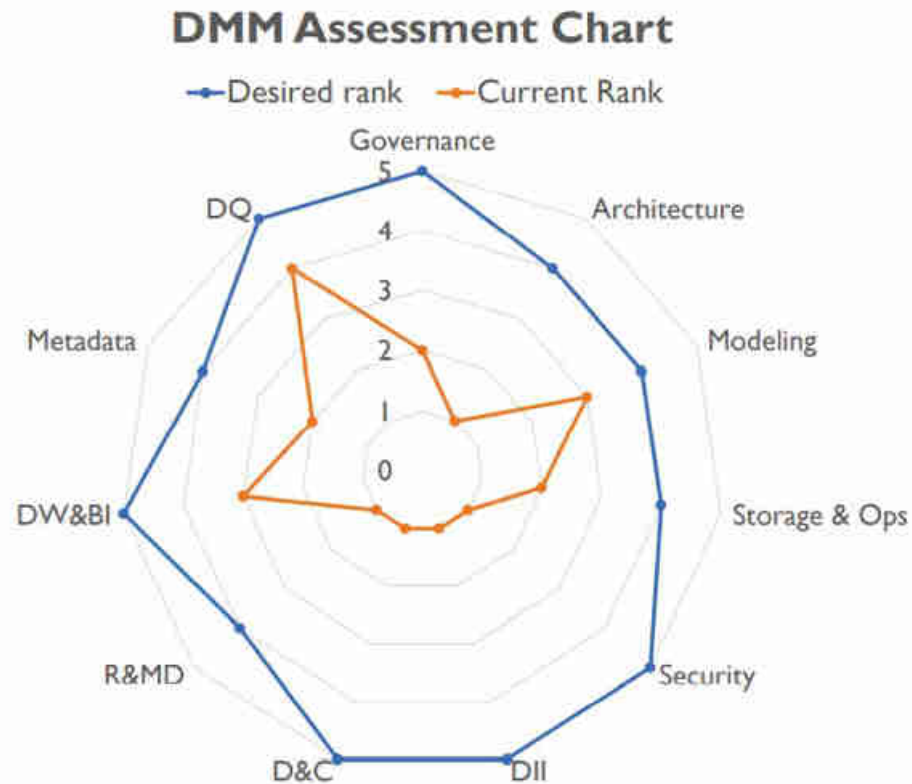
Source: DMBOK

Other alternatives ,

- I. CMMI-DMM
- II. EDM Council DCAM,
- III. IBM Data Governance Council Maturity Model,
- IV. Stanford Data Governance Maturity Model

Data Governance Implementation – Step 2a

2a. Perform discovery and Business alignment, then Identify desired rank, goals



Assess the model based on four categories, in the defined capabilities.

- I. Activity
- II. Tools
- III. Standards
- IV. People and Resources

For each of the capabilities, the outer ring displays the level of capability the organization wants to achieve, and the inner ring displays the current standing. Distance between the two ring at its widest represents the greatest risk to the organization and should be focused first.

Source: DMBOK

Data Governance Implementation – Step 2b

2b. Anticipate the effect of governance effort on the 4 P's

- I. Programs
- II. Projects
- III. Professional Discipline
- IV. People

Focus on SMART Metrics : Specific, Measurable, Actionable, Relevant, and Timely.

