

Frameworks

For Cybersecurity, Data Governance and Privacy

Alan Raubenheimer

alan.raubenheimer@datahorizons.co.za

 [linkedin.com/in/alan-raubenheimer-8015374/](https://www.linkedin.com/in/alan-raubenheimer-8015374/)



DATA HORIZONS
GOVERNANCE. PRIVACY. POTENTIAL

Introduction

Data Horizons is a specialist consultancy. We focus on:

- Data Strategy
- Data Governance
- Cybersecurity Governance
- Data Protection & Privacy
- AI Governance

Projects in South Africa, Africa , Singapore, Bermuda & UAE

We are an IAPP training partner

Currently partnered with Cenfri in Rwanda

- Working with 5 Ministries to build Data Strategies & implement Data Governance program
- Drafted Rwanda Data Sharing Policy – working with DPOs across Rwanda Government



Frameworks

For
Cybersecurity, Data Governance and
Privacy



The Multiple
Dimensions of Risk
can feel
overwhelming

Managing Information Risk

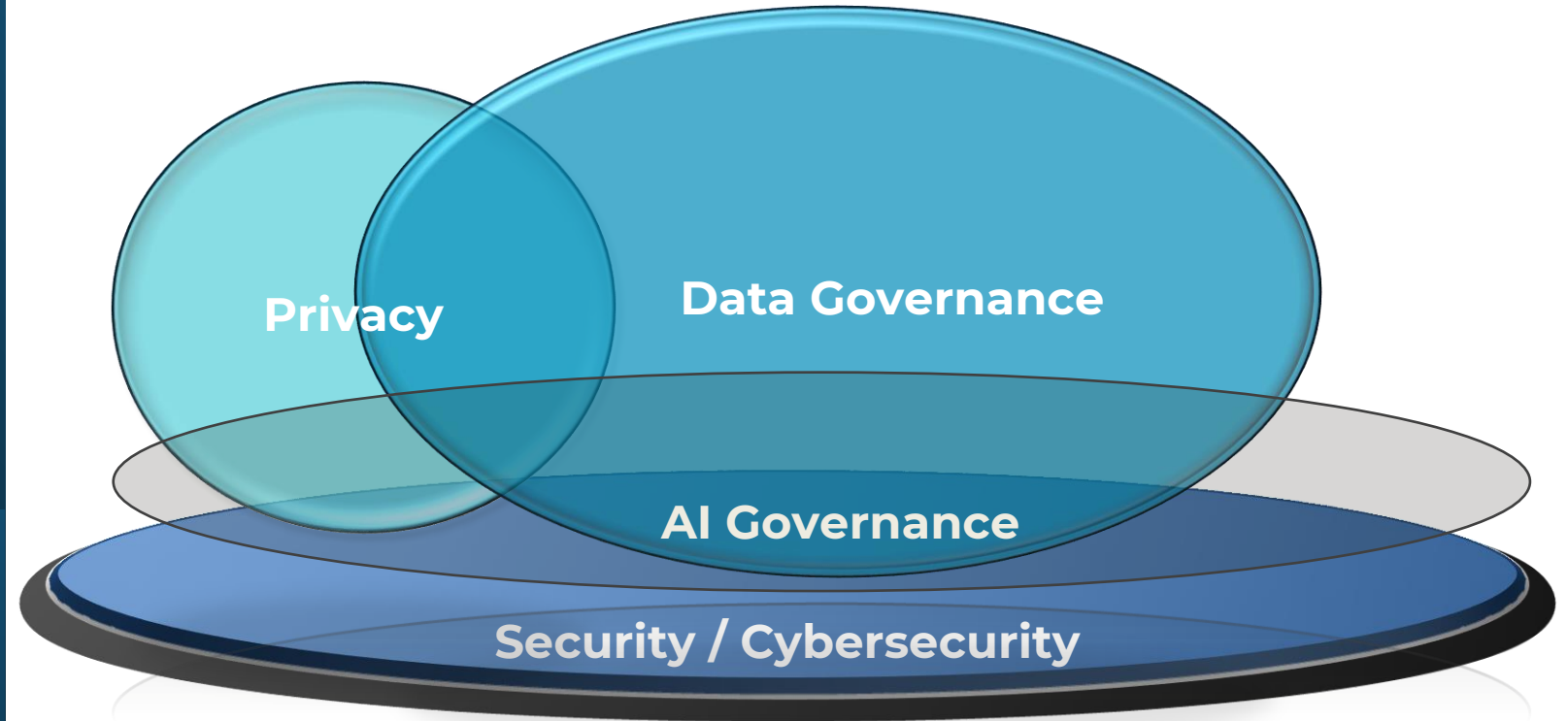


DATA HORIZONS
GOVERNANCE, PRIVACY, POTENTIAL



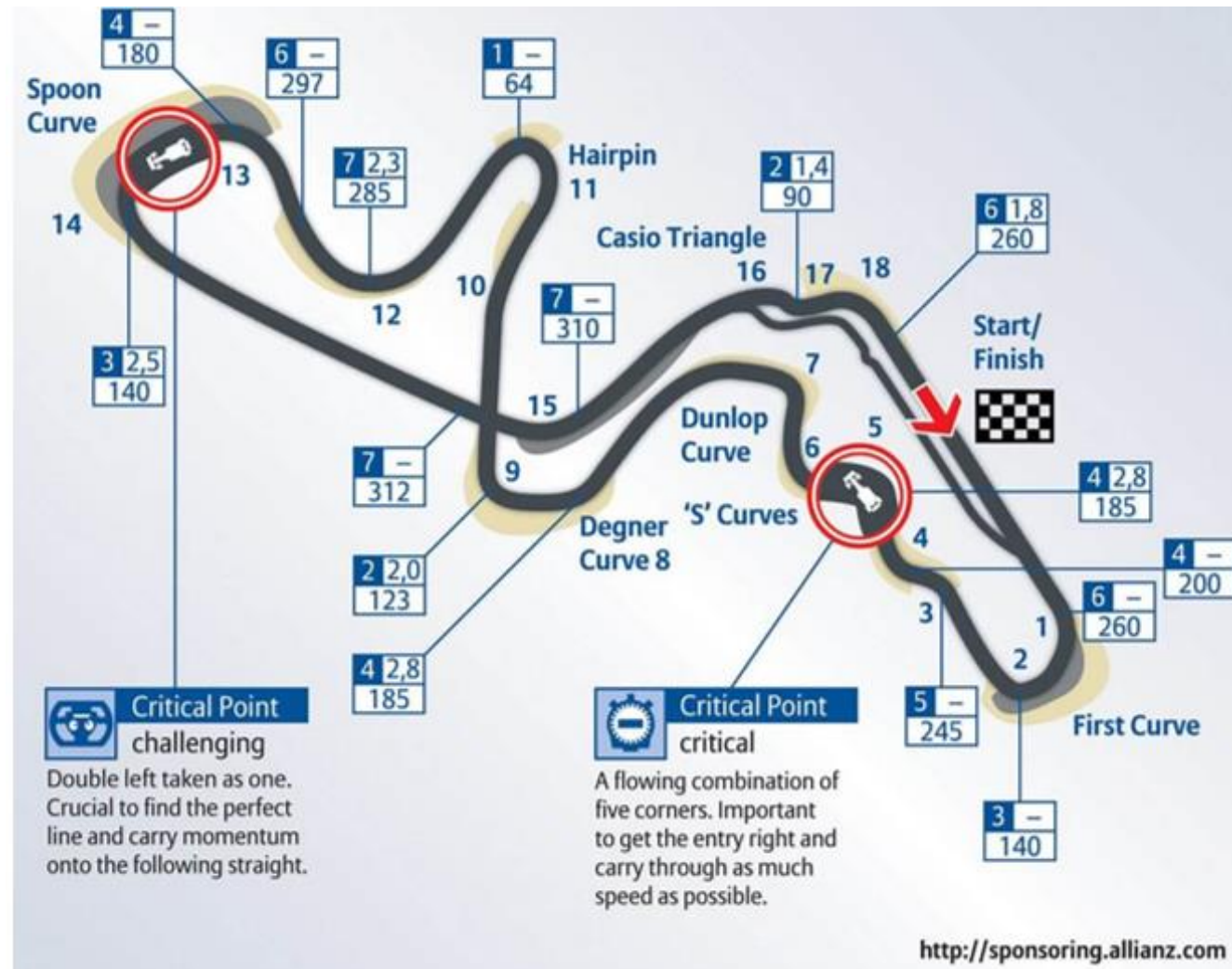
DATA HORIZONS
GOVERNANCE, PRIVACY, POTENTIAL

Relationship between Security, Data Governance, Privacy (and AI Governance)



- No organisation can survive without security - it is the foundation of data protection and governance.
