inetum realdolmen
Positive digital flow

GRC: een essentiële sleutel in securitytransformatie

Pieter De Backer, Inetum-Realdolmen

inetum realdolmen
Positive digital flow

Pieter De Backer

Principal GRC Security Consultant

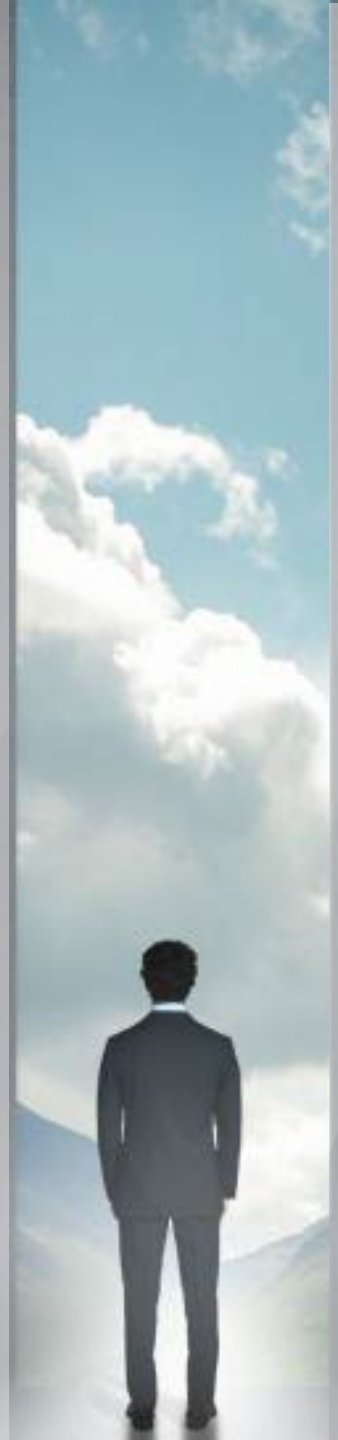
Pieter.debacker@inetum-realdolmen.world

inetum realdolmen

Positive digital flow

Governance, Risk & Compliance

The key to drive your transformations



Session Topics

01 Business and transformation context

02 GRC to navigate your tranformations

03 Digital transformed GRC

In order to understand the **value of GRC** for digital and security transformation we need to start with a **understanding the context** of organizations today

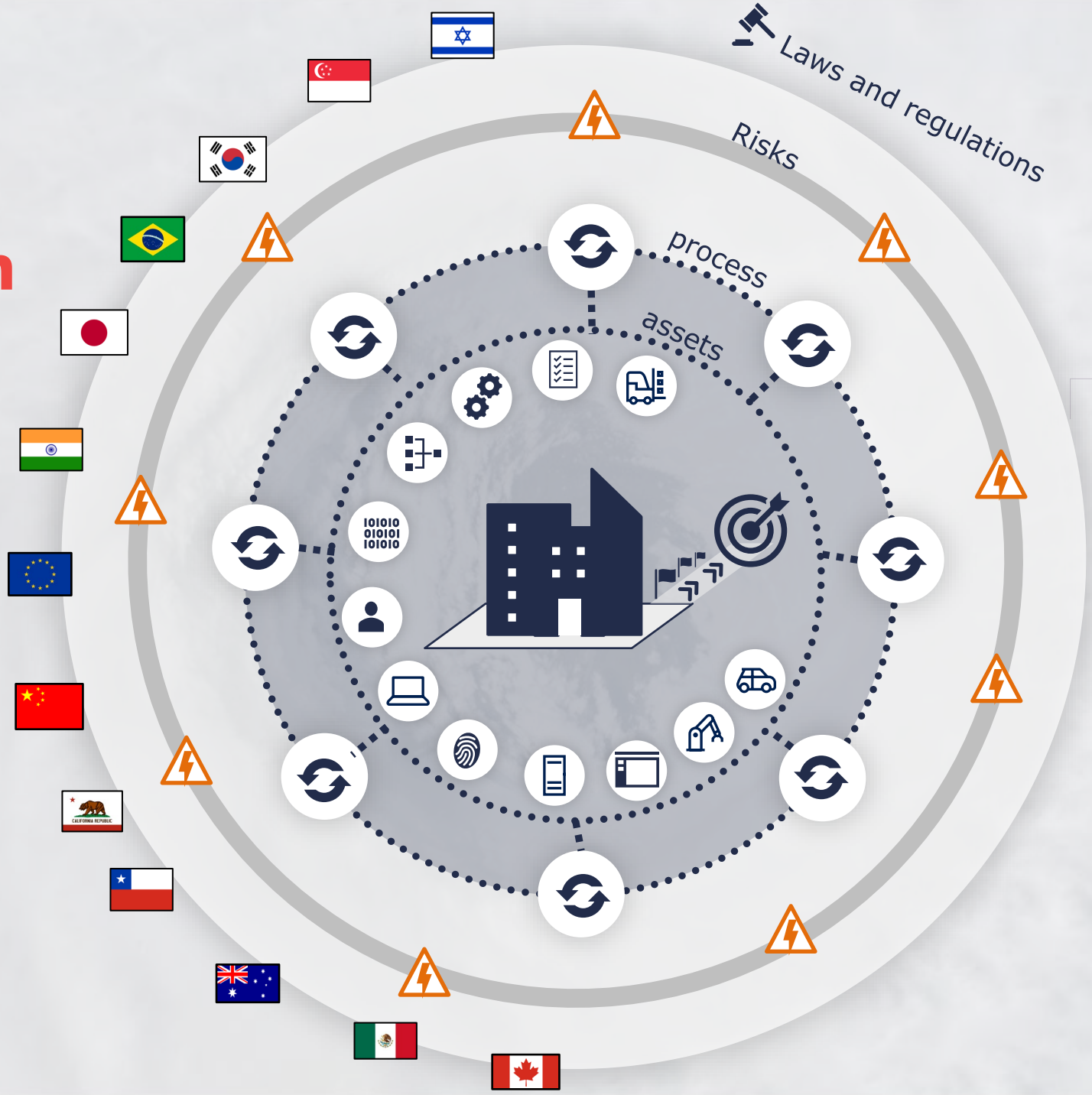
we ‘ve moved from linear to exponential changing times

