FORRESTER®

Dismantle The Three Lines Of Defense: Embrace Continuous Risk Management

Cody Scott
Senior Industry Analyst, Security & Risk

6 February 2025

BOLD AT WORK

Every superhero has a nemesis

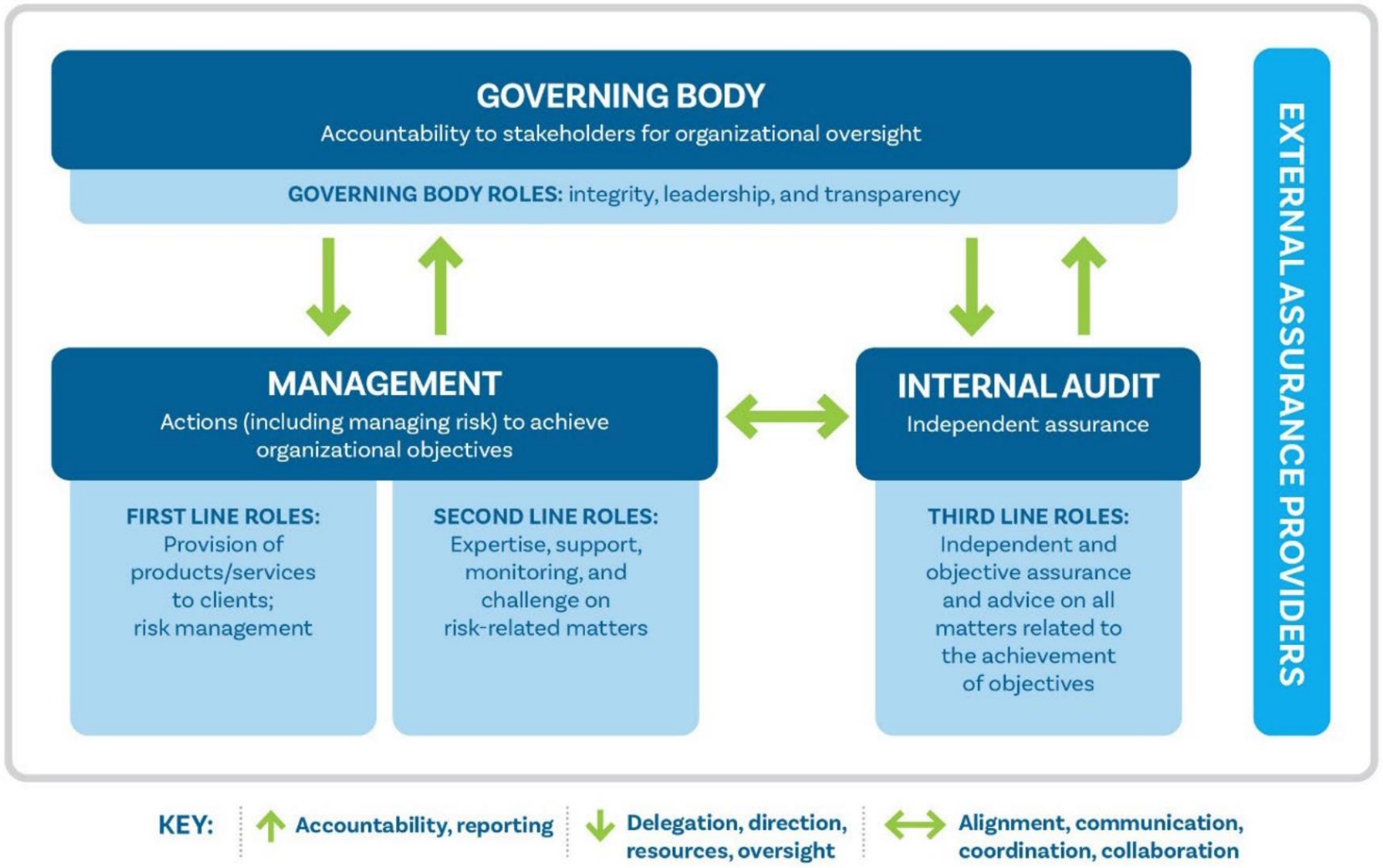

HA HA HA
HA HA HA
A

THREE LINES OF DEFENSE

How did we get here?