- Data Governance relies on and informs security but does not implement it.
- Data Privacy cannot exist without security.
- Data Governance addresses a large part of data privacy.
- AI Governance depends on all these disciplines.

What is a Framework?



Primary Framework Components

Primary components of an organization's framework are:

Mission / Vision – Aligned with Business & Data Strategy

Scope – Local, International Regulatory considerations, Organisation size & budget

Primary associated Regulations, Policies, Procedures and Standards

Roles and Responsibilities

- Including key structures & forums

Primary Activities

RACI

Ancillary Artefacts:

- Implementation Plan / Roadmap
- Measurements
- Communication Plan
- Risks, Controls, Mitigation
- Detailed R&R
- Measurement

- You should also have Data Strategy
- Associated Policies & Procedures



Defining Your Framework

Cybersecurity

Data Governance

Data Protection & Privacy

Risk Management

AI Governance



A Rationalized
Approach

Input To Your Frameworks

Key Insight




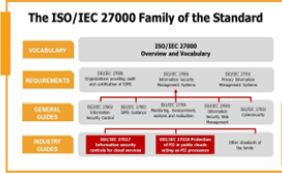



Do not try to invent something new

- Leverage internationally recognized frameworks & principles
- Align with regulatory requirements
- Adapt to your organisation
- Take the best and make it your own

