MANNHEIM
BUSINESS SCHOOL

MANAGING BIG DATA

PROF. DR. FLORIAN STAHL

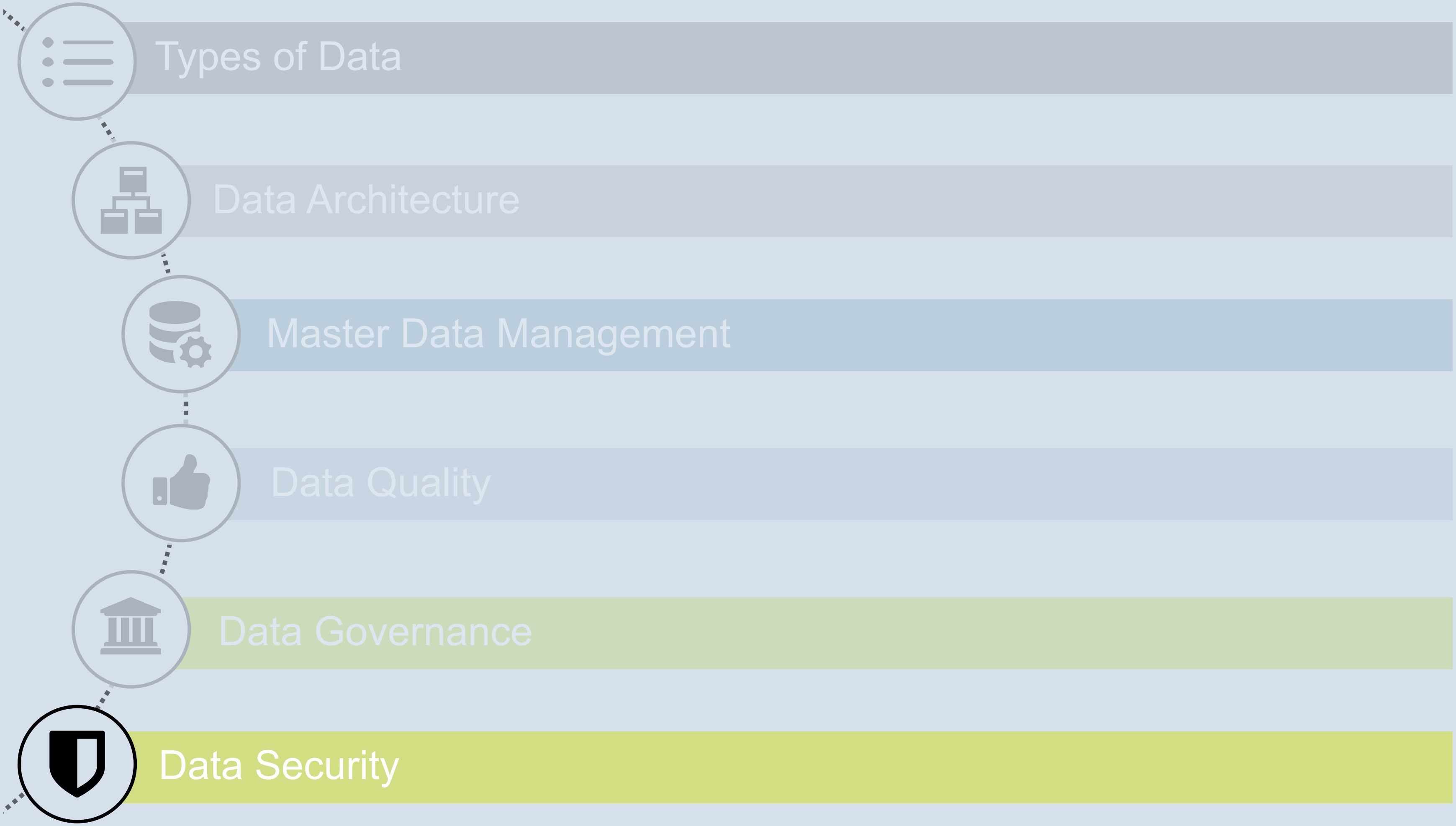
UNIVERSITY OF MANNHEIM

AACSB ACCREDITED

EQUIS ACCREDITED

ASSOCIATION OF MBAS ACCREDITED

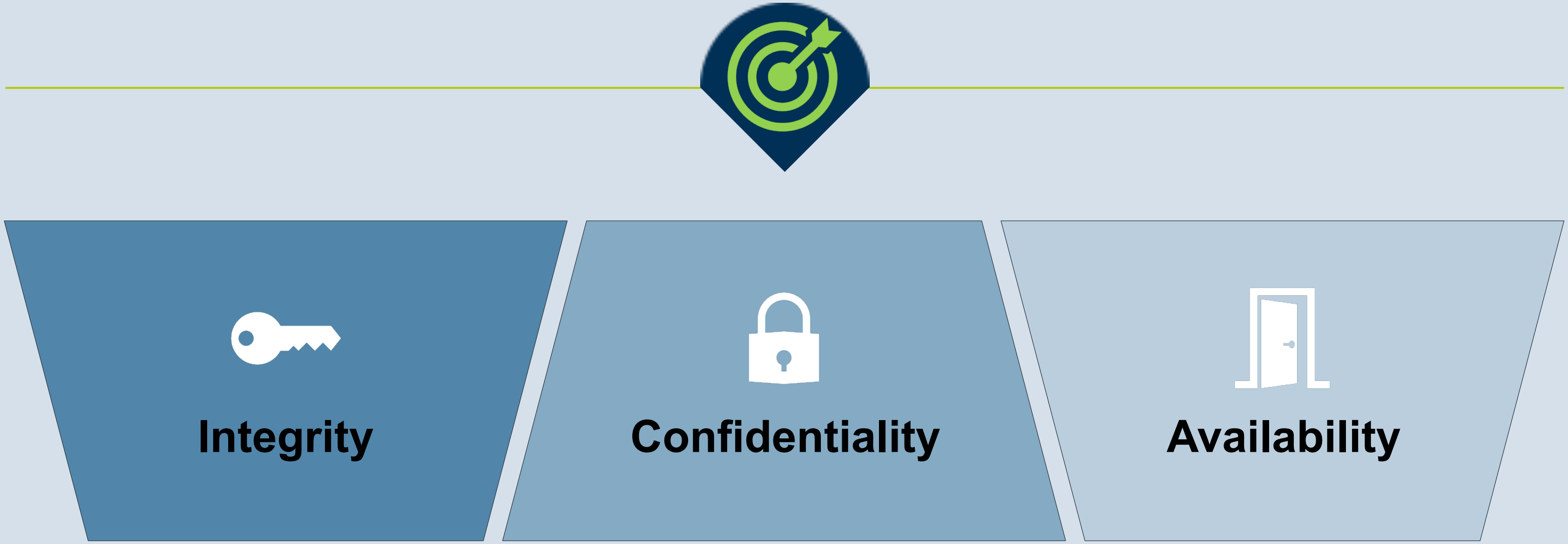
Managing Big Data



- Types of Data
- Data Architecture
- Master Data Management
- Data Quality
- Data Governance
- **Data Security**

What is Data Security?

Data security is one part of an organization’s overall data strategy and is about protecting information. It is often described as getting the right information to the right people at the right time.



Integrity

Confidentiality

Availability

Security Objectives

Integrity

Guarding against **improper information modification** or destruction, and includes ensuring information nonrepudiation and authenticity

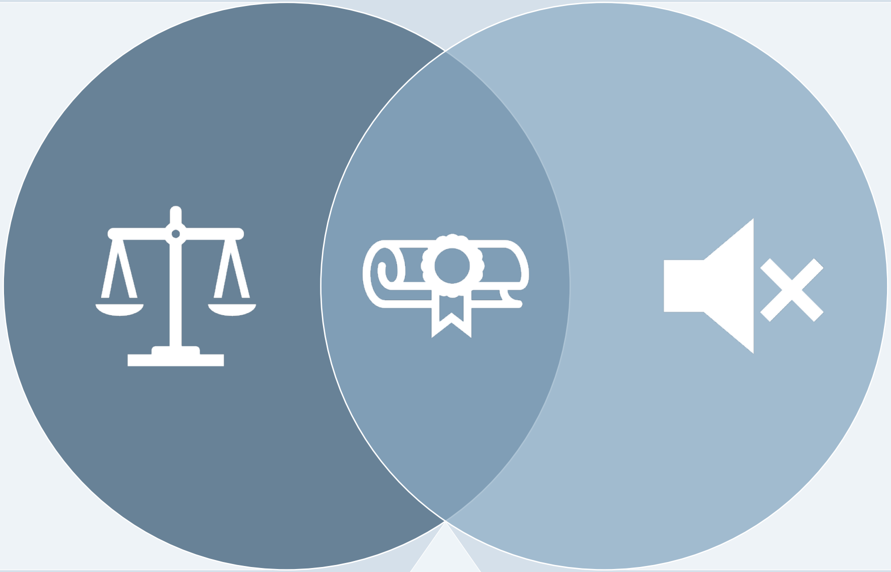
Confidentiality

Preserving authorized **restrictions on access** and **disclosure**, including means for protecting personal privacy and proprietary information