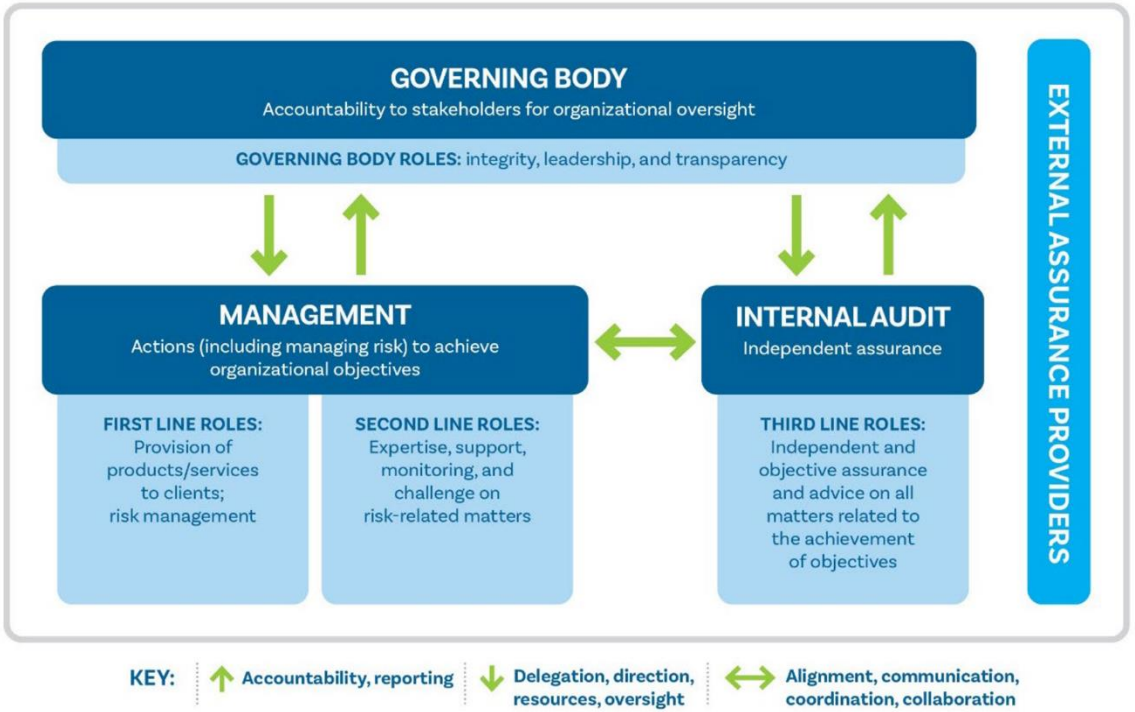
2001 **2002** **2003** **2008** **2013**

Three Lines Of Defense Model



3LOD doesn’t hold up to risk management demands

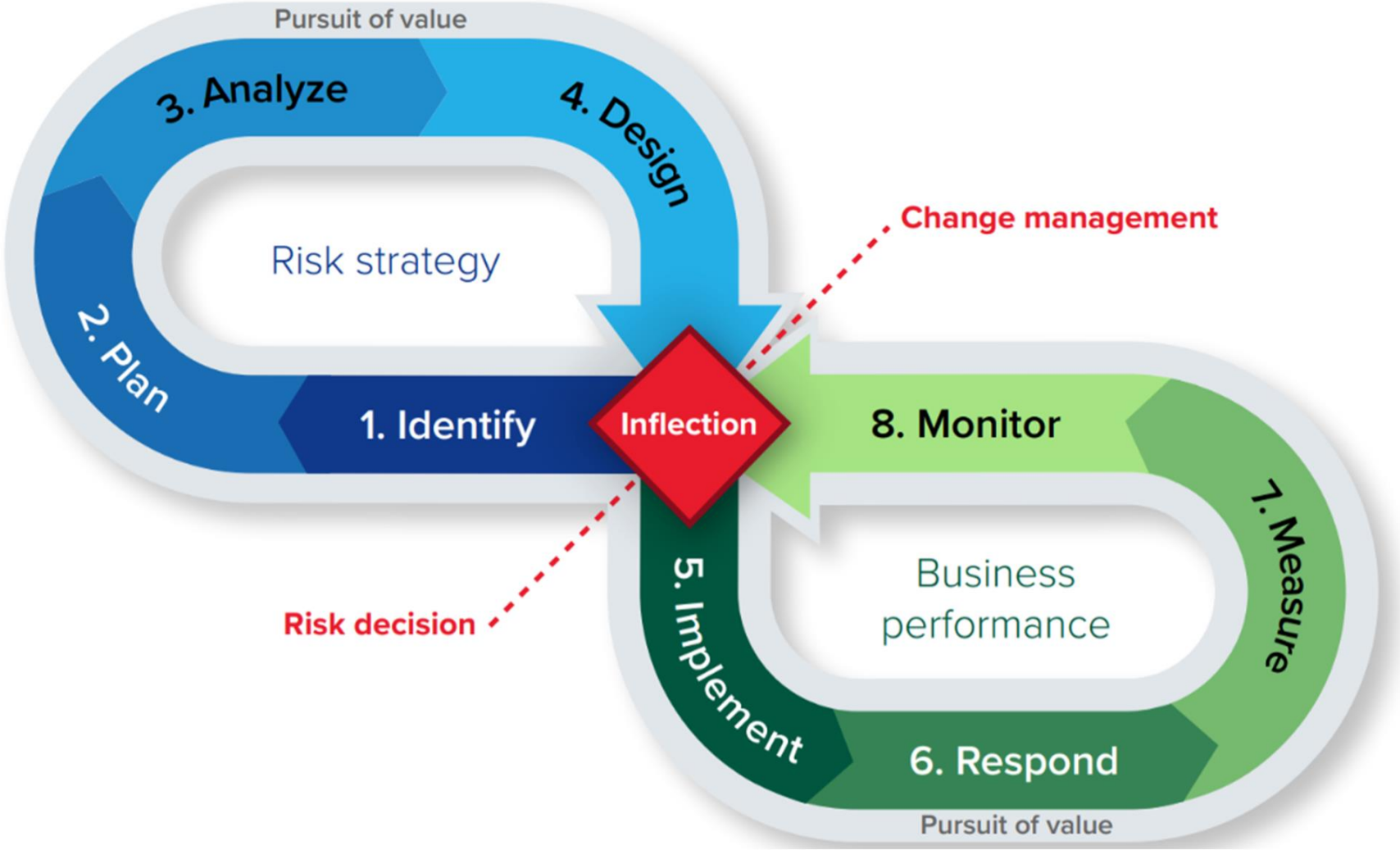
- Good marketing doesn’t prove efficacy!
- Regulatory support doesn’t make it mandatory!
- Present popularity doesn’t equal long-term success!