Increasing complexity and uncertainty

V U C A

Volatility Uncertainty Complexity Ambiguity

Simplifying the context of the organization



- People
- Process
- Information
- Technology

Complexity lies within the many universes that need to be managed simultaneously

risks grow, # compliance requirements grow and behavior of threats change constantly

To navigate change, lack of information and **complexity** we first need to understand the **digital transformation** context we are dealing with

Transformation, a byproduct of market changes

What is Digital transformation

Digital transformation is the **integration of digital technology**

into **all areas** of a business,

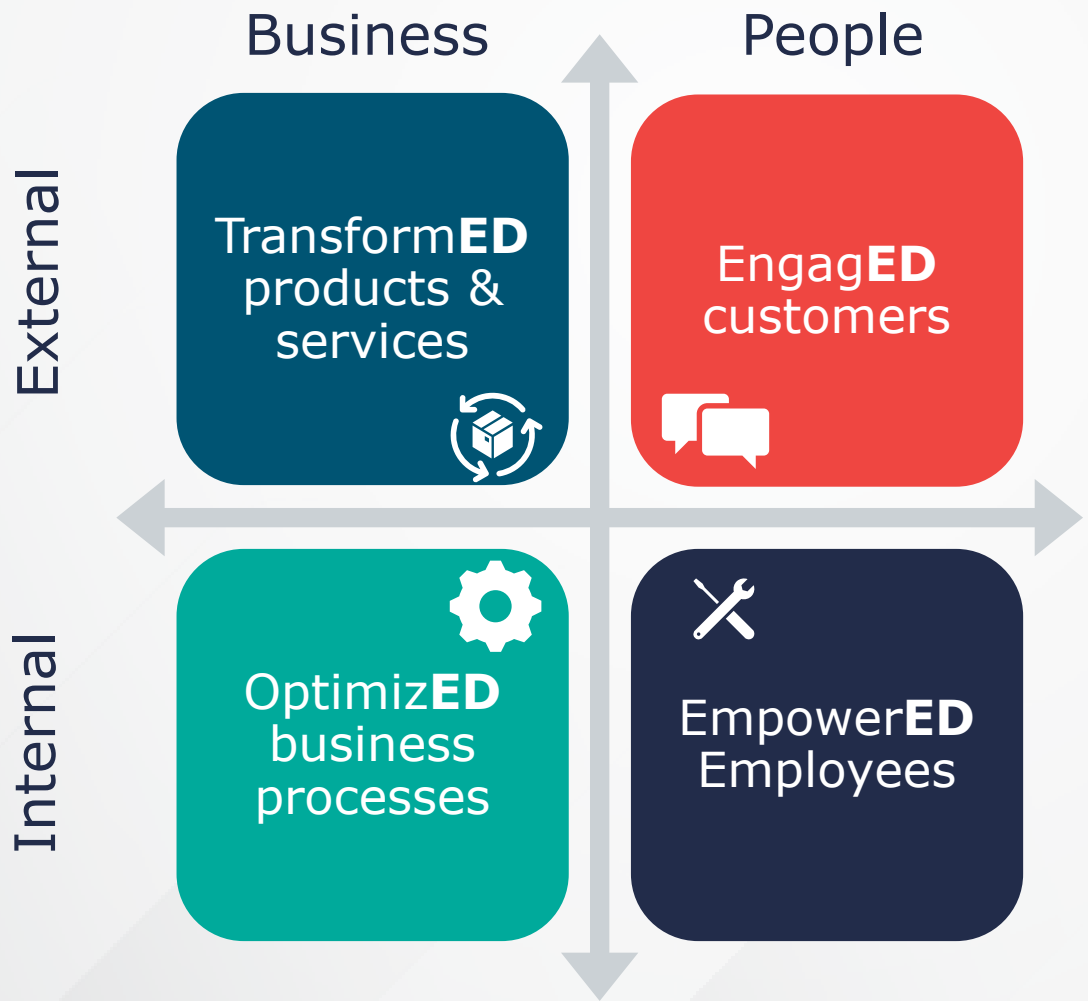
fundamentally **changing** how organizations **operate** and **deliver value to their customers**