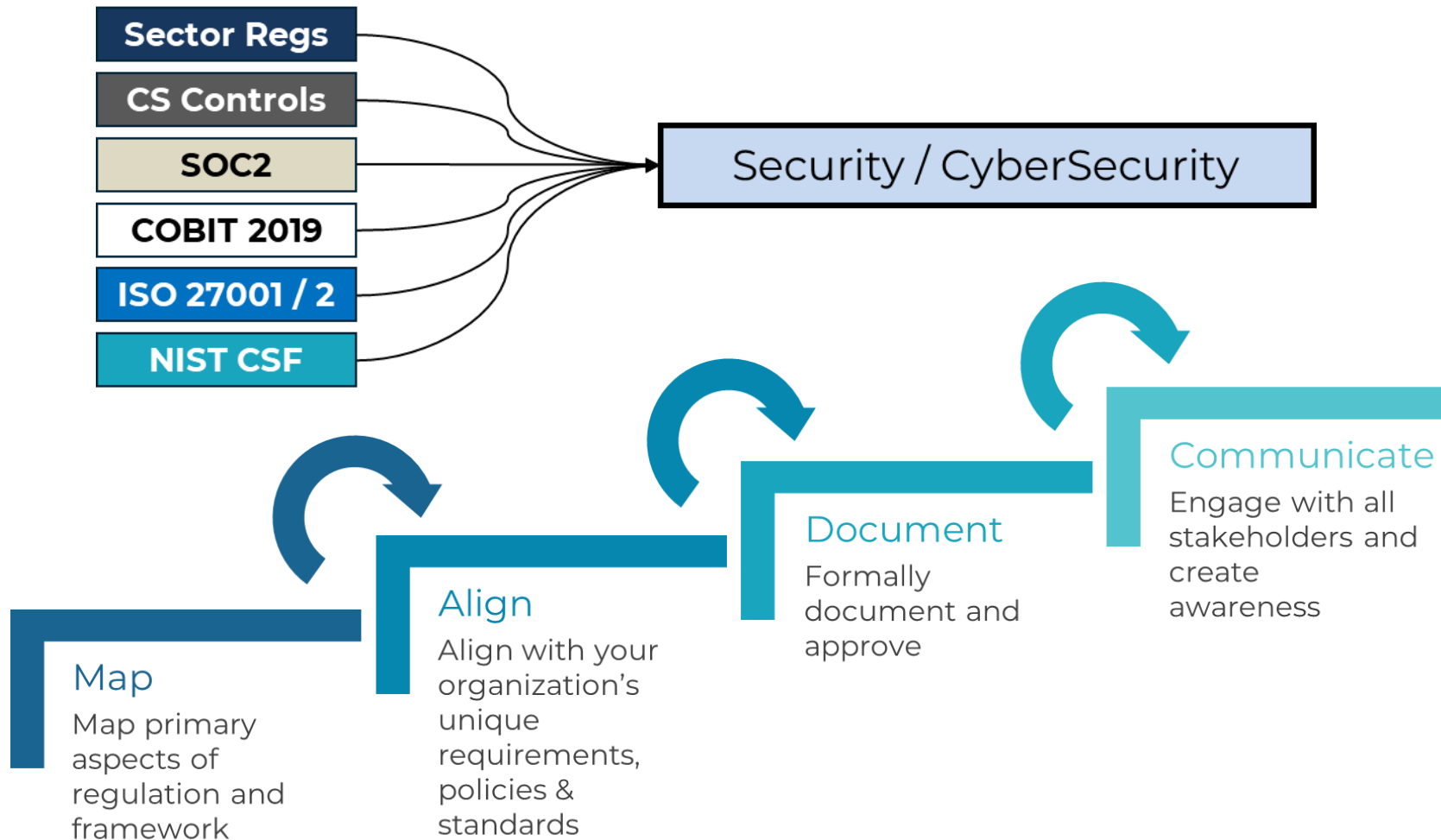


Top Cybersecurity Frameworks

Sector- and Region-specific regulation also must be considered – e.g., Banking & Insurance Sector Cybersecurity laws.

NIST CSF	ISO/IEC 27001	SOC2	CIS	COBIT 2019
<p>NIST CSF is the most widely used cybersecurity framework worldwide. The security controls in the framework are broken up into 5 key functions:</p> <ul style="list-style-type: none"> • Identify • Protect • Detect • Respond • Recover 	<p>ISO/IEC 27001 provides a comprehensive information security management (ISMS) framework and requirements for an information security management system (ISMS). It defines a 4-step cycle:</p> <ul style="list-style-type: none"> • Plan • Do • Check • Act 	<p>SOC2 is a framework from AICPA for service organisations. It covers 5 Areas and over 60 compliance requirements and addresses security, privacy and governance</p> 	<p>The CIS guidelines consist of 20 key actions, called critical security controls (CSC). They are organized into 6 key factors and address over 240 Controls</p> 	<p>COBIT 2019 has 5 domains and 40 control objectives, most of which have an impact on security best practice. It embodies the best practices of NIST, ISO/IEC 27001 and CIS. The COBIT 2019 framework serves as the primary basis for the Acumen Information and Technology (I&T) Governance Framework.</p> 

Build Your Cybersecurity Framework



Top Privacy Frameworks

There are many!
All address common principles

ISO 27701 – Privacy
(part of ISO 27000 series)

GDPR / Regulation

NIST Privacy Management Framework (PMF)

FIPs or FIPPs (Fair Information Principles / Practice Principles)

OECD Guidelines

Convention 108+
(European Court of Human Rights)