Every superhero has an origin story


©2022 MARVEL

Introducing the Continuous Risk Management Model



PHASE 1: IDENTIFY

Identify the opportunity and the business need

- What is your pursuit of value?
- What do you intend to accomplish?
- Establish the business case

PHASE 2: PLAN

Plan the risk strategy and governance approach

- Define the key objectives and milestones to achieve your pursuit of value
- What are the risks associated with meeting those objectives?
- Refine the business case with your initial risk assessment

PHASE 3: ANALYZE

Analyze the business context and feasibility

- Assessment and due diligence
- Translating the goal into an attainable project
- Finalize the business case and initial project plans based on risk-informed inputs

PHASE 4: DESIGN

Design the risk mitigation approach

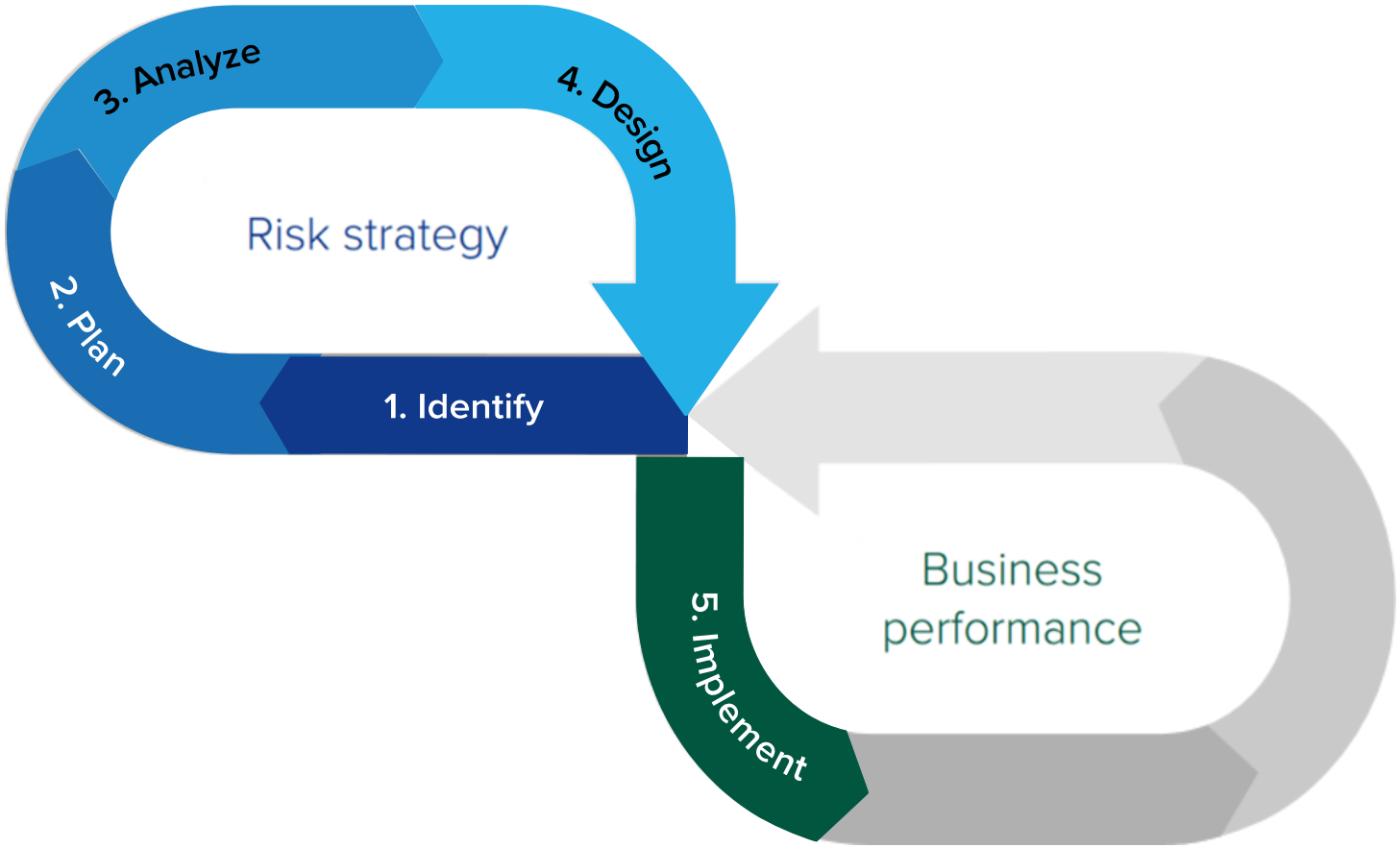
- Identify which risks to accept, transfer, and mitigate
- Incorporate risk mitigation plans into the initial project plan
- Propose an initial control baseline to mitigate identified risks so far