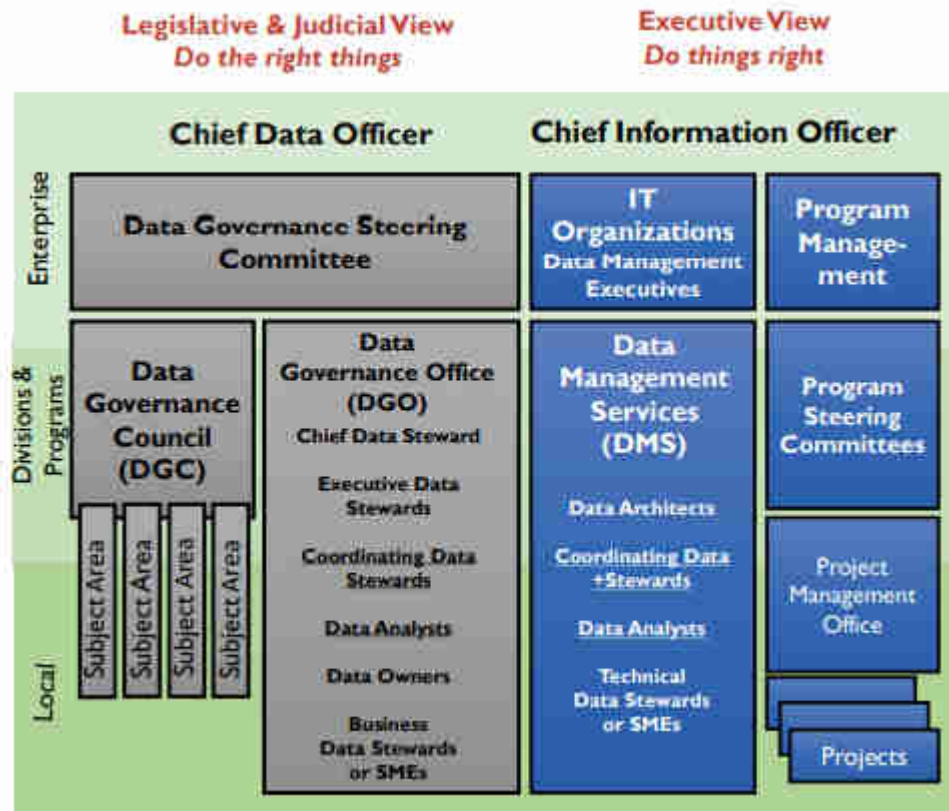


Best Practice

Bring discipline to your program by translating goals to formal value statements.

Data Governance Implementation – Step 3a

3a. Define Accountability & Control



- Who gets to make the decision, and when, and using what process?
- It is the responsibility of the Data Governance program to facilitate (and to sometimes document and store) the collection of decision rights that are the “metadata” of data-related decisions.
- Decision rights for compliance-based programs.
- With the proliferation of sensitive data breaches – and the consequences for those who were entrusted with the data. How do we deal with risk?.
- Controls must be Preventative, Detective, Corrective