by enabling greater agility, efficiency, effectiveness, productivity, transparency, better decision making, and significant cost savings

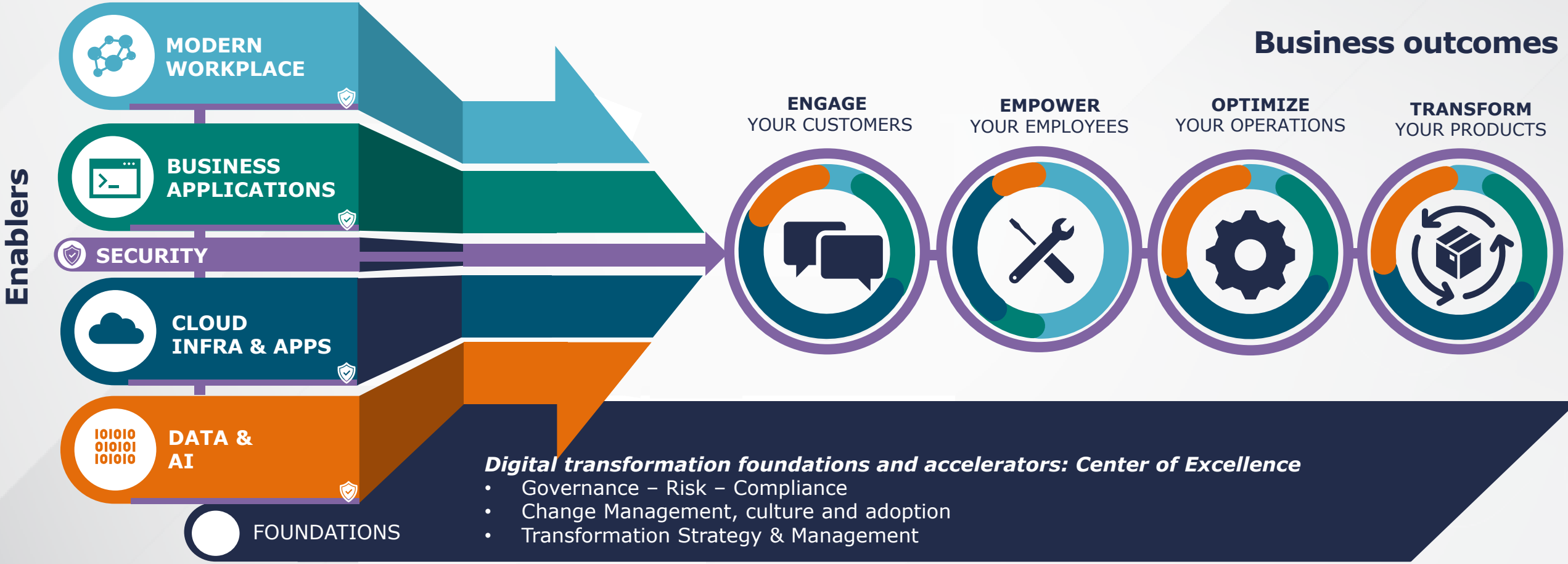
Is all about **transforming** the business and **reimagining** how to create **value** for customers and **competitive advantage** in a **digital first world**