FIRST INFLECTION POINT! RISK DECISION

Risk decisions made earlier

- Risk-based decision to approve the project (pursuit of value) or to go back and revise
- Similar to a formal project approval process – but for risk!
- Communication is key to establish risk and control ownership

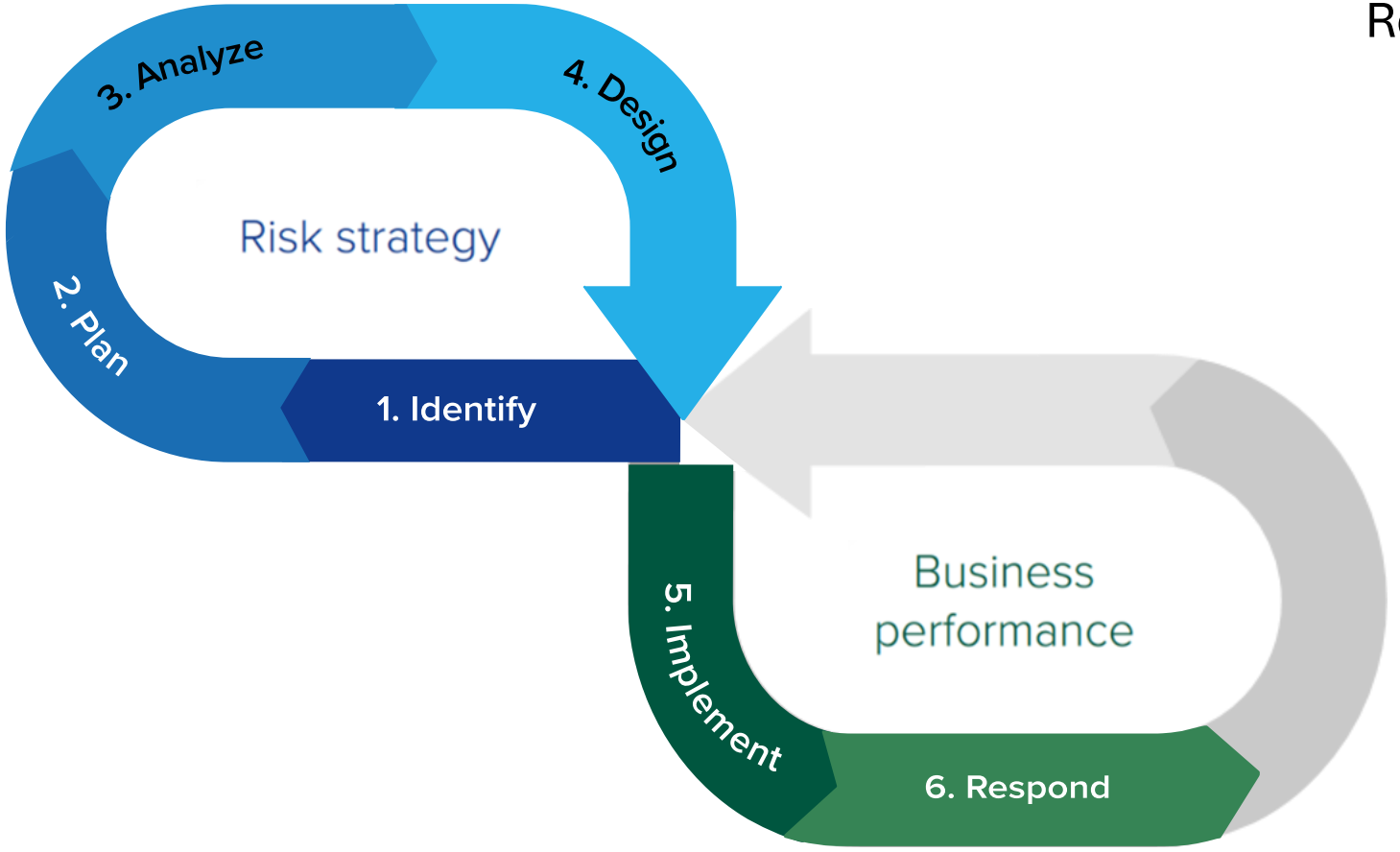
PHASE 5: IMPLEMENT



Implement the appropriate mitigating controls

- The tactical work begins
- What is our success criteria for implementing or augment our controls?
- Integrated teams keep the effort aligned