IAPP CIPM Framework

AICPA PMF

Nymity/TrustArc Framework

ISO 29001

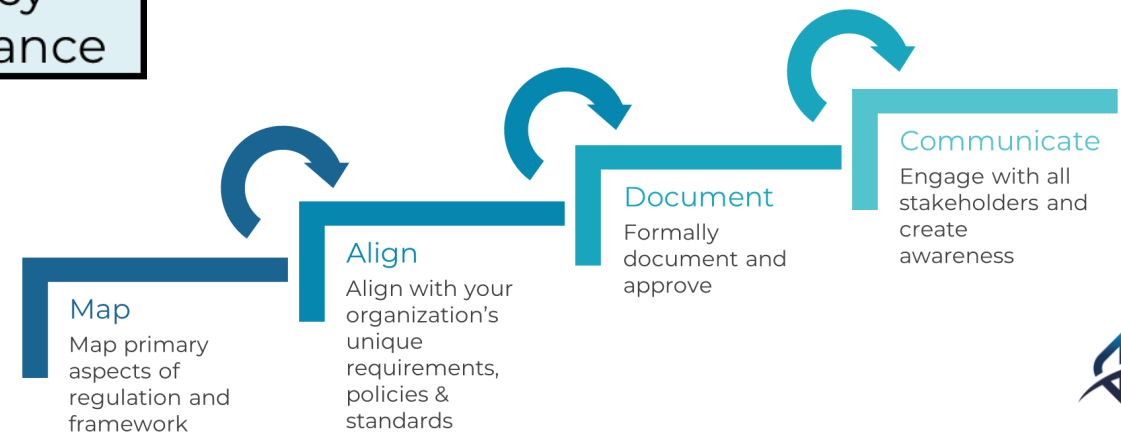
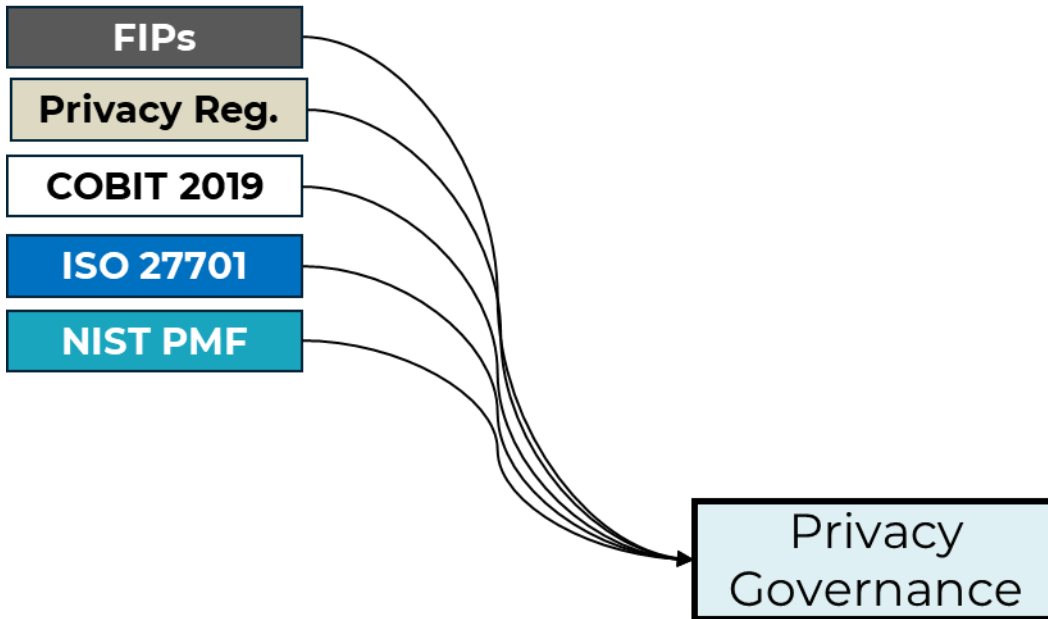
Generally Accepted Privacy Principles (GAPP)

Regional standards
e.g., APEC Privacy Framework

Sector privacy requirements & laws – e.g., HIPAA

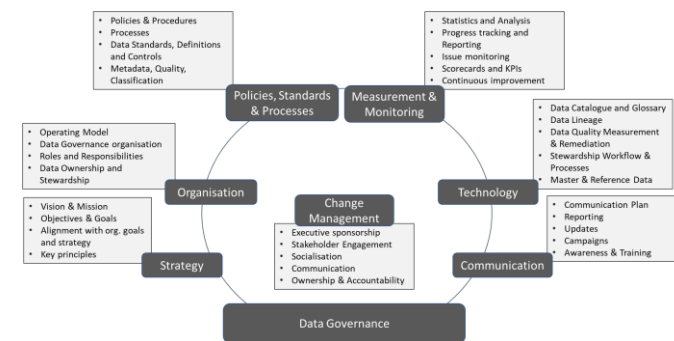
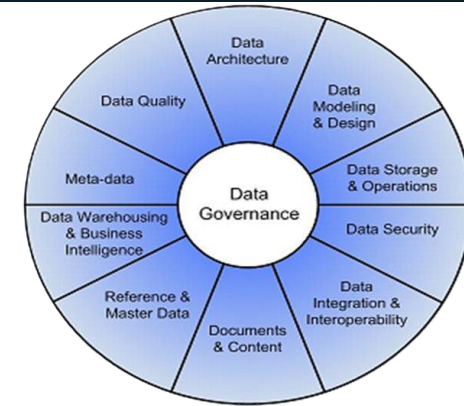