Availability

Ensuring **timely and reliable access** to and use of information

Private Data Security

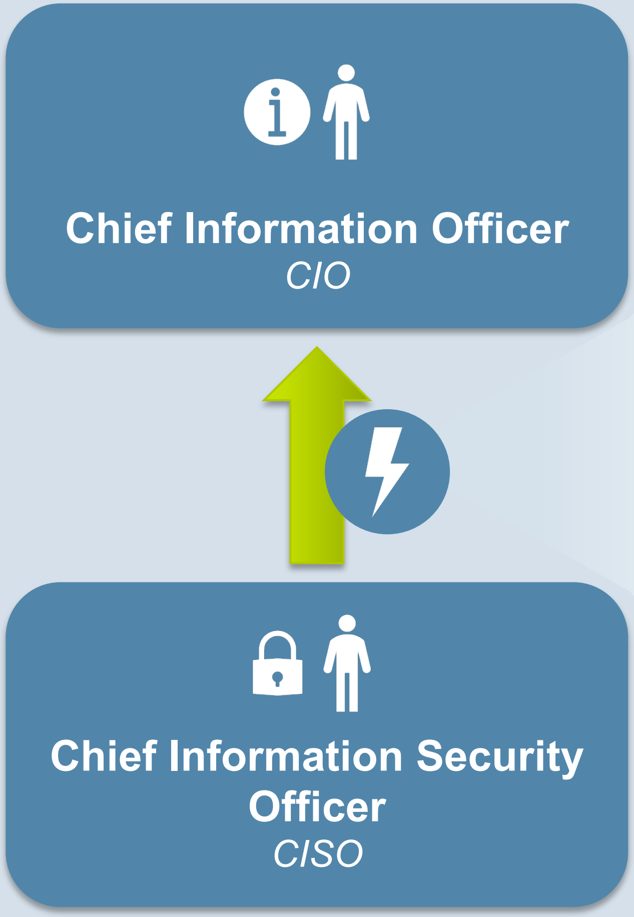


Broad data security **laws**, **regulations** and **standards**

Sound security practices

Industries that tend to deal with **highly sensitive personal information** (e.g., financial or healthcare sectors)

Who is Data Security?

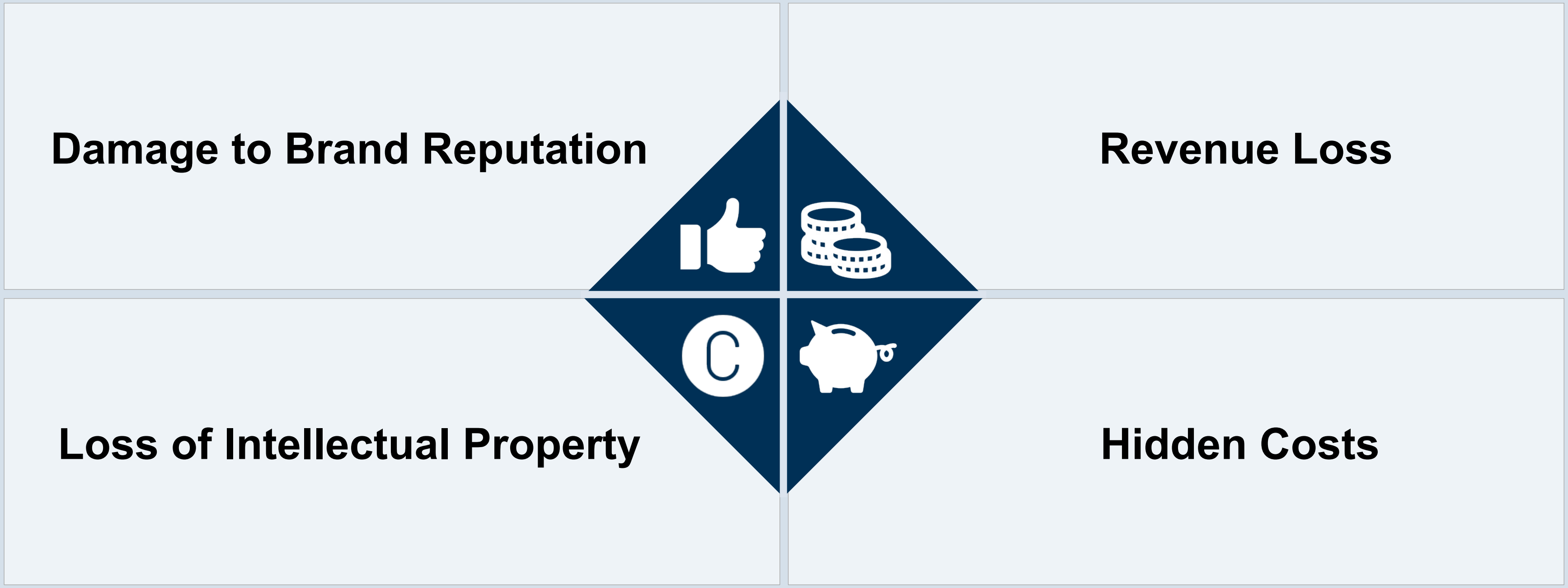


Chief Information Officer
CIO

Chief Information Security Officer
CISO

- CIO may **insulate executive leadership from data security perspectives** and concerns
- CISO may be **excluded** from direct participation in **cross-functional enterprise risk teams** and must rely on the CIO
- Security may be considered a **part of the information technology trade-space**