Business agility and resiliency facilitated by culture, technology and processes

Digital transformation is leading to these 4 main business outcomes



Enablers of Digital transformation



Multiple connected transformations

Digital Transformation

Employee empowerment transformation
Customer engagement transformation
Operations optimization transformation
Product transformation

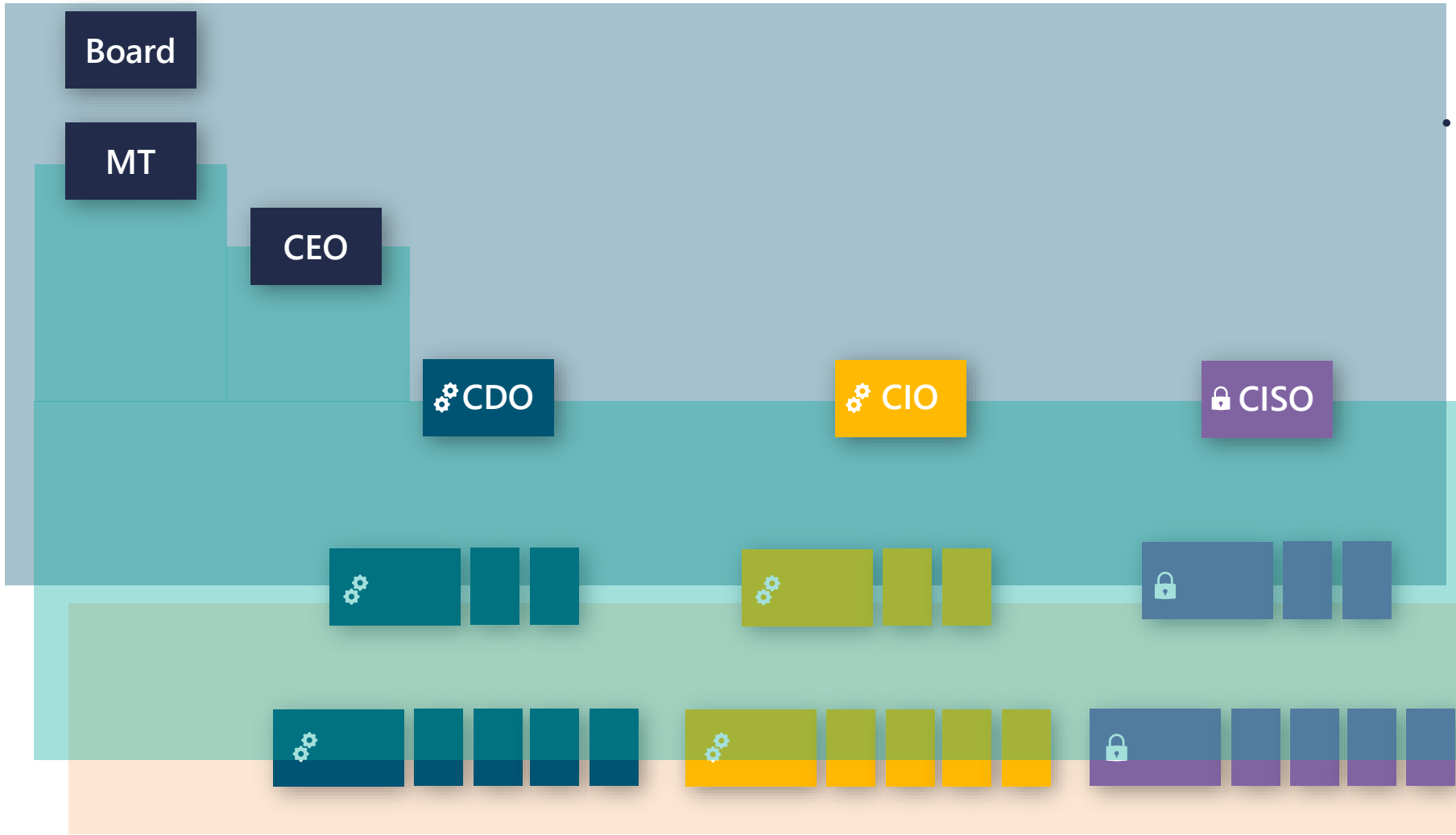
IT Technology Transformation

Cloud Transformation
Data & AI transformation
Modern Workplace transformation
Business application transformation

Security Transformation

Zero trust transformation
Business driven risk management transformation
Modern Security Operations transformation
DevSecOps transformation
Modern Security Management transformation

All resulting in Discussion @ Different Levels



Governance & Strategy
strategy, objective, priorities and steering

Management
Planning and managing the execution

Operations
Build, implement, integrate, operate and optimize activities

So, **how** can we **navigate** these transformations and discussions **towards success**