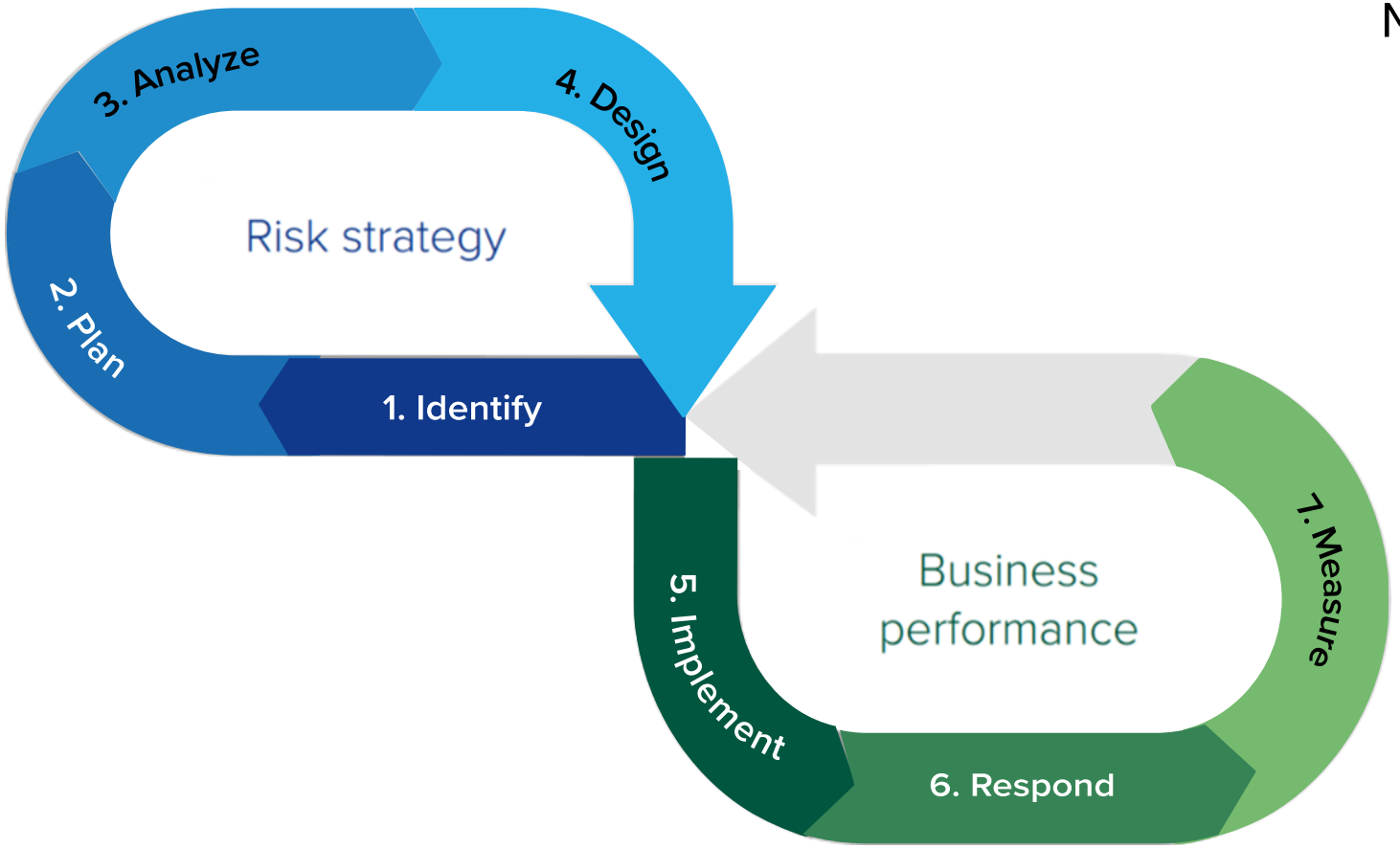
PHASE 6: RESPOND



Respond to deviations from the control baseline

- Change is a constant!
- Are the planned controls still the best option for the job? Has something changed?
- Are additional compensating controls needed?