Consequences of Poor Data Security



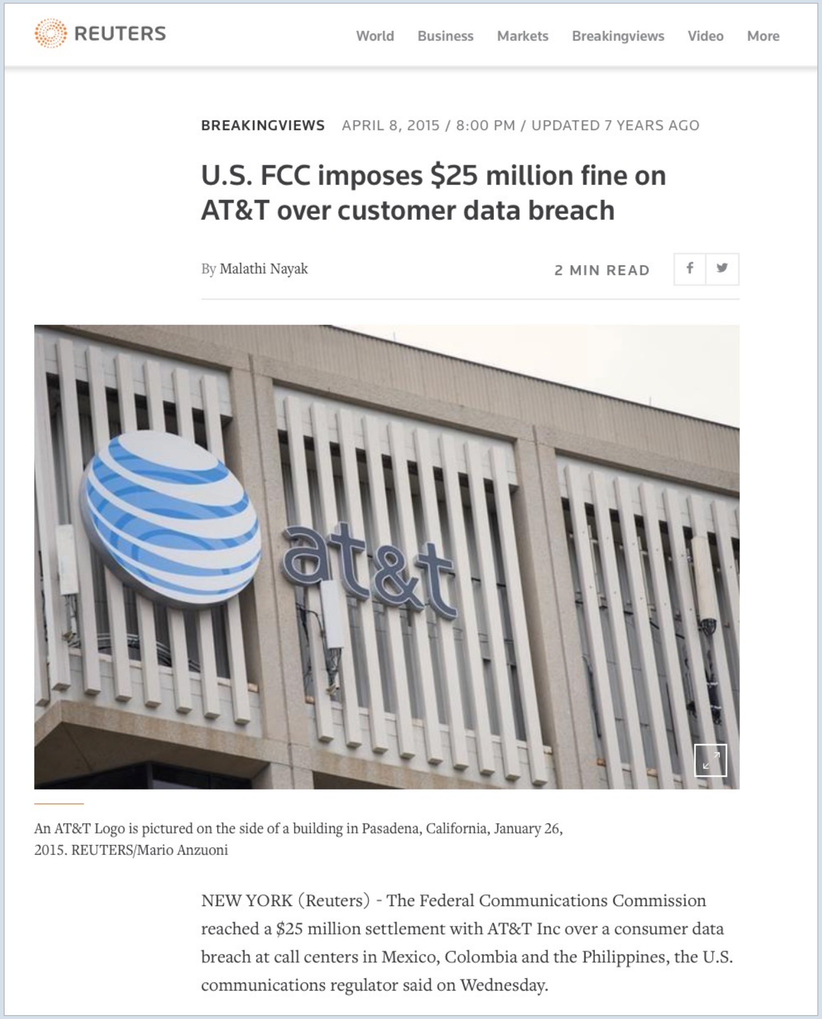
Damage to Brand Reputation

Revenue Loss

Loss of Intellectual Property

Hidden Costs

Consequences of Poor Data Security



BREAKINGVIEWS APRIL 8, 2015 / 8:00 PM / UPDATED 7 YEARS AGO

U.S. FCC imposes $25 million fine on AT&T over customer data breach

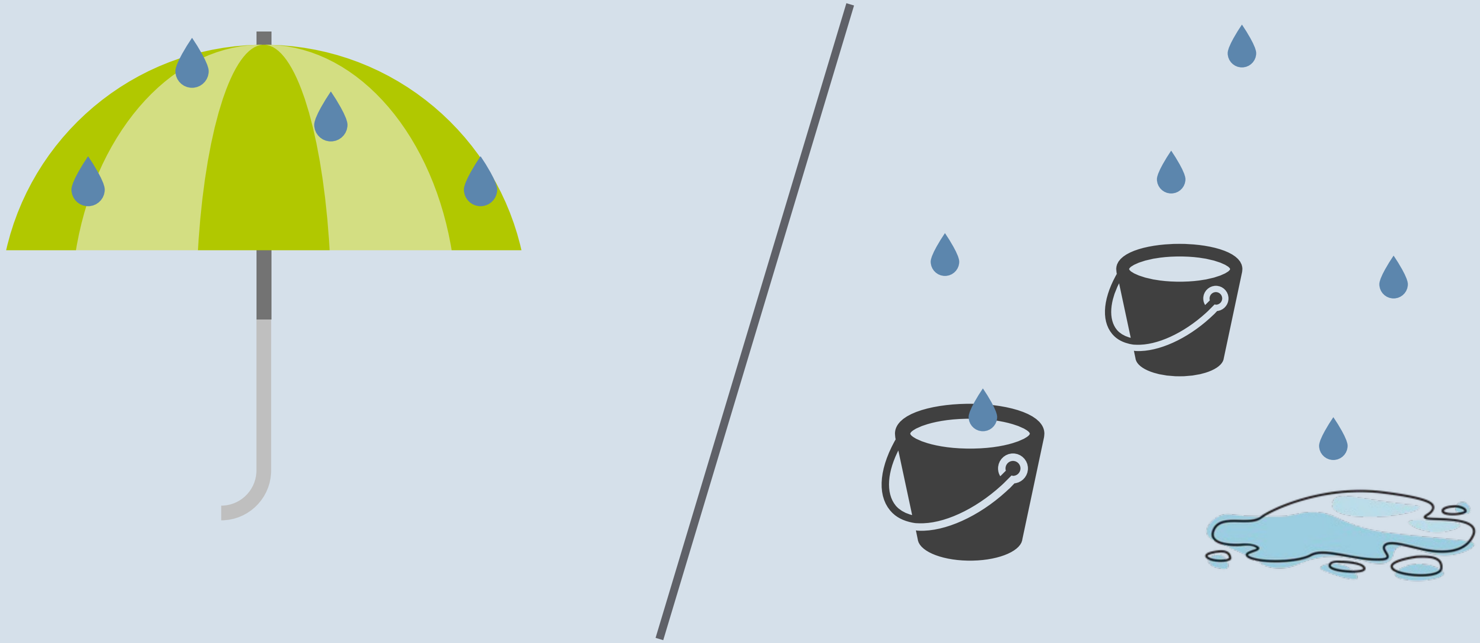
By Malathi Nayak

2 MIN READ

An AT&T Logo is pictured on the side of a building in Pasadena, California, January 26, 2015. REUTERS/Mario Anzuoni

NEW YORK (Reuters) - The Federal Communications Commission reached a $25 million settlement with AT&T Inc over a consumer data breach at call centers in Mexico, Colombia and the Philippines, the U.S. communications regulator said on Wednesday.

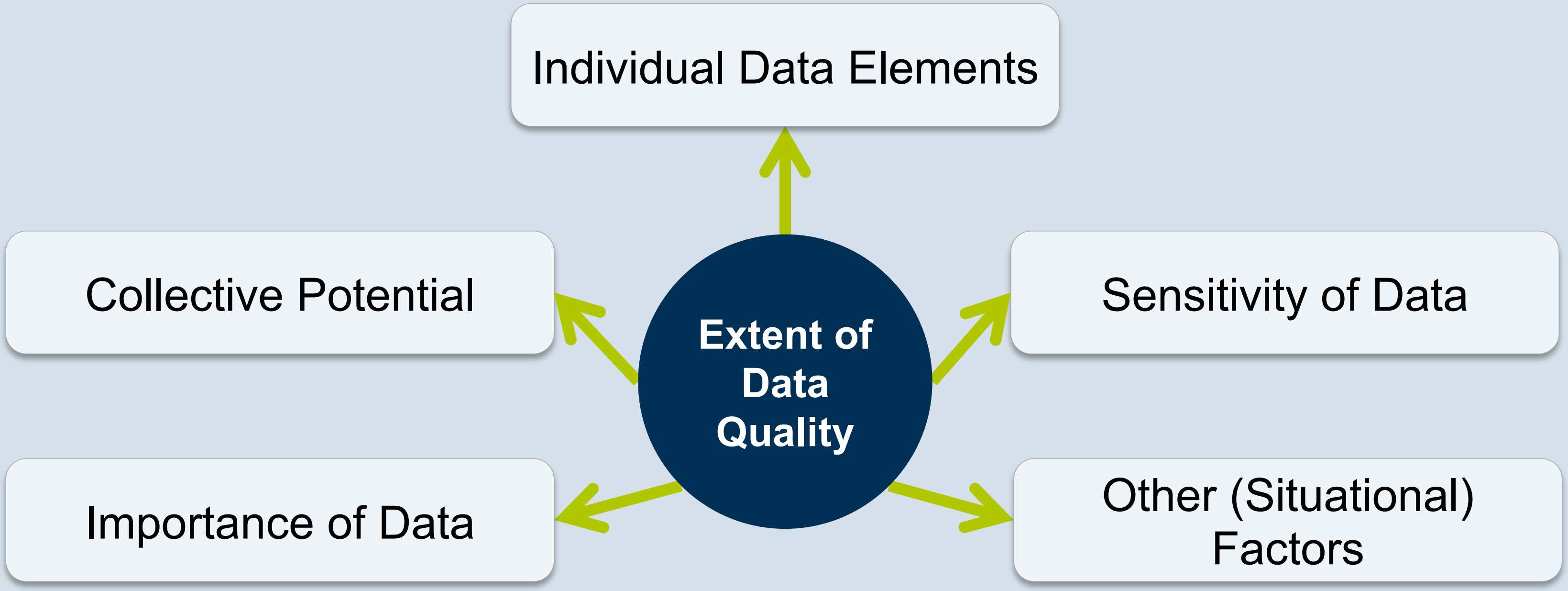
Data Security is a Process of Risk Management rather than a System of Risk Mitigation



Risk Mitigation

Risk Management

Assessing the Need for Data Security



Extent of Data Quality

Individual Data Elements

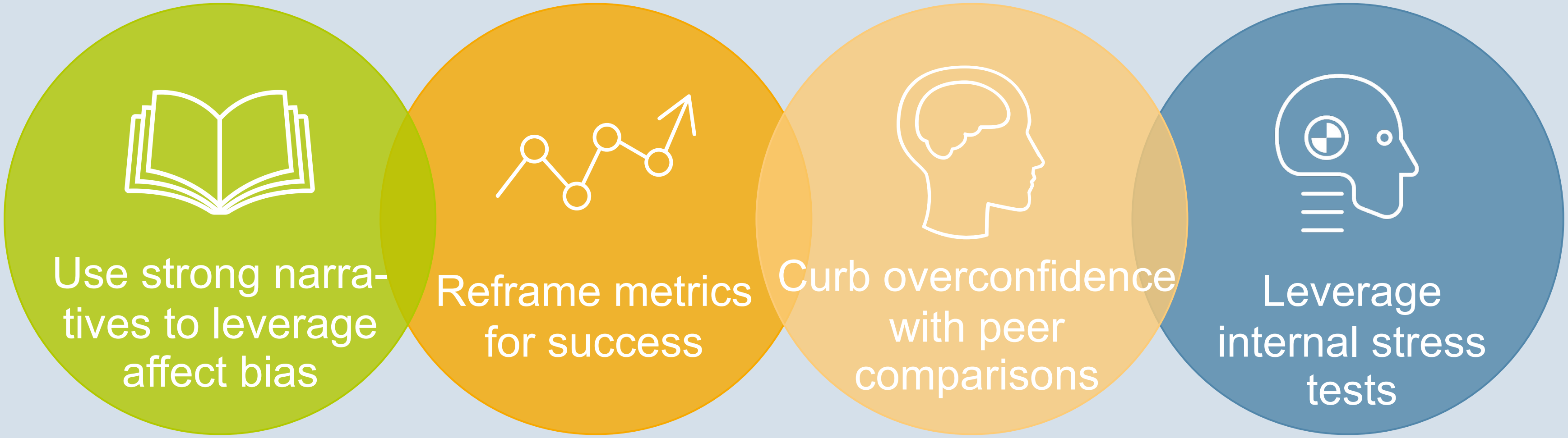
Collective Potential

Sensitivity of Data

Importance of Data

Other (Situational) Factors

How Establish Data Security on Executives‘ Agenda and Drive Investments



Use strong narratives to leverage affect bias

Reframe metrics for success

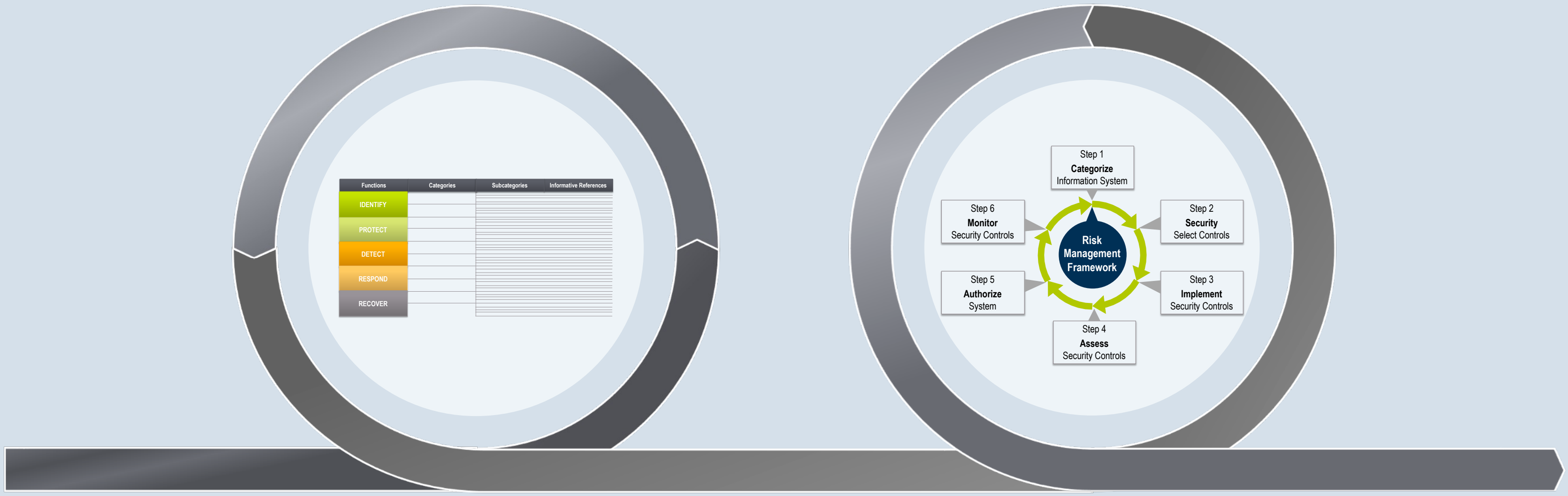
Curb overconfidence with peer comparisons