It starts with **GRC** and the **effectiveness of GRC** function within the organization

Transformation requires

I. **Vision** to shape a new future translated into the transformation strategy

II. **Effective governance** to steer the implementation of the digital transformation efforts

III. **Managing change** which in return requires

- effective governance
- **proactive risk management**
- adherence to internal and external **compliance** requirements to optimize benefits of the transformation

IV. **Successful adoption** and operations which depend on the appropriate management of the risks associated with that new technology

Study revealed the GRC importance for companies in transformation

62%

of the respondents believe that the shift to digital transformation exposed gaps in the existing GRC processes

77%

believe that risks have increased as they become more reliant on digital channels

- Increase of the importance of GRC function
- New regulations have influenced the drive to digital world
- Increase of the need to anticipation to more unexpected events and deal with greater volumes of data
- GRC approach needs to support a more agile risk mitigation, improve visibility of risk and better connection with business priorities.

Resource study digital transformation and future of GRC by risk.net in 2022 sponsored by IBM

What is GRC

GRC is the integrated **collection of capabilities**

that **enable** an organization **to**

- **(G)** reliably **achieve objectives** → art of corporate governance
- **(R)** **address uncertainty** → art of risk management
- **(C)** and **act with integrity** → art of compliance management

GRC **"a toolbox to reliable achieve business objectives"**

GRC unfolded

(G) Governance (and internal control environment)

is **directing** the organization to **their objectives**

While overseeing **control** and **evaluating** the organization via the internal control environment

to **realize sustainable success**

(R) Risk management

is addressing **effect of uncertainty** on the **organization's ability to meet** its [business] **objectives**

Effect *= deviation from what was expected which can be negative or positive (positive risks are referred to as opportunities)*

Uncertainty *= lack of information or knowledge concerning an event, its consequences or likelihood*

Objective *= the goal of an activity @ different levels of the organization entity, department, product, etc.*

(C) Compliance management

is **acting with integrity or in accordance** with requirements set by others: **external applicable laws, regulations,** contract, standards and with the voluntary chosen or specifically designed requirements that are set by the organization's governing body via **internal policies**

GRC capability exists @ corporate / enterprise level and within all underlying business functions such as sales, security, privacy, hr, marketing, legal, operations, finance etc.

Essence of Governance

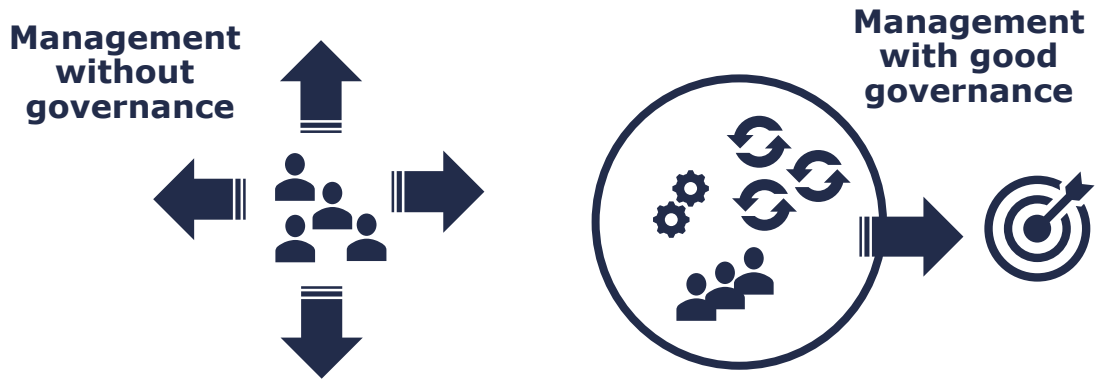
A Business does not run itself

Governance and the control environment

to ensure that we reliably achieve our objectives and create **sustainable success**