Build Your Privacy Framework

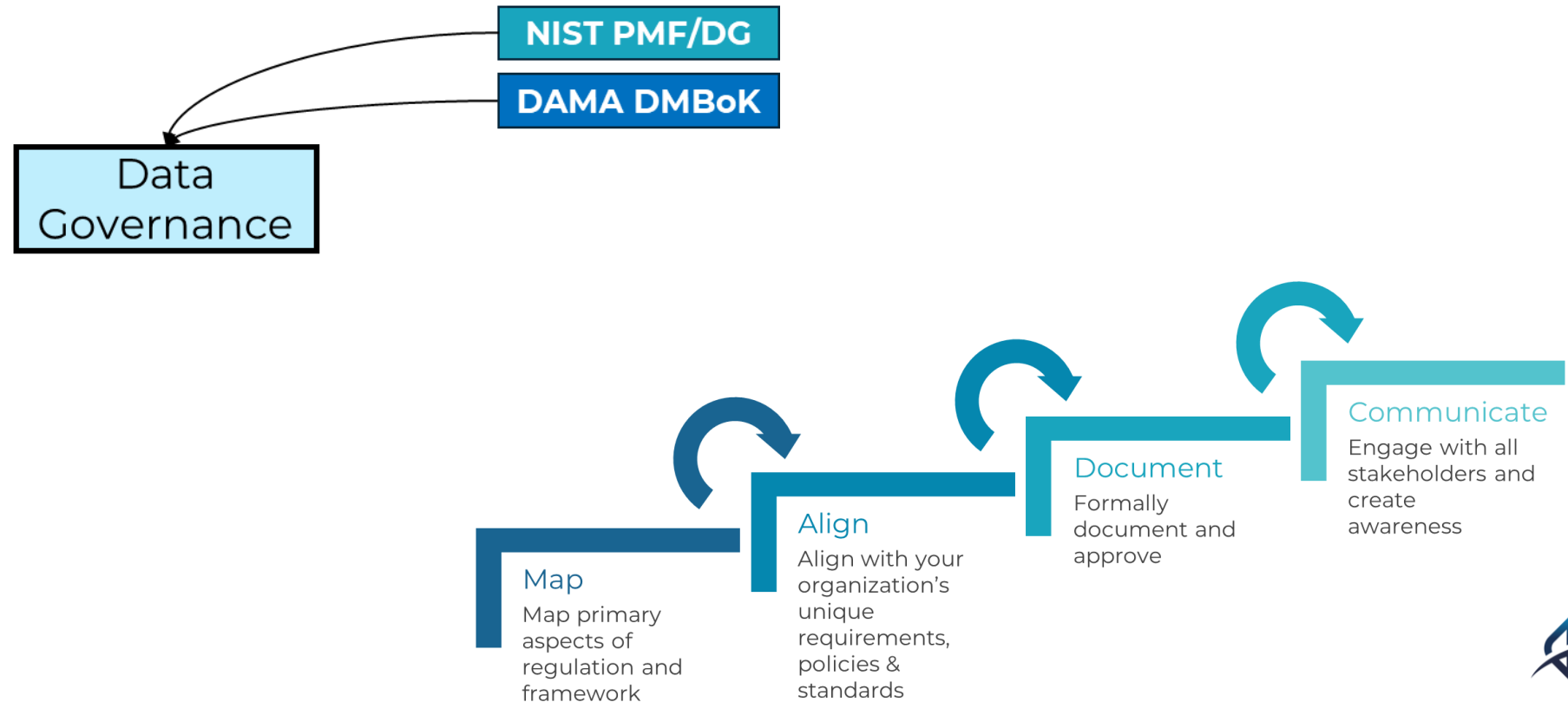


Top Data Governance Frameworks

- DAMA DMBok is recognized internationally as the standard
 - It is a set of Data Management guidelines, including Data Governance
- NIST is creating a Data Governance Profile as a companion to its Privacy, Risk and Cybersecurity management frameworks.
- Data Governance Institute
- ISO 8000 (Data Quality)
- Scholarly books & articles
- There is currently no internationally recognized certification for Data Governance (aside from the DAMA CDMP Master elective).
- HOWEVER...
There are MANY examples of well-defined data governance frameworks