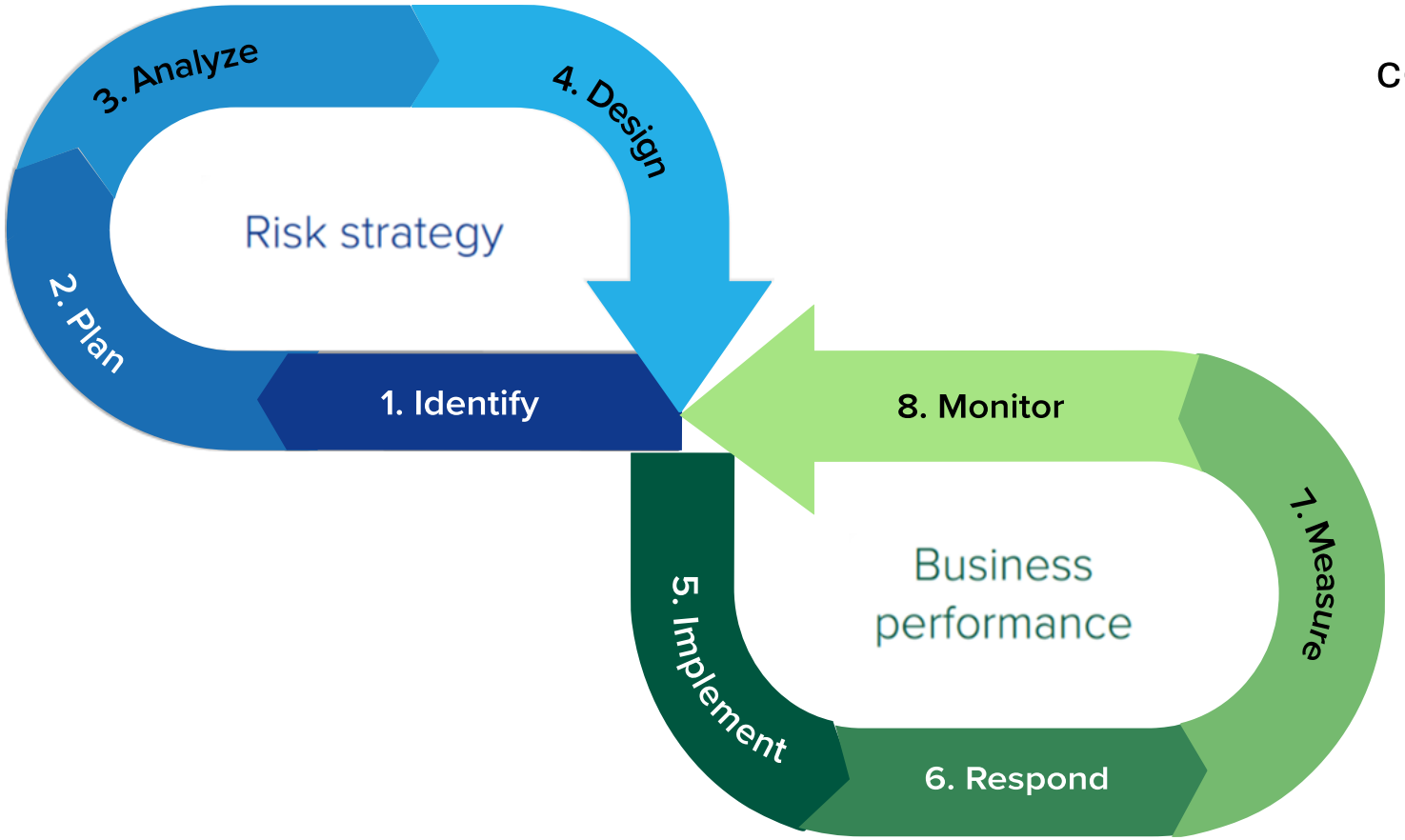
PHASE 7: MEASURE



Measure control effectiveness against expected outcomes

- You need a risk measurement system
- Control coverage is not enough… how effective are your controls at reducing risk to your pursuit of value?
- Are additional compensating controls needed?