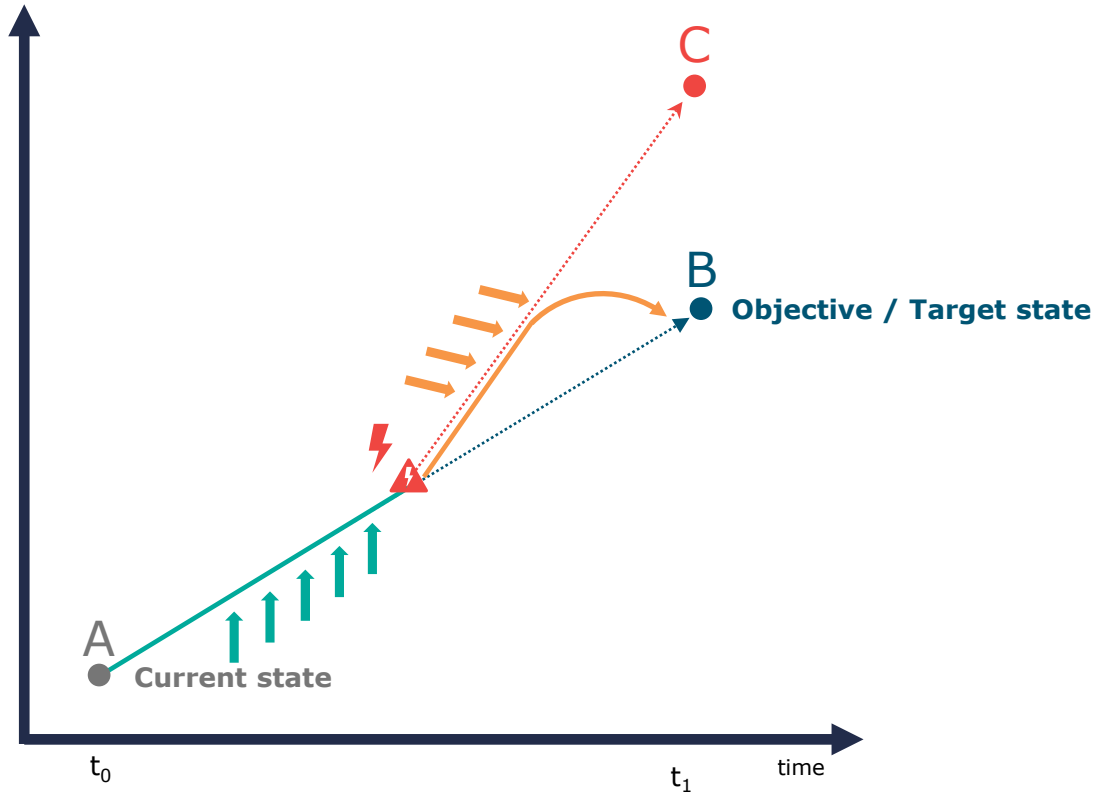
Governance is about **setting the premise** for success by equipping managers with **clear directions, expectations, objectives, resources and installing the control environment**

- Vision, values, principles
- Strategy and objectives
- Roles and responsibilities
- Policies
- Processes
- Ethics and culture



Essence of risk

Risk management is about identifying and managing uncertainties that might impact the objective or asset in order to improve the ability to meet the objectives



0 Organization determines where they are now at t_0

1 Organization sets objective at t_0, they want to be @ position B at t_1

2 Organization creates an action plan to get from A to B and starts executing it in the period between t_0 an t_1

Discovered risk : The presence of uncertainty, new information or lack of information means that an unexpected perturbation can have an effect and can cause a deviation from the action plan as defined in t_0. If nothing would be done the organization would not reach objective B but end up in a position C at t_1

This is the effect of uncertainty on the possibility of reaching the objectives

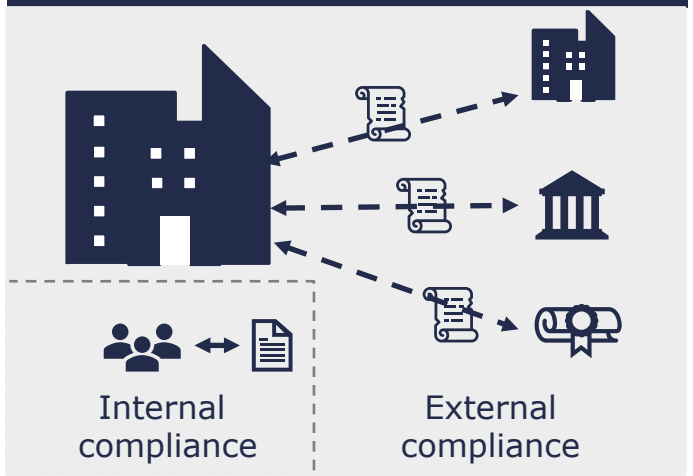
3 Execute risk management to try to anticipate and look out for deviations from the plan and implementing corrective actions so that the objectives are reached despite the unexpected perturbations.