Leverage internal stress tests

Implementing Data Security

Cybersecurity Framework

Risk Management Framework

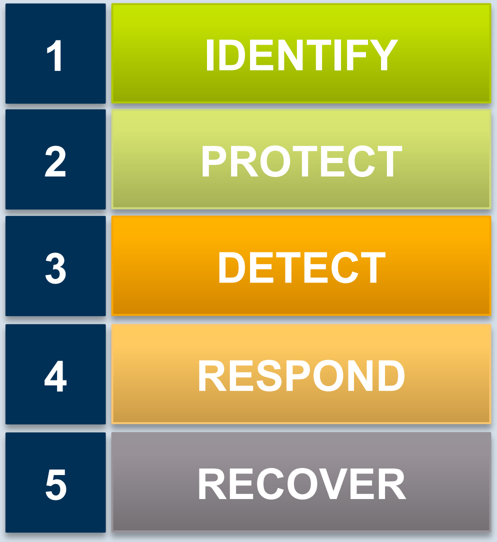


Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

The Cybersecurity Framework

!

The **Cybersecurity Framework** discusses data security programs in clear, simple terms, making it consumable by almost anyone.
It defines **five key ongoing functions** for protecting assets, including information.



1 IDENTIFY

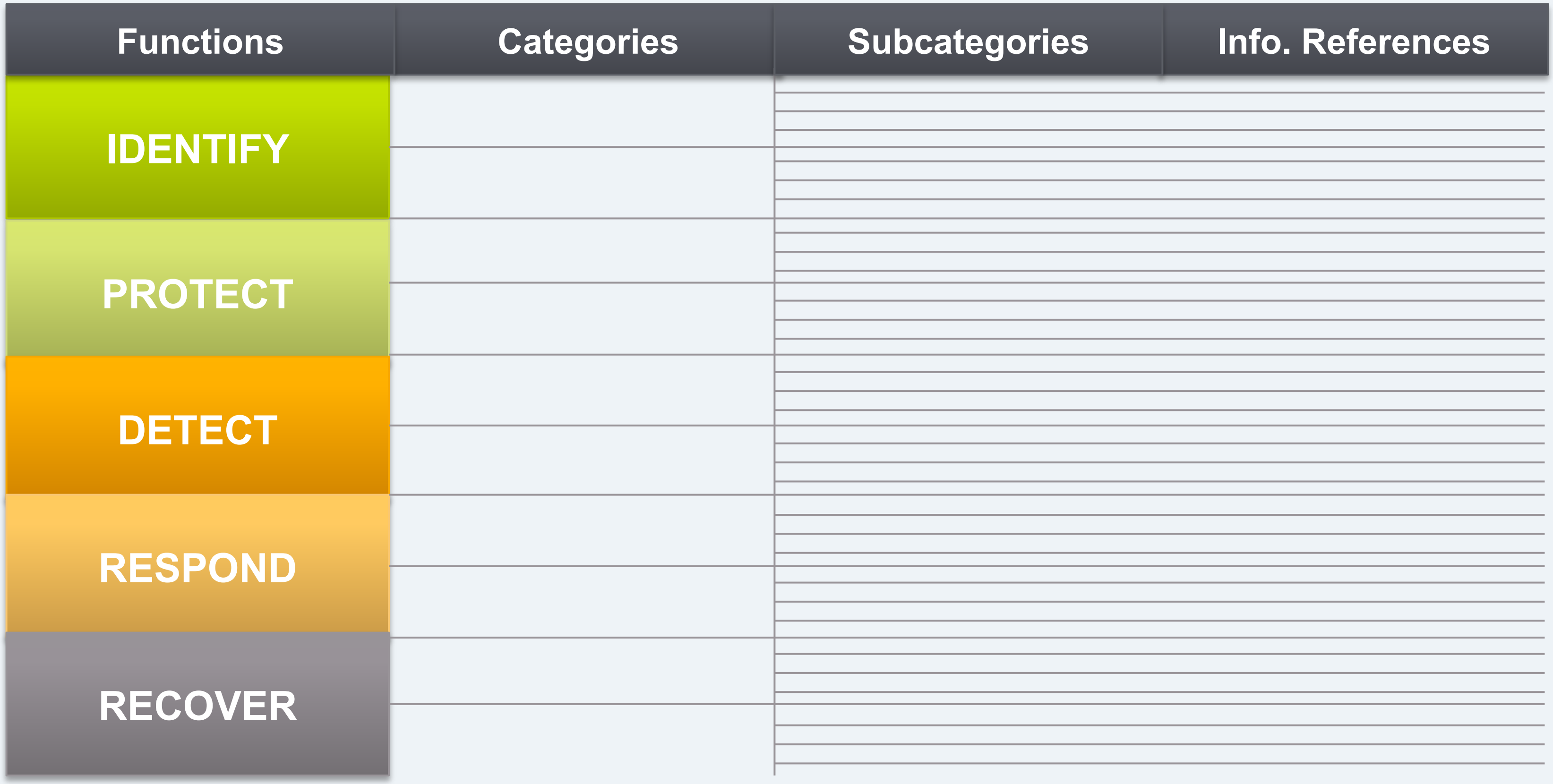
2 PROTECT

3 DETECT

4 RESPOND

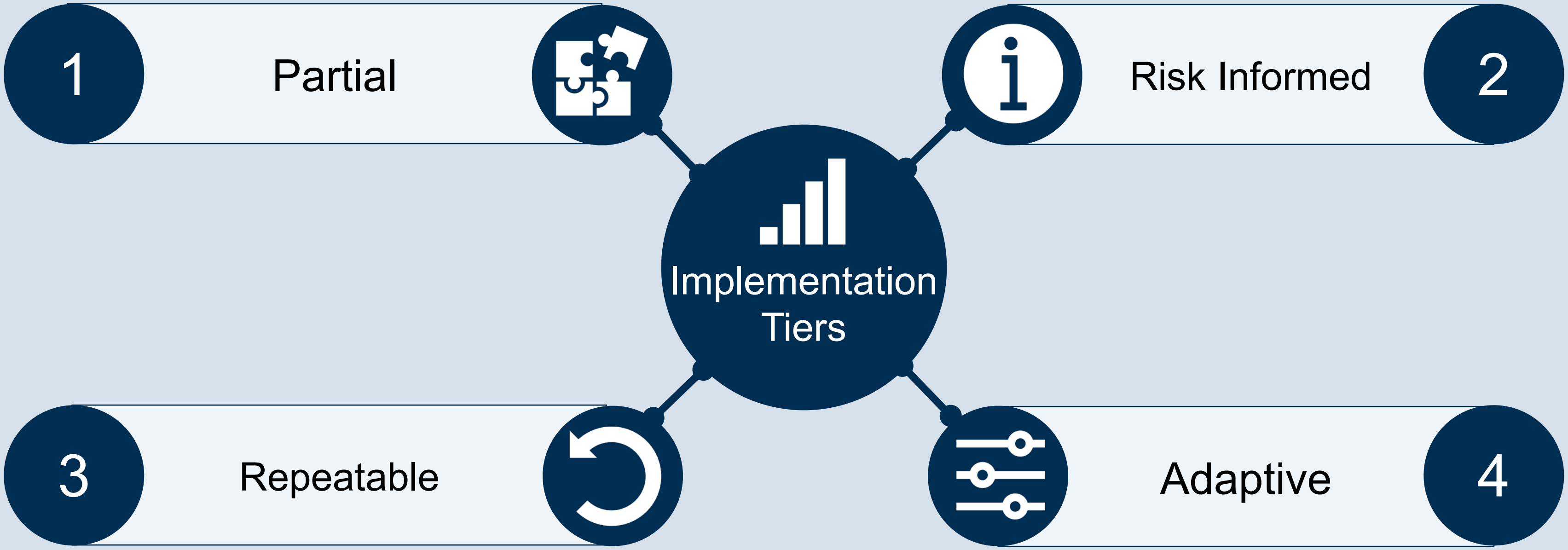
5 RECOVER

Cybersecurity Framework Core Structure

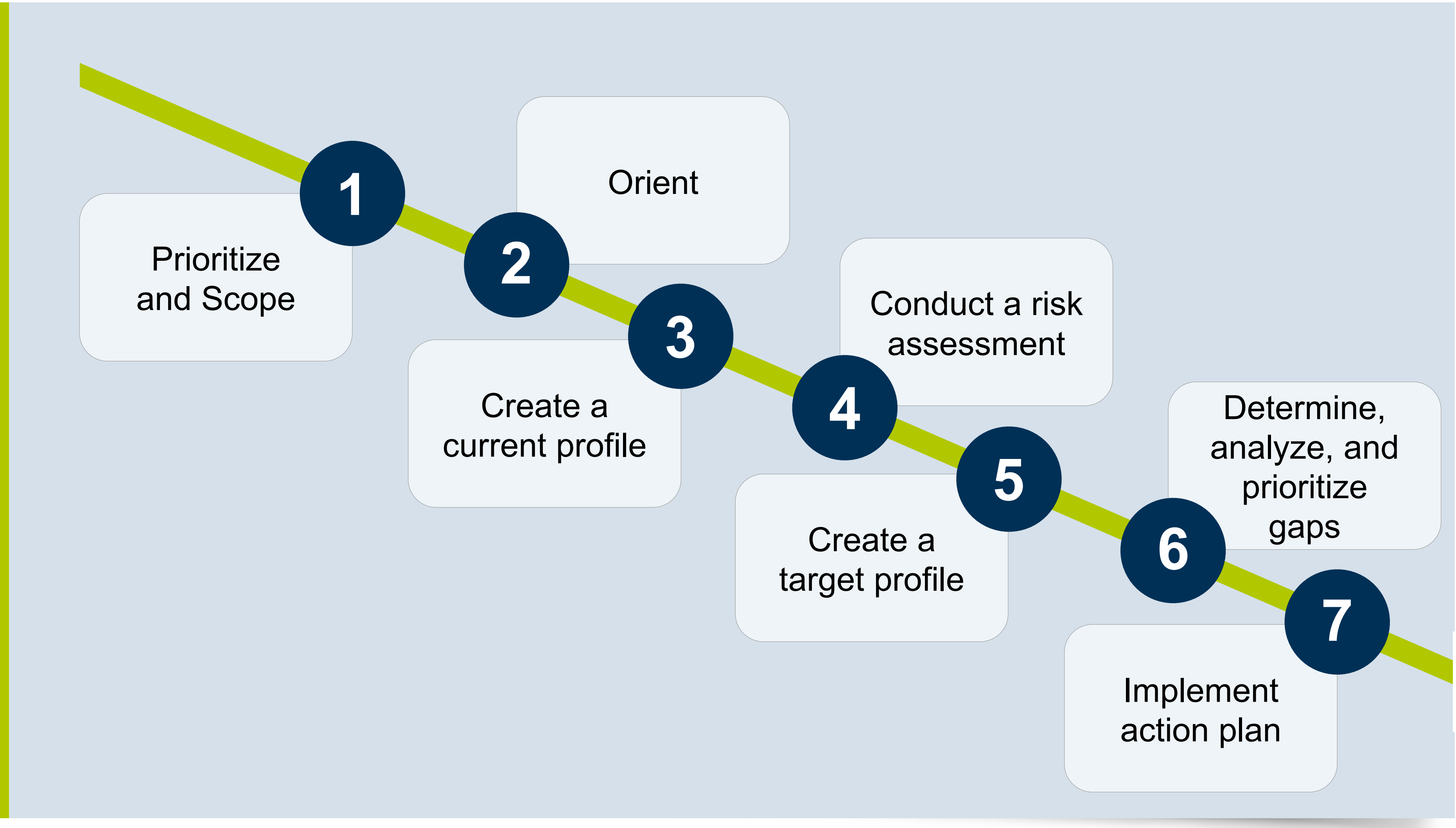