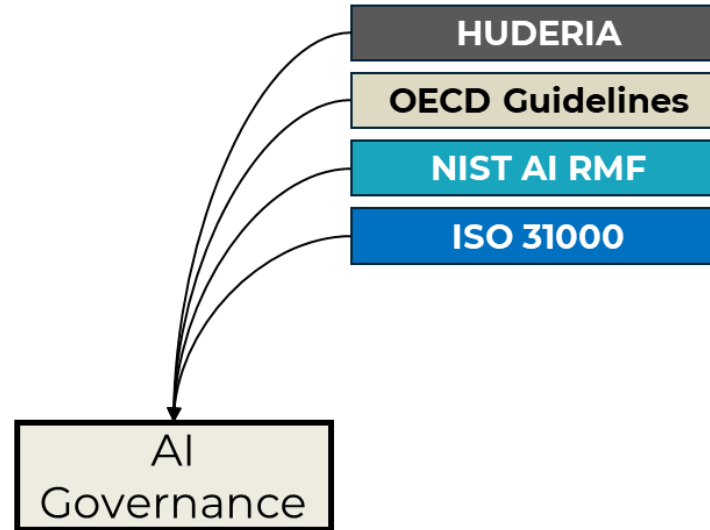


Build Your Data Governance Framework



A Rationalized Approach

Additional Considerations

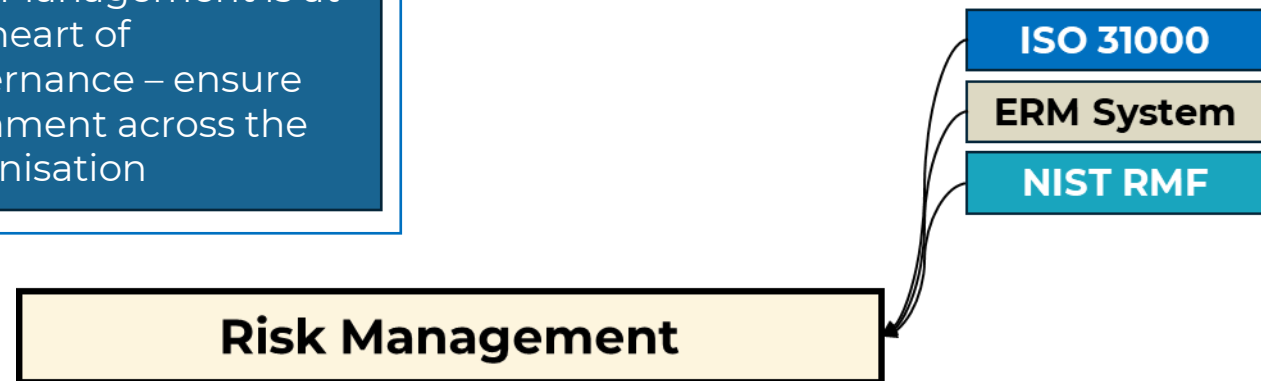


Key Insight

AI is going to play an ever-increasing role in your activities – be sure you consider it sooner, rather than later

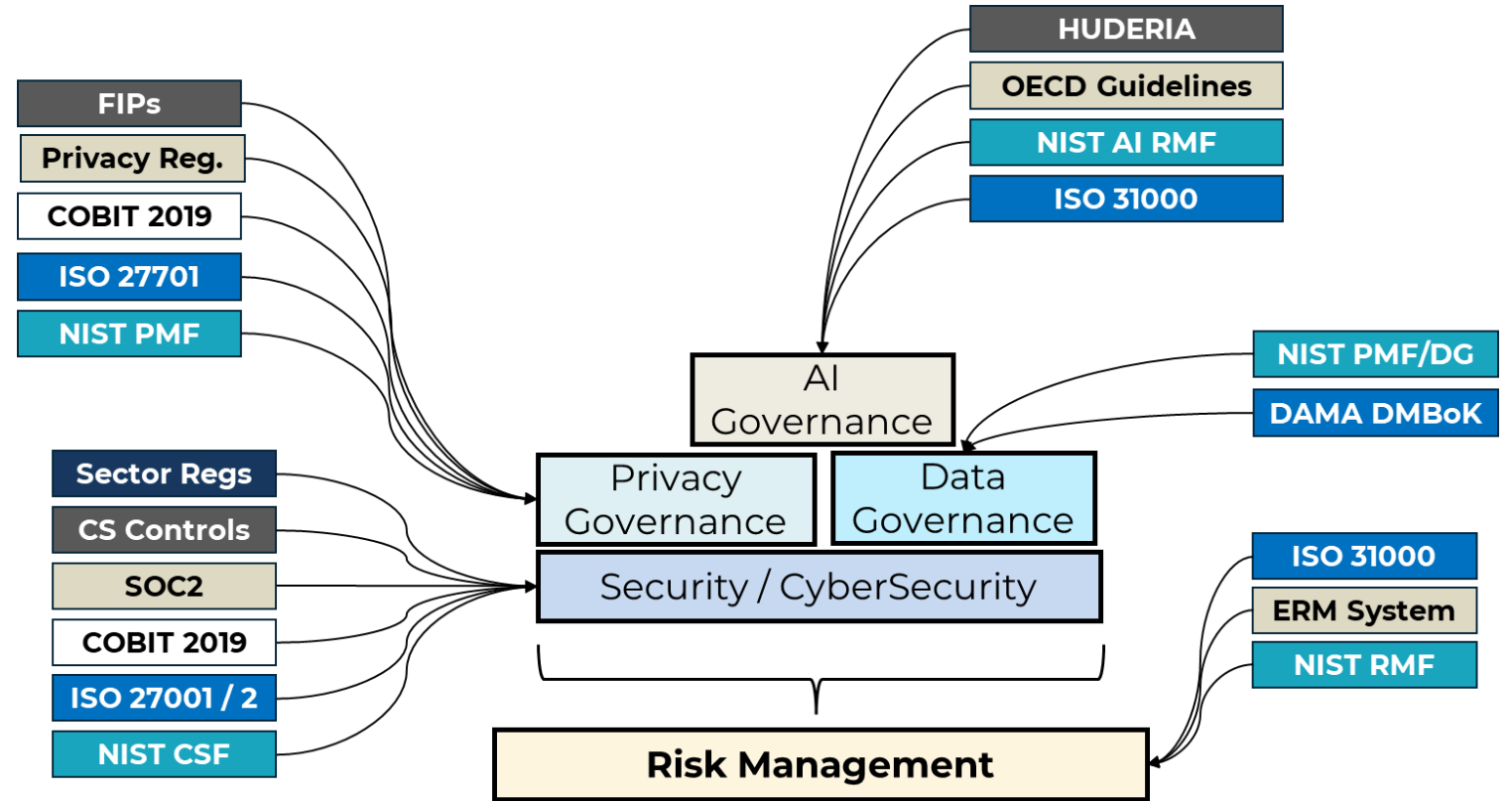
Key Insight

Risk Management is at the heart of governance – ensure alignment across the organisation