Essence of compliance

Compliance is having to meet requirements set by others

- requirements → **Laws, regulations, contracts, standards**
- others → **government, customers, certification bodies,…**

Internal vs external



Compliance dimensions

1. Regulatory compliance
2. Organizational compliance
3. Legal / contractual compliance

Compliance risk management

By **treating compliance as a risk** your organization will better focus on the important aspects of compliance, be **more efficient** and **agile** to **respond to changes** in the compliance universe that affects the organization

Compliance posture to indicate how compliant the organization is performing against its internal controls

GRC is key but traditional GRC is not

Overall Traditional GRC challenges

- Perception of a Bureaucratic barrier to transformation " Red Tape"
- Department of "No"
- "Paper security"
- Lacks effectiveness and efficiency
- Lacks whole coverage of your control capability
- Siloed components
- Lack of collaboration with IT operations, developer and other security stakeholders

Governance

- Disconnect between organizational policies and technical implementation of these
- Slow to adapt to changes in market, risk, technology and processes

Risk management

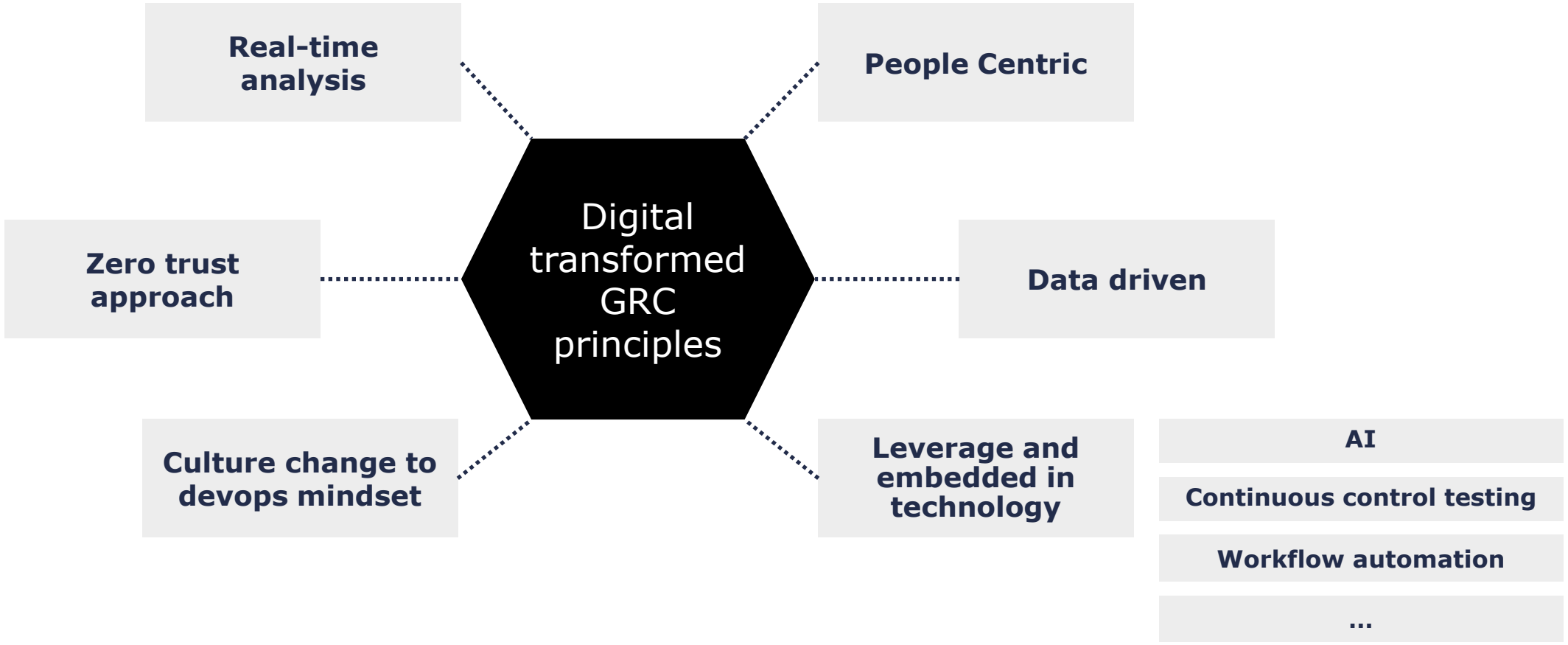
- Disconnect between organizational risk, business line risk, IT risks and security risks
- Management process is often time and resource intensive which lacks agility
- Risks often identified via a static scenario-based approach and is disconnected from security operation that looks at risk from a dynamic real-time perspective

Compliance Management

- Overall Resource intensive
- Audit preparation is intensive
- Audits are only snapshots in time
- Compliance does not equal security, it supports security
- Compliance gets in the way with what business wants
- Compliance gets in the way with what security operations wants to do to mitigate threats

We need a **transformed digital GRC** to bring the value of GRC @ the table

Principles of Transformed digital GRC



It is important to remember that organizations have been governed, and risk and compliance have been managed, for a long time — in this way, GRC is nothing new. The way it is able to **provide value today** in an **era of digital transformation** is totally new and requires a new approach.