Functions	Categories	Subcategories	Info. References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Cybersecurity Framework Core Structure



Cybersecurity Framework Execution



1 Prioritize and Scope

2 Orient

3 Create a current profile

4 Conduct a risk assessment

5 Create a target profile

6 Determine, analyze, and prioritize gaps

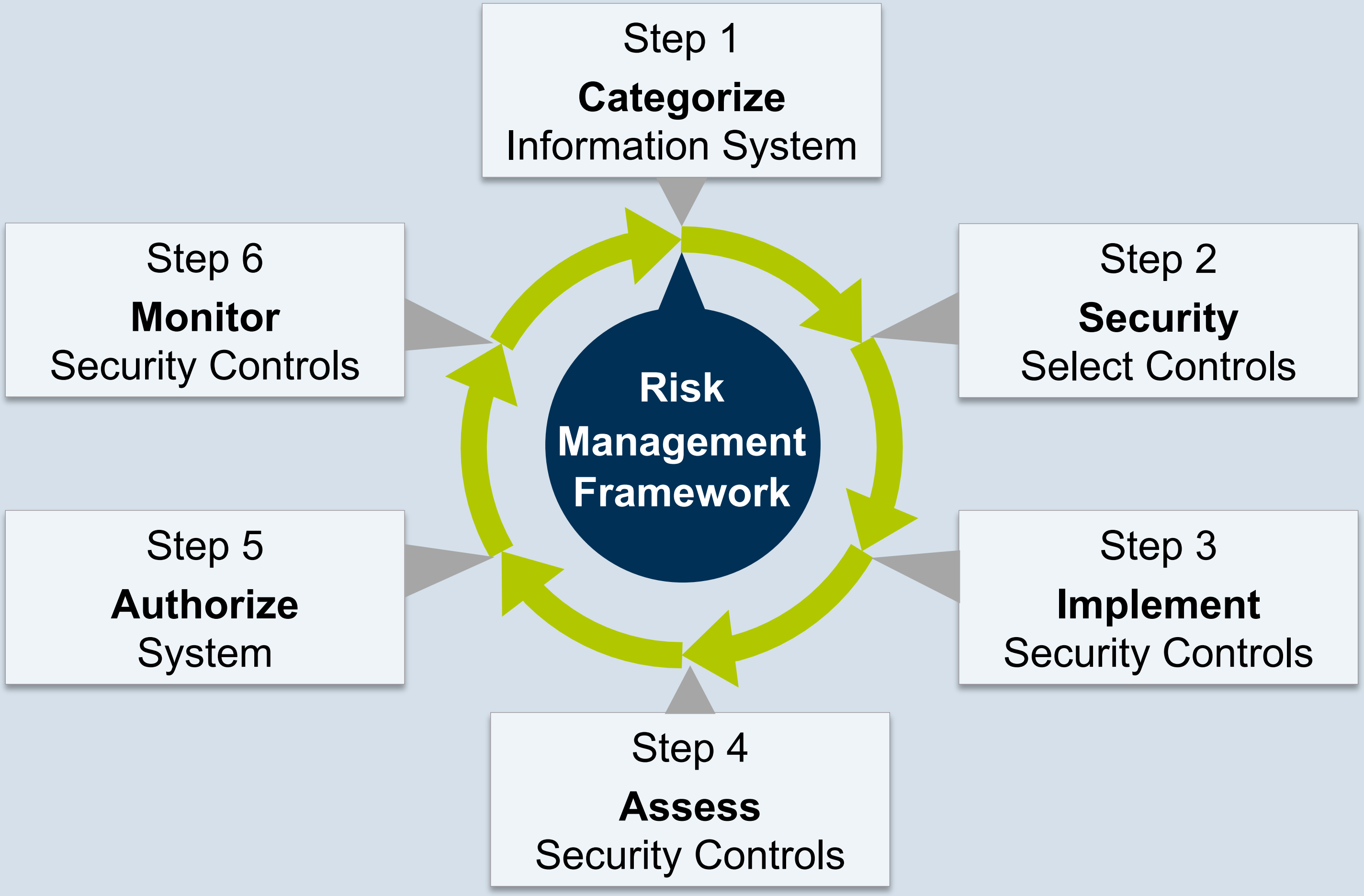
7 Implement action plan

Cybersecurity Framework Case Study - UMass Memorial Health Care

> As a leading healthcare institution, we align with industry-recognized frameworks and needed a solution that would simplify and scale our compliance and risk management initiatives, while also giving insights on these efforts from a risk perspective.
>
> \- Bruce Forman, CISO

UMass Memorial Health

The Risk Management Framework (RMF)