A Rationalized Approach

Putting It All Together



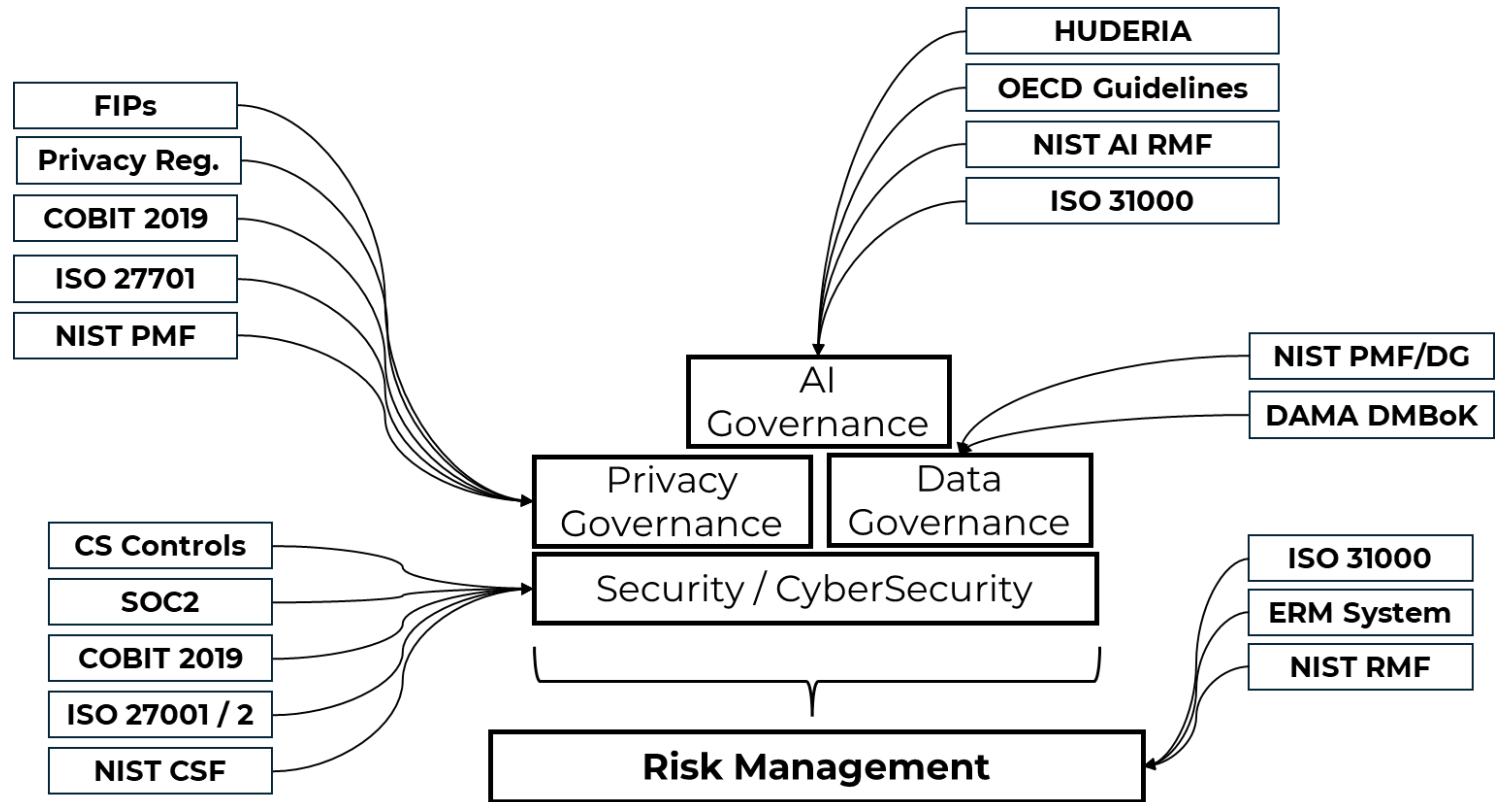
Key Insight

Leverage common and existing functions and work WITH these – do not reinvent the wheel