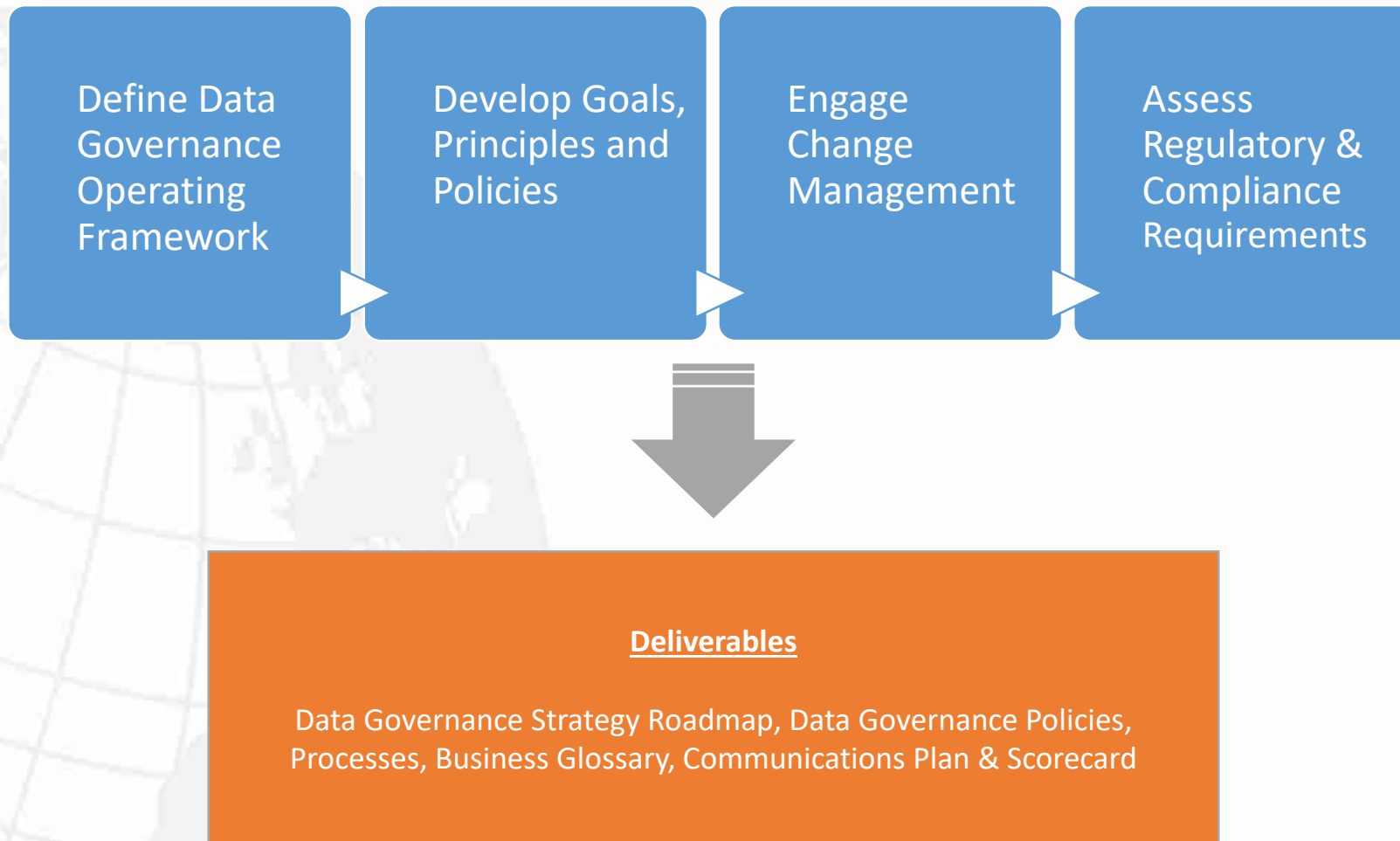
Best Practice

Consider implementing a Data Governance Board made up of executive-level stakeholders.

Source: DMBOK

Data Governance Implementation – Step 3b

3b. Define Data Governance Strategy



Data Governance Implementation – Step 4

4. Define Data Rules & Definitions



This component refers to data-related policies, standards, design, architecture and so forth. Depending on your focus areas, your program may work to

- Create new rules/definitions
- Gather existing rules/definitions
- Address gaps and overlaps
- Align and prioritize conflicting rules/definitions
- Establish or formalize rules for when certain definitions apply.

Deliverables

Data Architecture Design, Data Flows, Data Value Chains, Enterprise Data Model, Data Lifecycle