Step 1
Categorize
Information System

Step 2
Security
Select Controls

Step 3
Implement
Security Controls

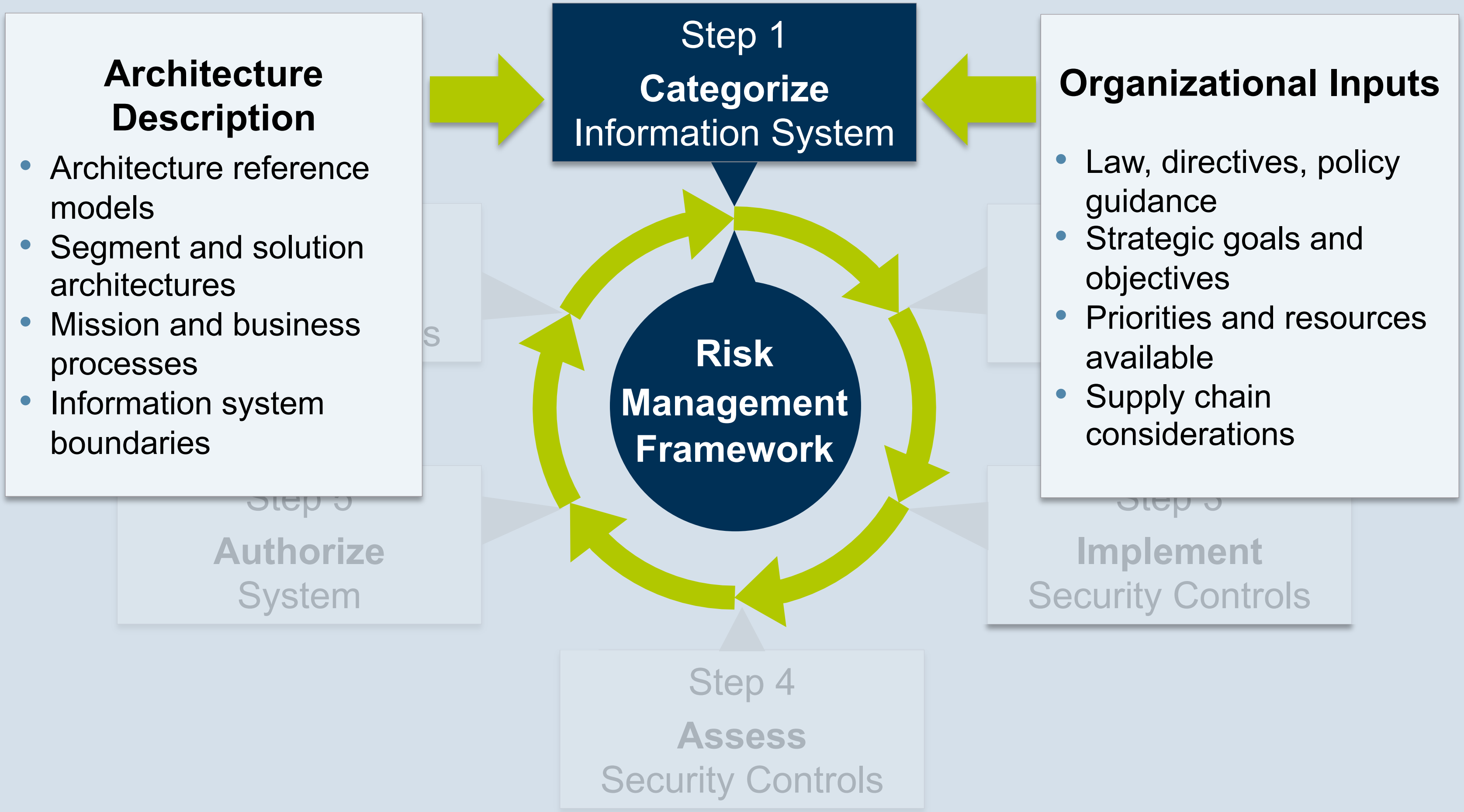
Step 4
Assess
Security Controls

Step 5
Authorize
System

Step 6
Monitor
Security Controls

Risk Management Framework

The Risk Management Framework (RMF)



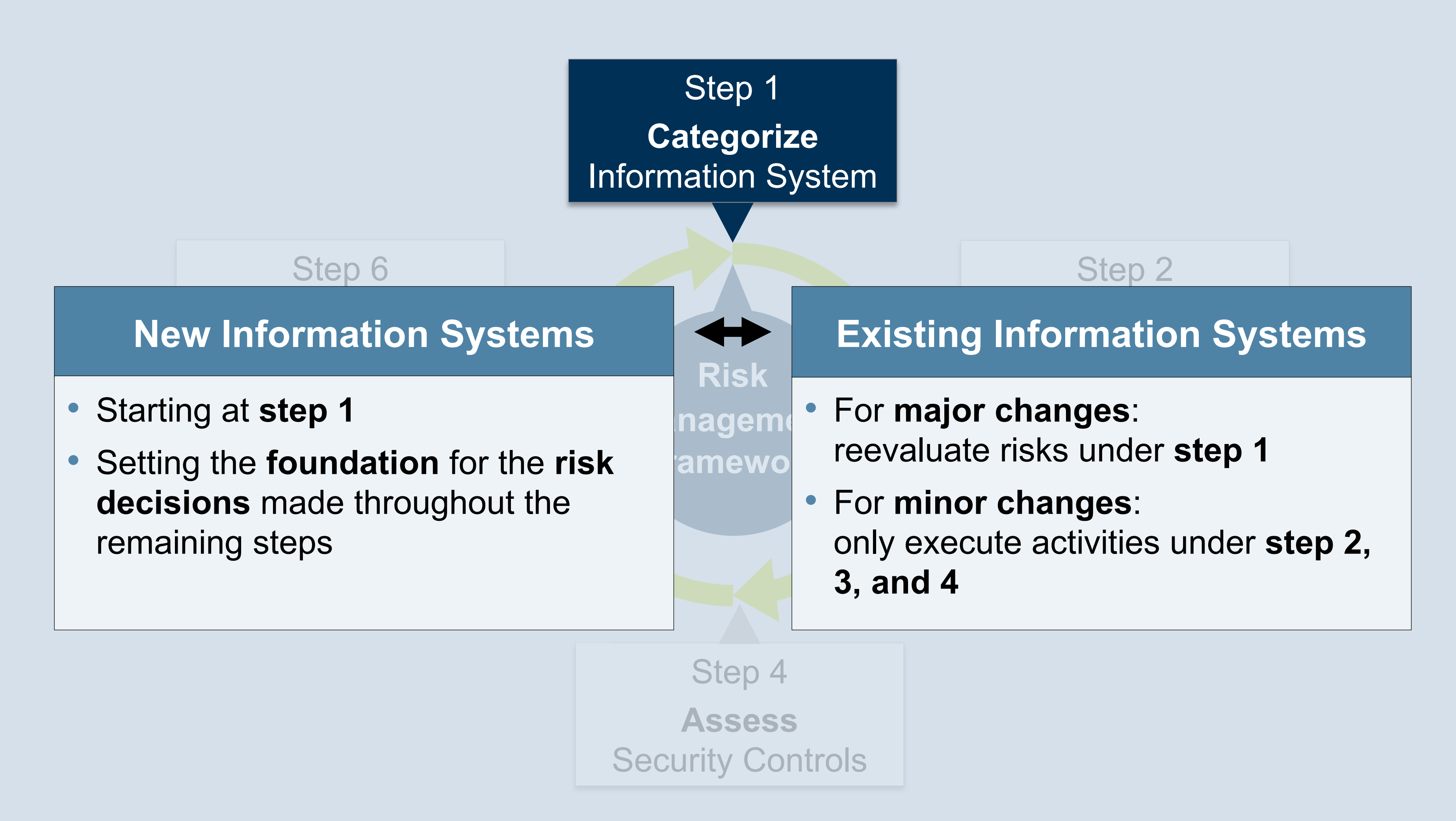
Architecture Description

- Architecture reference models
- Segment and solution architectures
- Mission and business processes
- Information system boundaries

Organizational Inputs

- Law, directives, policy guidance
- Strategic goals and objectives
- Priorities and resources available
- Supply chain considerations

New vs. Existing Information Systems in RMF



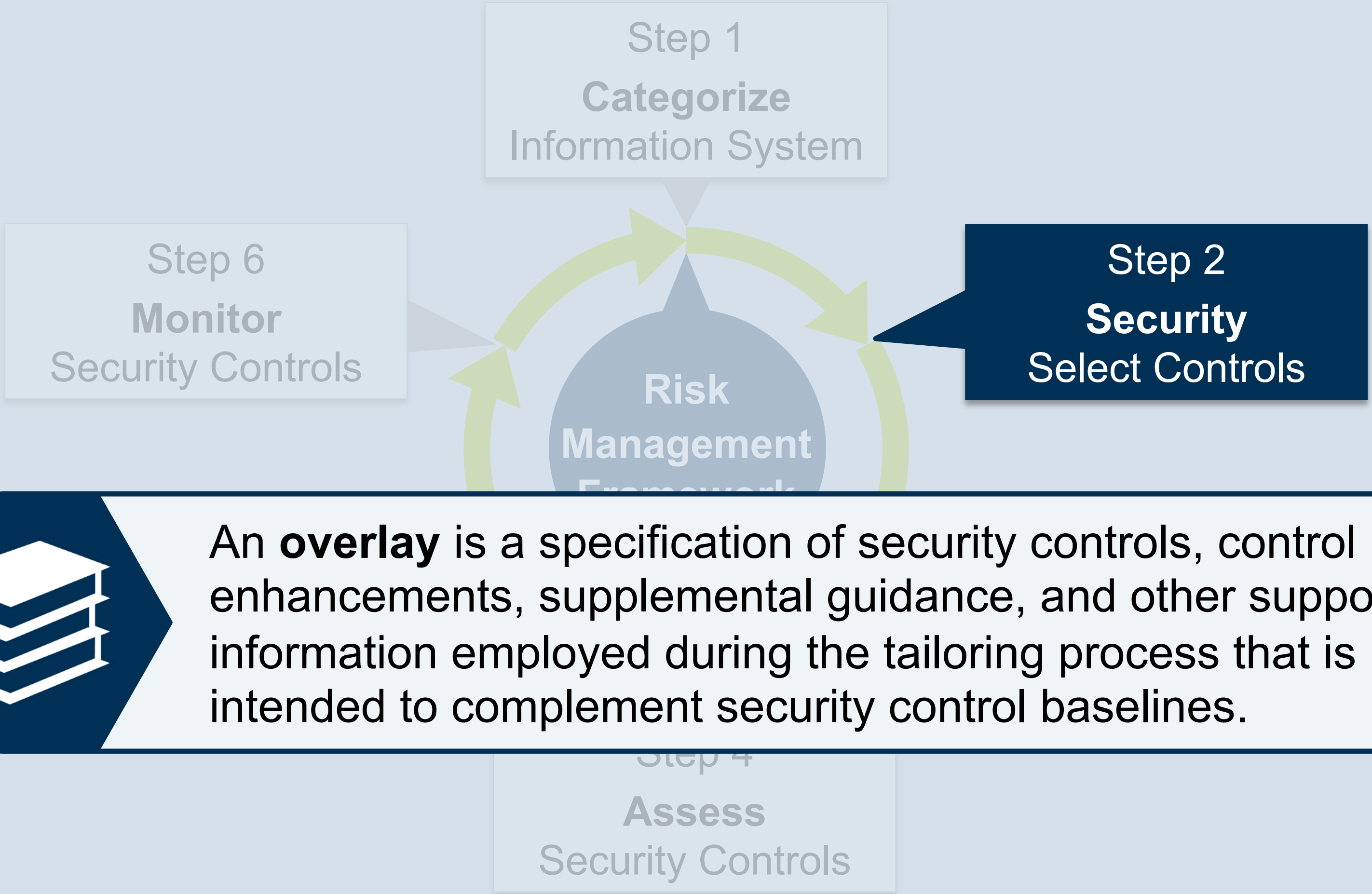
New Information Systems

- Starting at **step 1**
- Setting the **foundation** for the **risk decisions** made throughout the remaining steps