GRC and your security transformation

inetum realdolmen
Positive digital flow

Security transformation to modern security that protects the trust in a digital first world

foundations

Zero trust

Improve security foundations

Shift from always trust never verify to trust but verify

Shift From trust but verify to never trust always verify

Use a baseline-to-baseline approach

Business risk Driven

Use an integrated risk management approach that prioritizes and treats risks based on the business impact

Combine a scenario-based approach when starting your risk management and convert to an event-based approach in operations

Modern Security Operations

Organize your security operations from a service perspective and use technology to facilitate the operations within your security operation services

Automate controls, detection and response

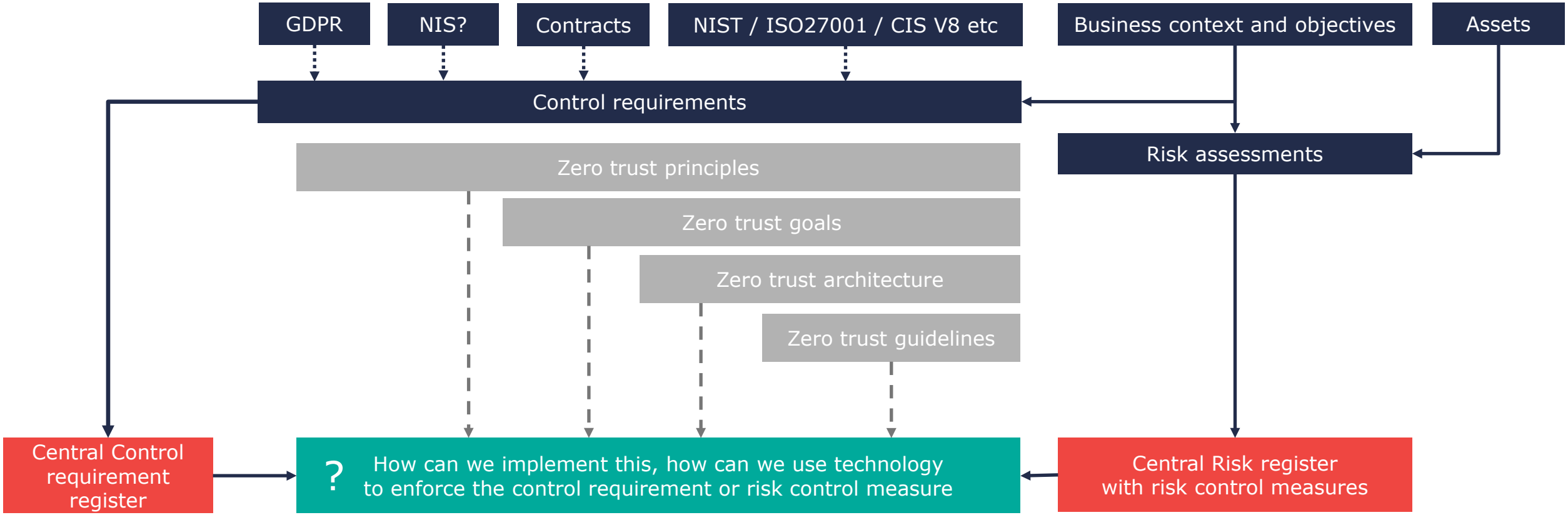
DevSecOps

Adopt the Devops / agile way of working and use DevSecOps as basis to support security innovation

Security transformation, an integrated approach focused on transforming 6 technology domains & GRC

domain	Identity	Device	Infrastructure	Data	Applications	Network	Governance Risk and compliance
	Verify and secure every identity with strong authentication	Allow only compliant and trusted apps & devices to access data	Harden defense and detect & response to threats in real time	Protect data of value wherever it lives, resides or travels	Ensure applications are available, visible and secured	Move beyond traditional network security approaches	Embed GRC into technology to enforce, manage efficiently and effectively
Change	**Modern Workplace Transformation**	**Cloud Transformation**	**Data & AI Transformation**	**Application Transformation**	**Network Transformation**	**GRC Transformation**	
	Modern workplace solutions	Multi cloud / Public cloud / Private cloud	Data & AI solutions	Modern application solutions	Network solutions	People, process, organization	

Look again at your control environment and its implementation



How to embed GRC in DevSecOps