PHASE 8: MONITOR

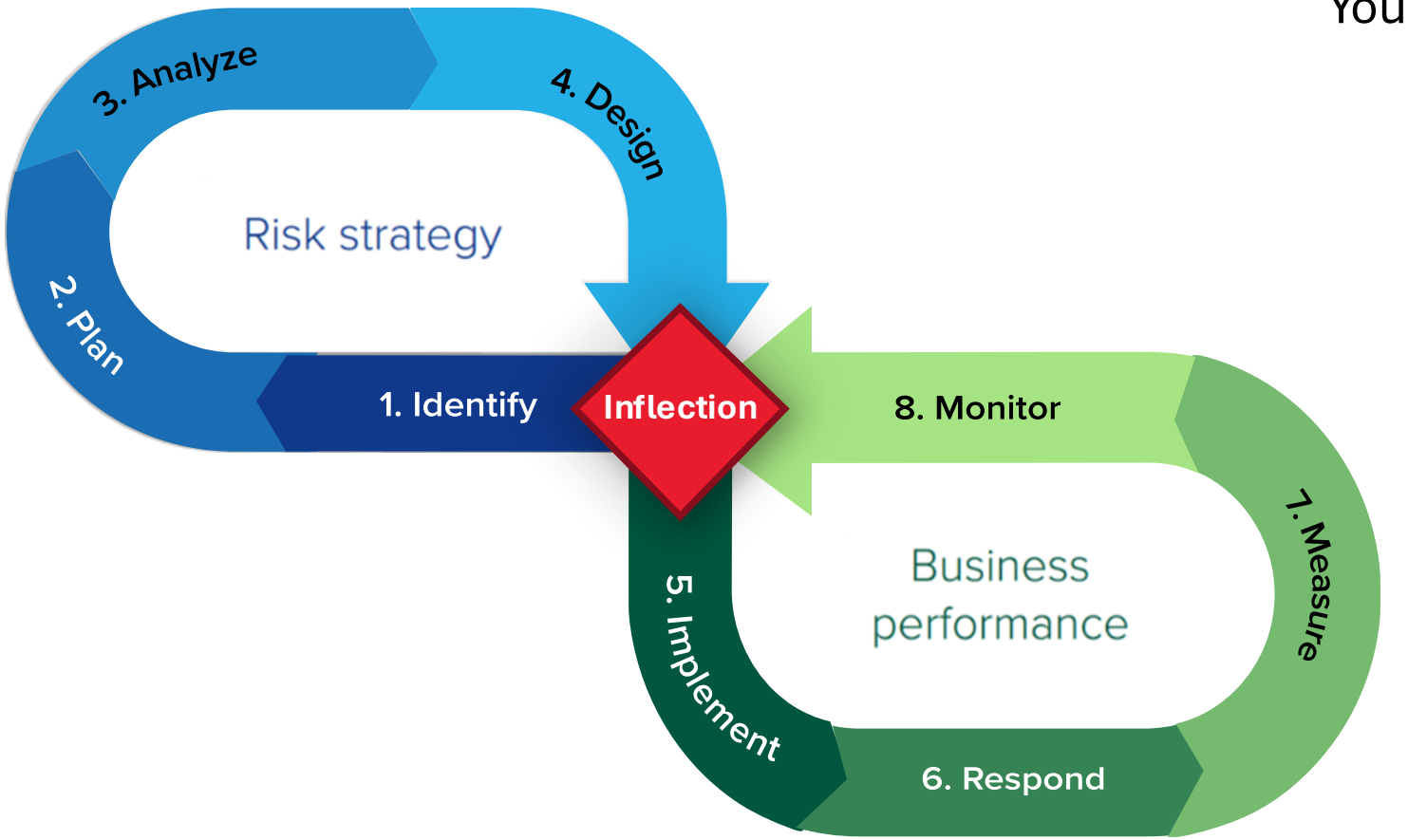


Monitor continuously and communicate to stakeholders

- What signals, metrics, or indicators can you rely on to know if/when to act?
- How well is your control baseline functioning to reduce risk to an acceptable level for the pursuit of value?

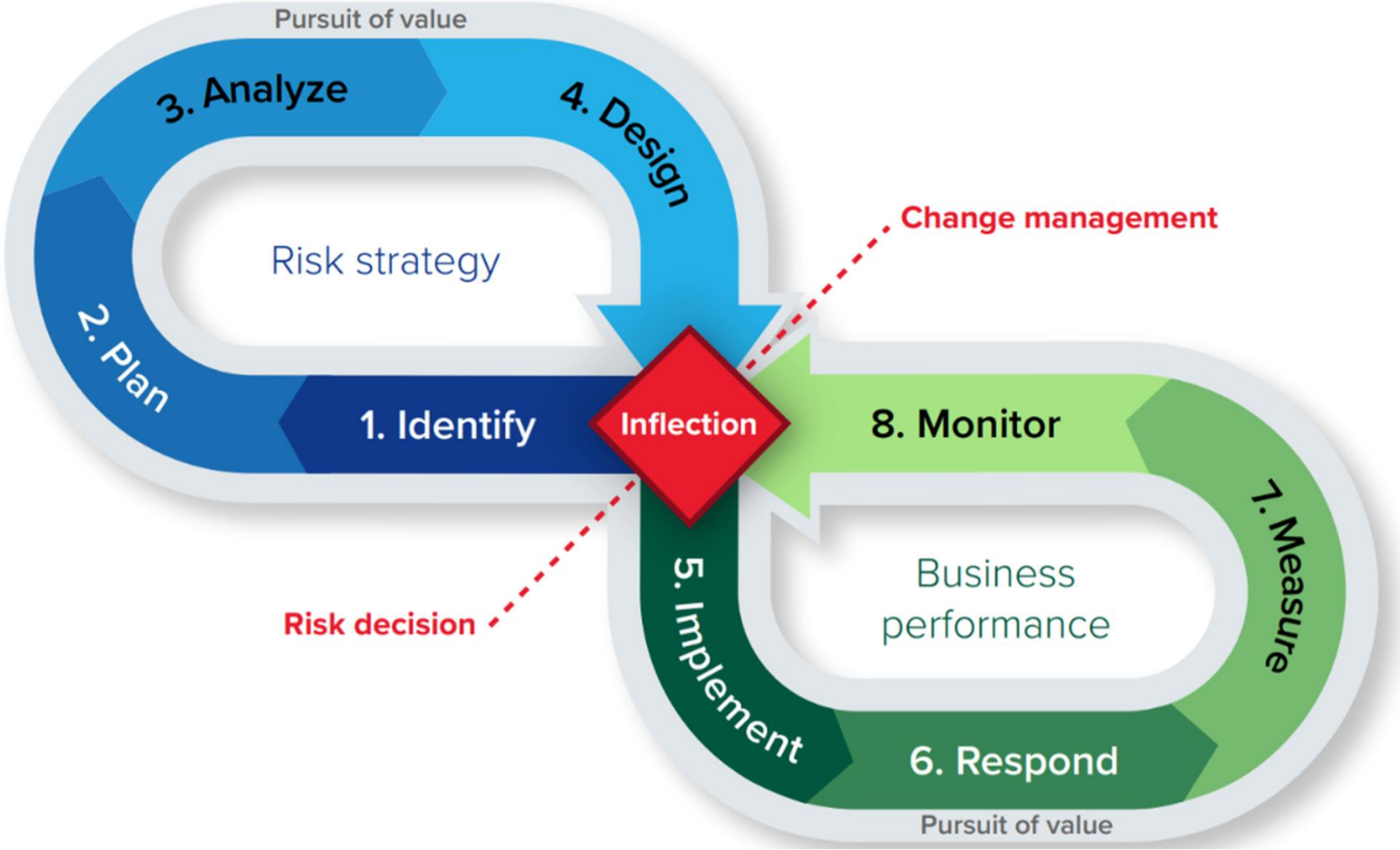
SECOND INFLECTION POINT! CHANGE MANAGEMENT