Data Governance Framework – Step 5

5. Measure Success

Metrics that reinforce the Data Governance need to be validated in terms of

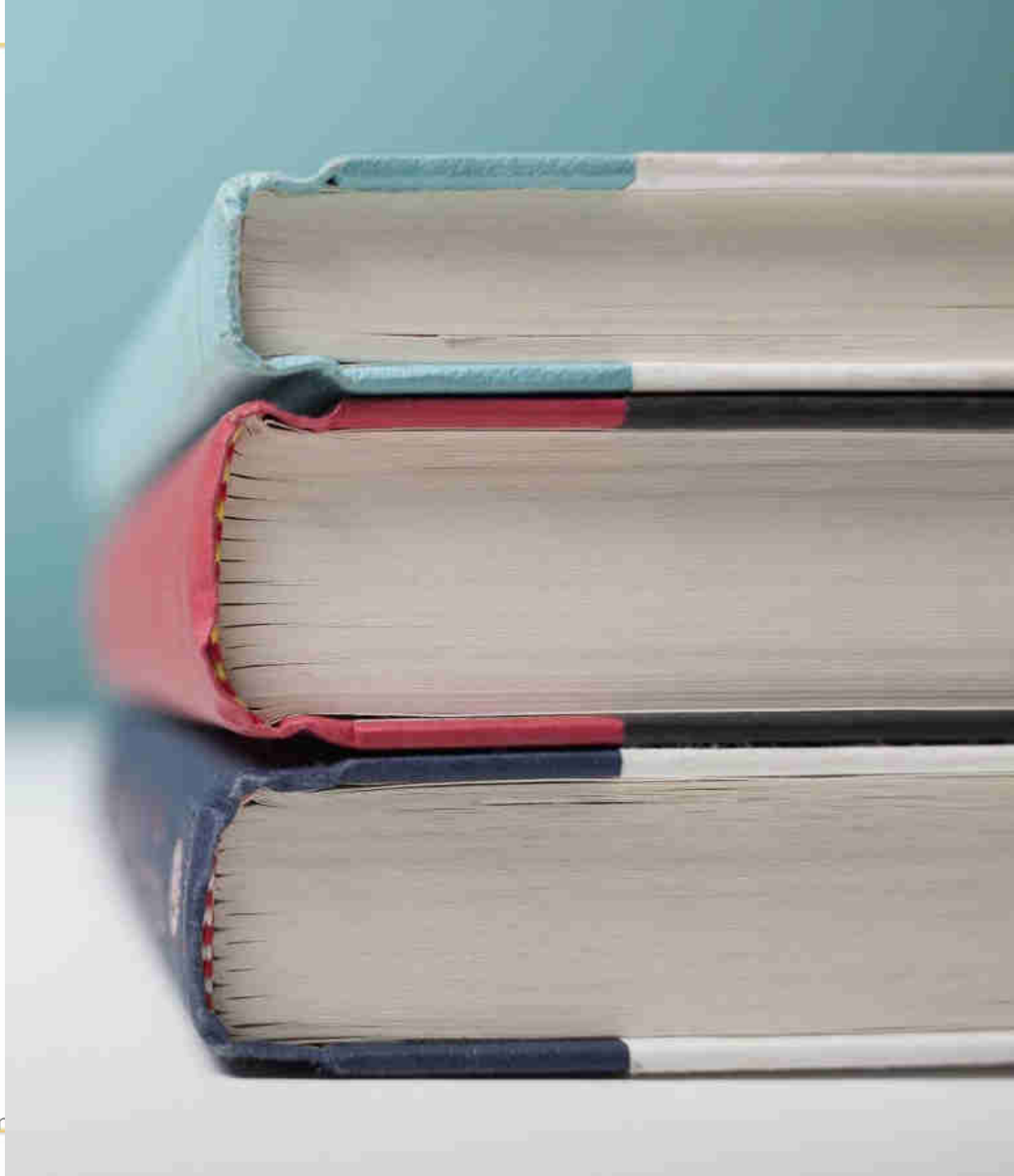
- Value
 - Contributions to the business objective
 - Reduction of Risk
 - Improved efficiency
- Effectiveness
 - Achievements of goals and objective
 - Extent of stewards using the relevant tool
 - Effectiveness of education/training
- Sustainability
 - Performance of policies and processes
 - Conformance of standards and procedures



Thank You!



Usha Balasundaram, DBA
Head of Data Governance || Successful
Data Governance Practitioner || Special...





GLOBAL CONFERENCE 2025

ENTERPRISE RISK MANAGEMENT:
RISING FROM THE ASHES

THANK YOU

-  InstituteOfEnterpriseRiskPractitioners
-  institute-of-enterprise-risk-practitioners
-  ierp_official