Existing Information Systems

- For **major changes**: reevaluate risks under **step 1**
- For **minor changes**: only execute activities under **step 2, 3, and 4**

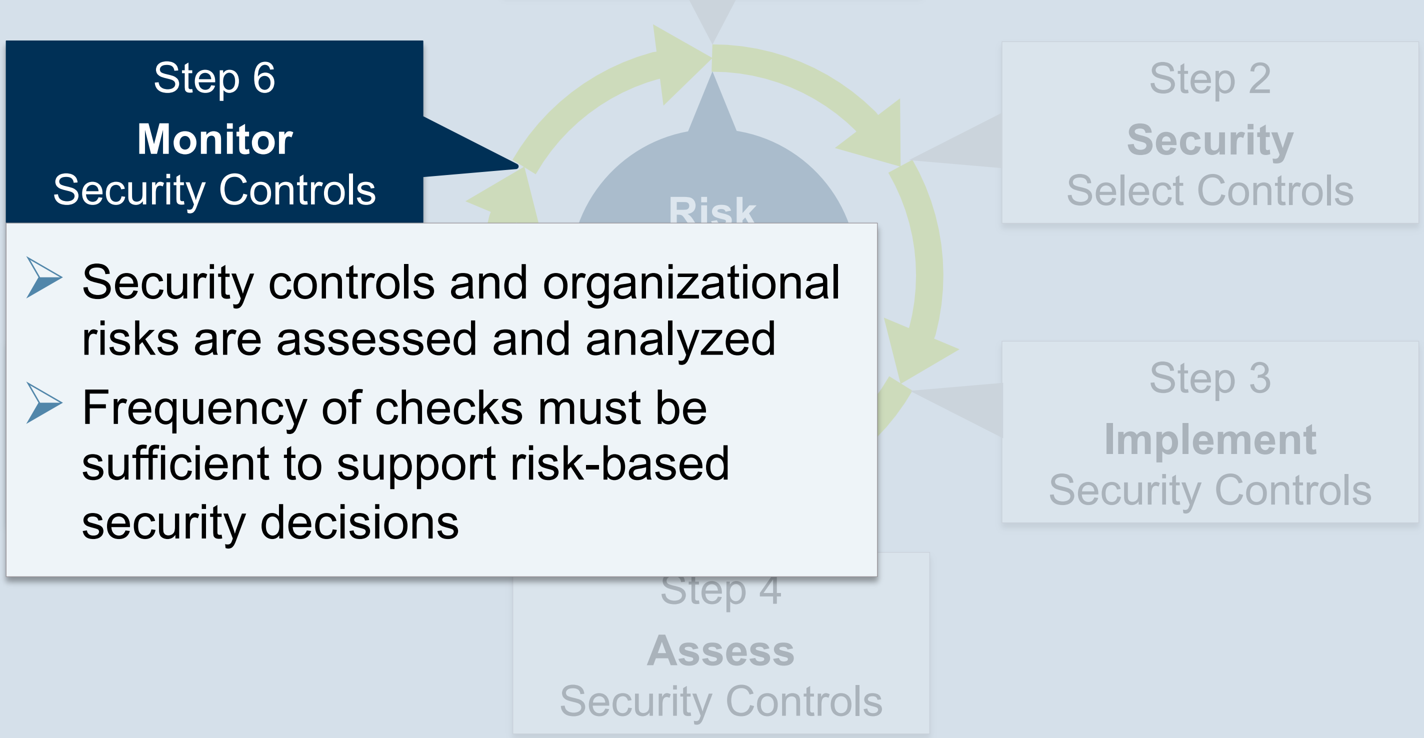
RMF Step 2 – Application of overlays



An **overlay** is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process that is intended to complement security control baselines.

RMF Step 6 – Continuity in Monitoring

Data security continuous monitoring means maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.



Step 6
Monitor
Security Controls

- Security controls and organizational risks are assessed and analyzed
- Frequency of checks must be sufficient to support risk-based security decisions

Purpose of Data Security Guidelines

More consistent **approach** for **selecting/specifying security controls** for information systems/organizations

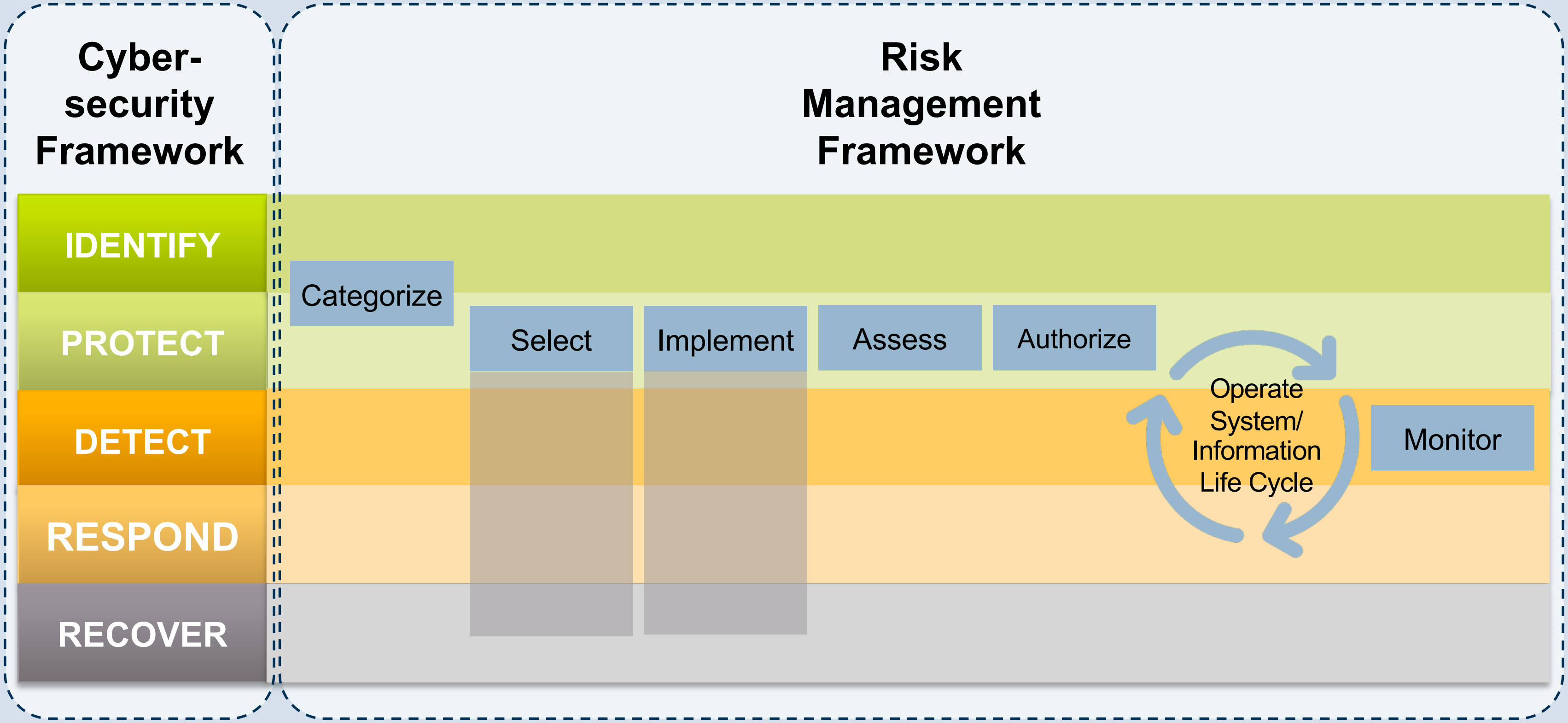
Stable, flexible catalog of **security controls**

Provision of a **common lexicon** for risk and management concepts to improve **communication** among organizations

Recommendation for security controls for information systems

Creation of a foundation for the development of **assessment methods** and procedures for determining security control effectiveness

Cybersecurity Framework vs. Risk Management Framework (RMF)