Your opportunity to make changes



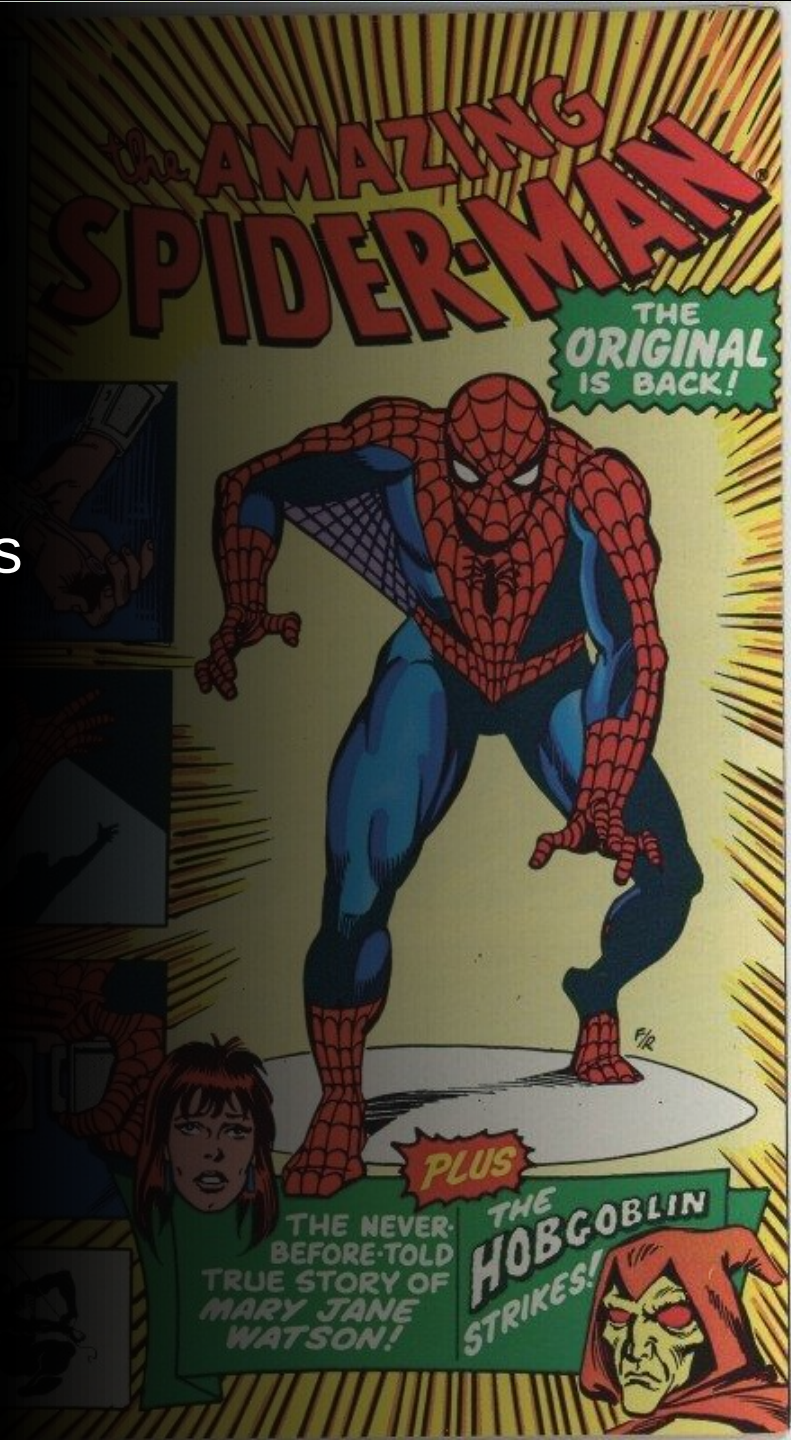
- Change is a constant… and must be managed!
- Avoid the sunk cost trap
- Leverage a risk escalation process
- Are things operating as intended? On schedule? Within budget?

Continuous Risk Management



What it means

- Lead with pursuit of value instead of fear of penalties
- Navigate turbulence/uncertainty for resilient outcomes
- Identify upside opportunities and act on them
- Keep pace with speed of innovation



Every superhero has a sidekick

You have the power to get started!

Use the Continuous Risk Management model to define your ideal GRC end-state

Mirror your technology workflow to your decision workflow

Use 3LOD to right-size your communication and process structure


Questions?

Thank You.

Cody Scott
Senior Industry Analyst

Connect with me on LinkedIn for more research and insights!