A Rationalized Approach

Putting It All Together

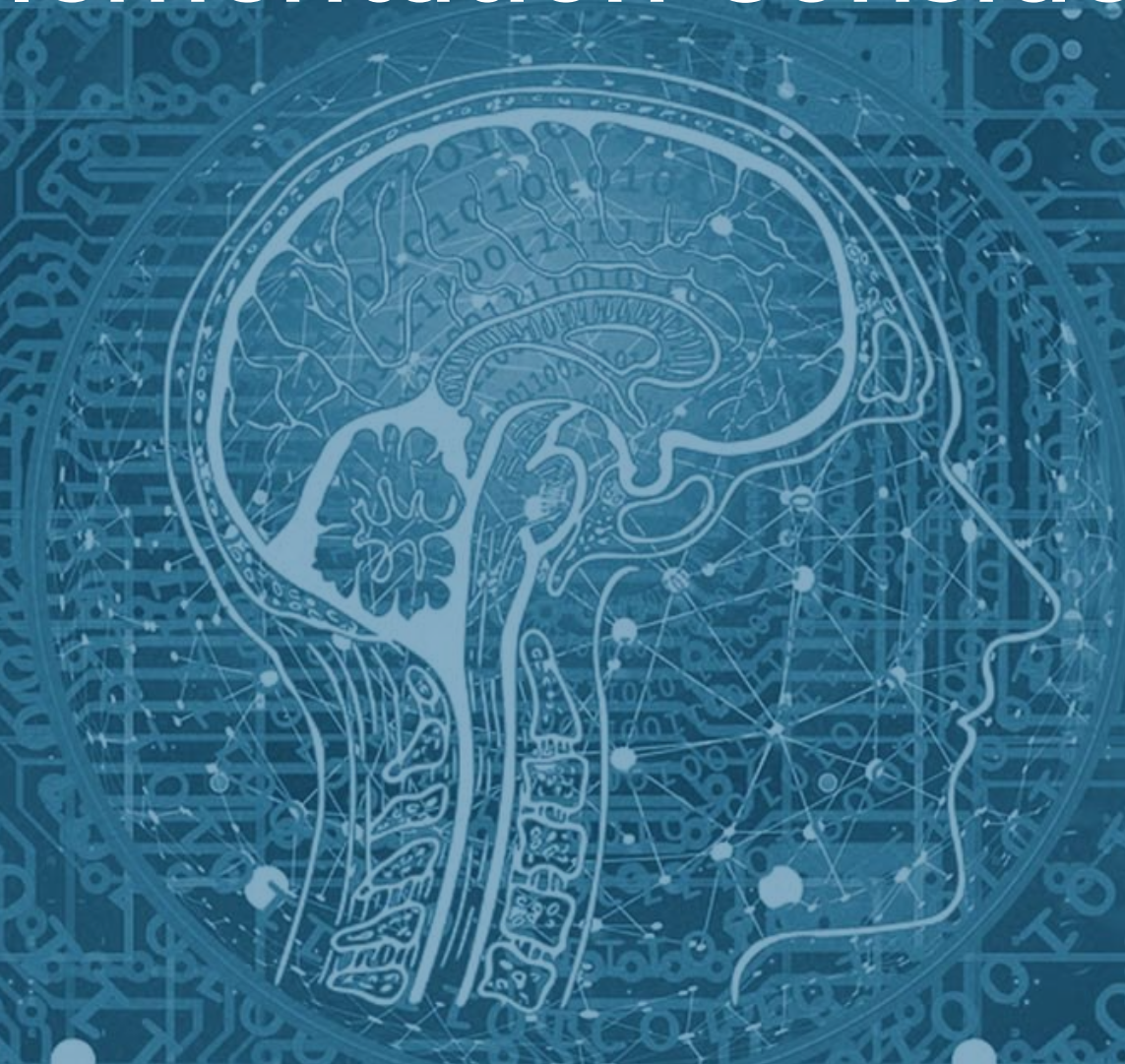


Key Insight

Leverage common and existing functions and work WITH these – do not reinvent the wheel



Implementation Considerations



Creating Programs not just projects



DATA HORIZONS
GOVERNANCE, PRIVACY, POTENTIAL

Implementation Considerations

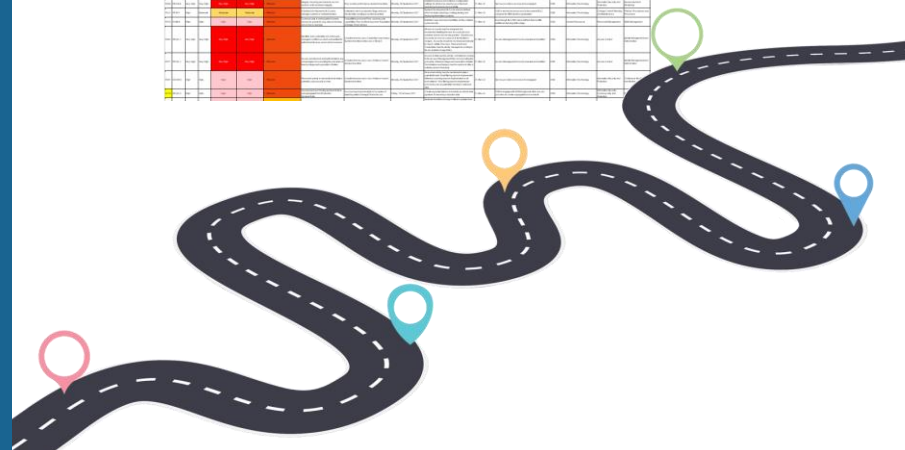
A Rationalized
Approach



- Create **Programs** not just projects
- **Executive Sponsorship** and involvement are vital
 - Without it, your program will fail or have little effect
 - Get **support from leadership**
- Engage the right **stakeholders**
 - Make Risk, Compliance and Legal functions your ally
 - Avoid Turf Wars
 - Cross functional involvement, internal & 3rd-Party experts
- Use existing capabilities
 - Risk Register, Controls & Audits



Risk ID	Risk Description	Risk Category	Risk Level	Risk Owner
R001	System Downtime	Operational	High	IT
R002	Data Breach	Security	Critical	IT/Security
R003	Compliance Failure	Legal	Medium	Legal
R004	Supply Chain Disruption	Operational	Medium	Procurement
R005	Customer Churn	Operational	Low	Marketing
R006	Employee Turnover	Operational	Low	HR
R007	Reputation Damage	Operational	Medium	PR
R008	Financial Instability	Operational	High	Finance
R009	Regulatory Changes	Legal	Medium	Legal
R010	Market Volatility	Operational	Low	Finance



- Create an actionable plan
 - Start small, think BIG
- **Know your data** landscape
 - You cannot govern what you do not know
 - Centralize - Map, inventory, catalogue
- Communicate
 - Create a **Communication Plan** which includes training and awareness
- **Measure**, monitor and Report for Success

Q&A



Thank you