Steps to Create a Common Language Around Cyber Security in Business

Bring together C-level management

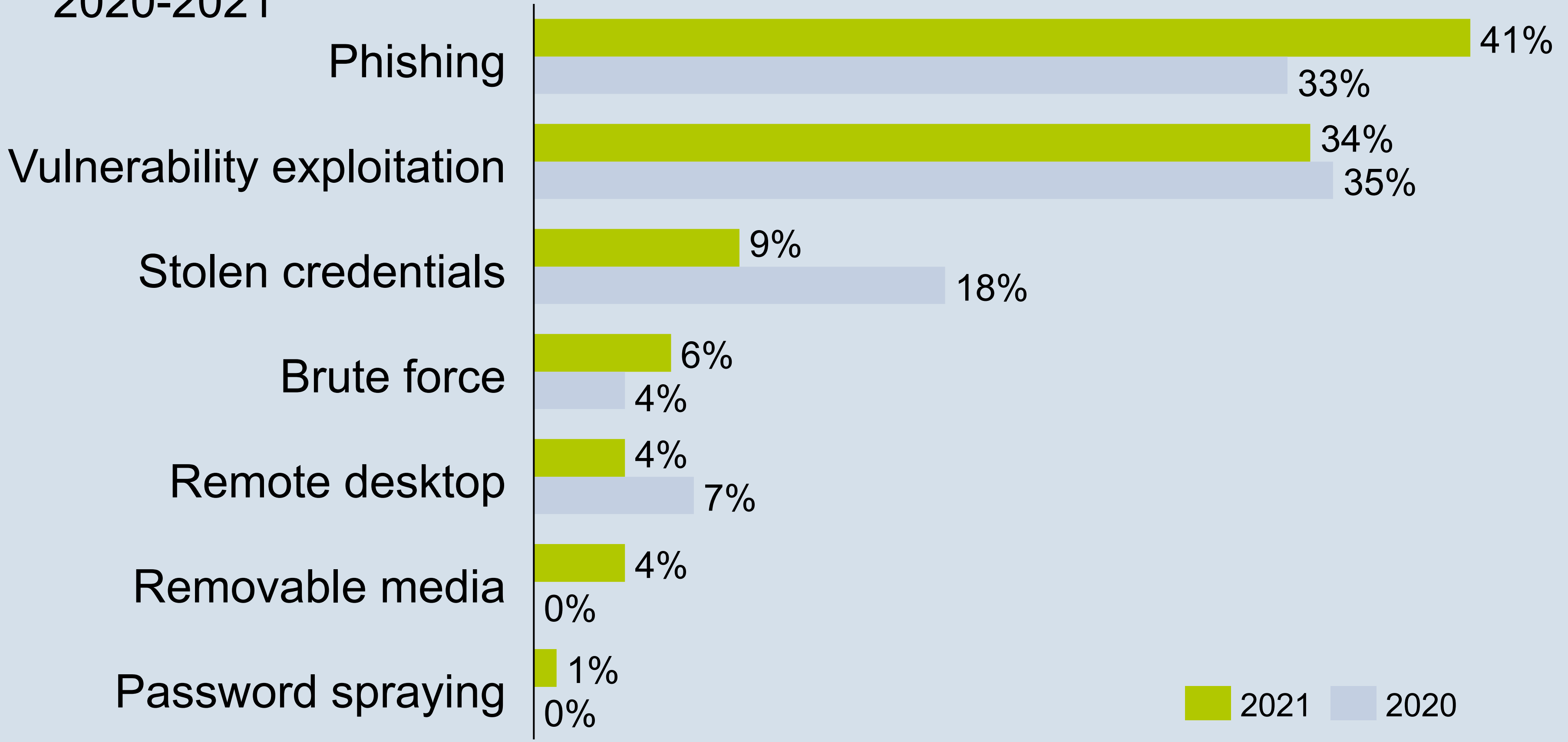
Create a culture of open dialog

Establish an incidence-response plan

Audit for readiness

End Users are the Weakest Link in Cyber Security

Top infection vectors observed by IBM Security‘s X-Force Incident Response, 2020-2021



Addressing Behavioral Risks in Cyber Security – Tactical and Strategic Steps

Adopt tactical steps

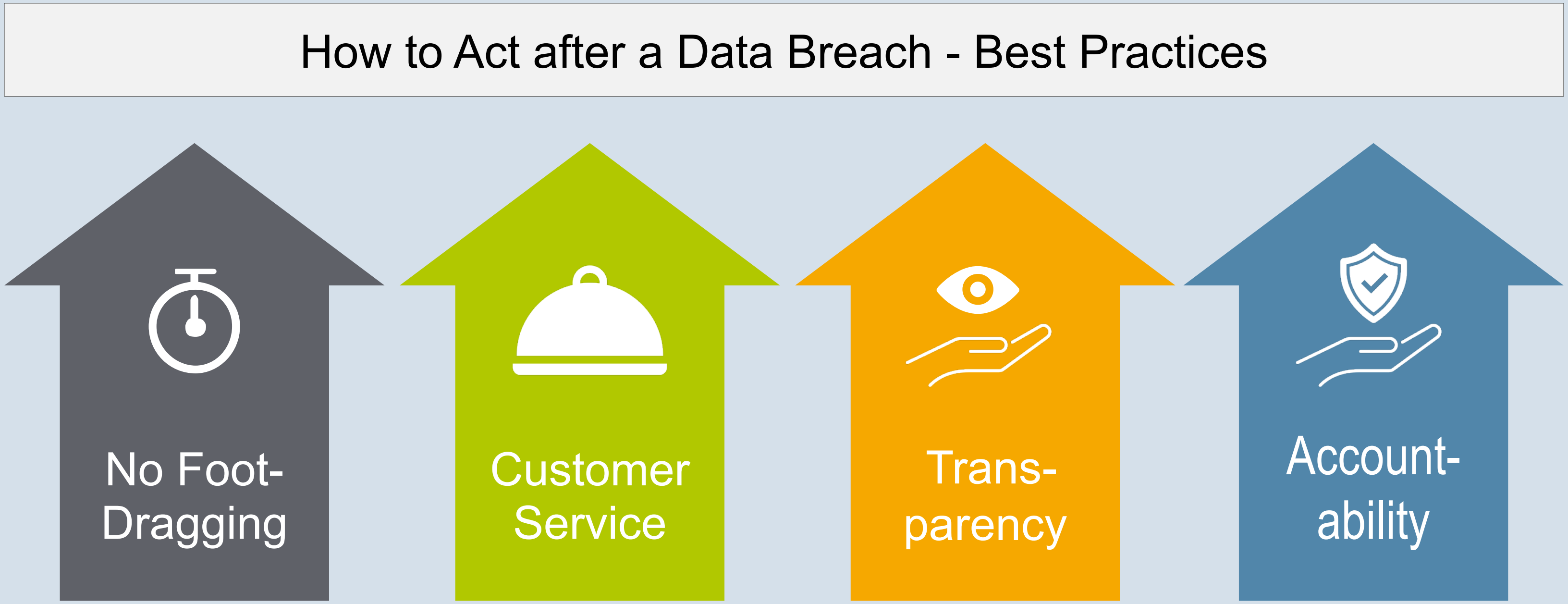
- Set strong defaults
- Leverage concrete commitments
- Facilitate comparisons across peers

Develop user-centric security rules

Customize training and guidance

Create a culture of openness

How to Act after a Data Breach



How to Act after a Data Breach - Best Practices

No Foot-Dragging

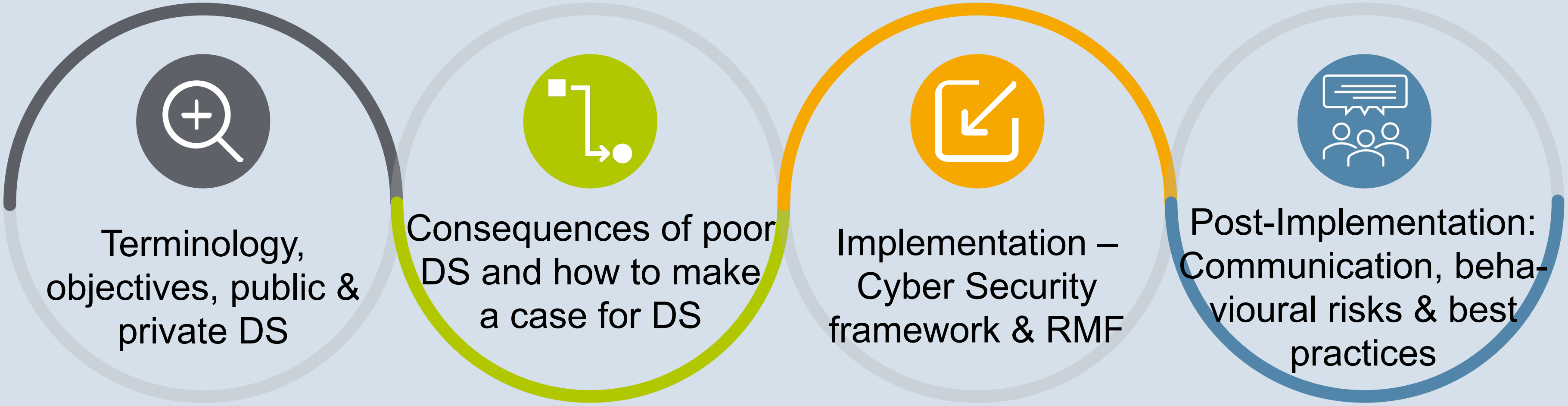
Customer Service

Trans-parency

Account-ability

Key Take Aways

Data Security



Terminology, objectives, public & private DS

Consequences of poor DS and how to make a case for DS

Implementation – Cyber Security framework & RMF

Post-Implementation: Communication, behavioural risks & best practices