

# Governing Cybersecurity Risk

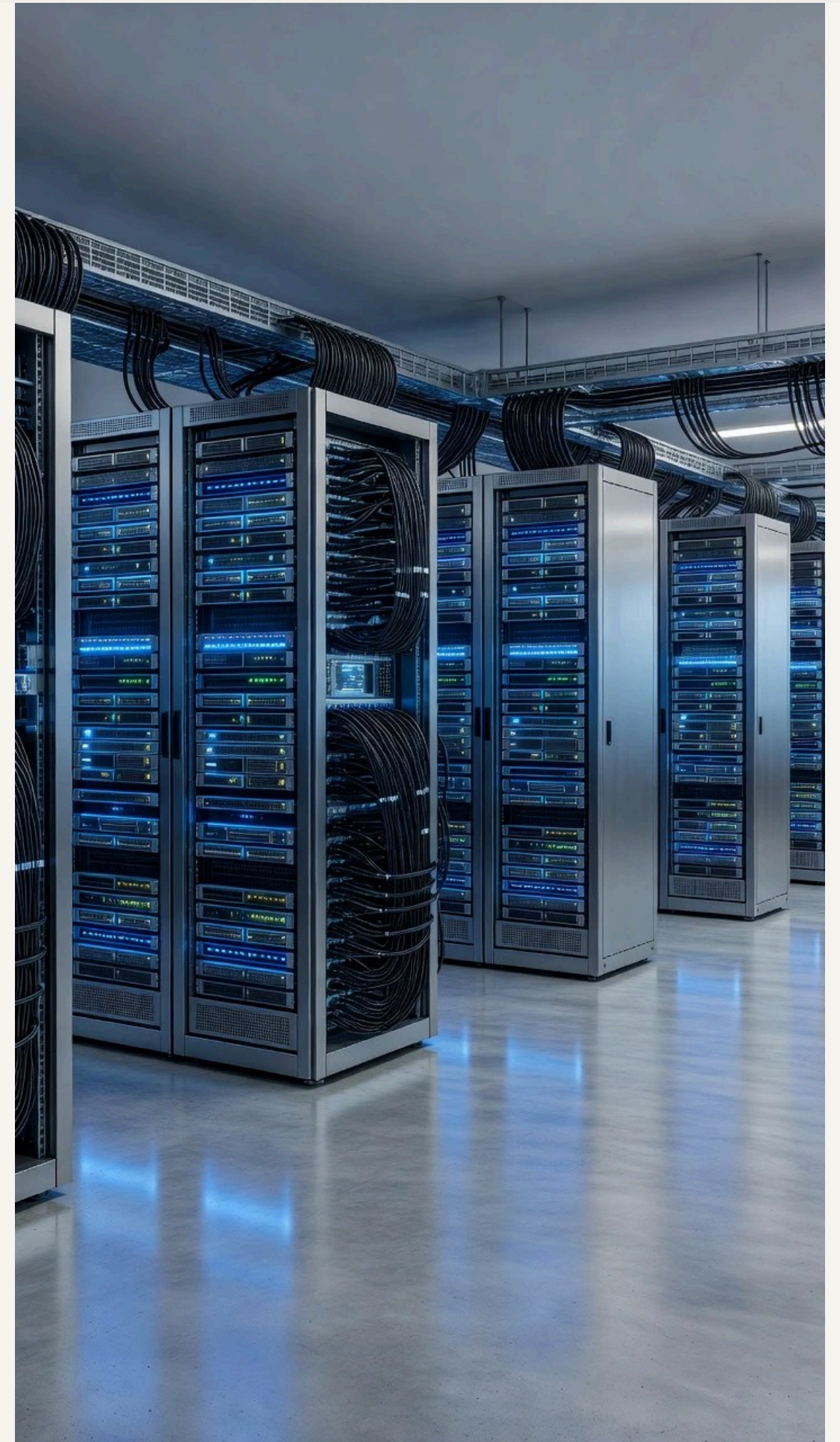
An executive briefing on NIST Cybersecurity Framework 2.0.



# CSF 2.0 gives leaders a common language for cybersecurity risk.

It helps the organisation understand, assess, prioritise, and communicate cybersecurity efforts alongside enterprise risks.

*Use outcomes to connect strategy, resources, and operational action.*



# The framework is designed for every type of organisation.



## **FLEXIBLE BY DESIGN.**

Industry, government, academia, and nonprofit organisations can tailor outcomes to their missions and unique risks.

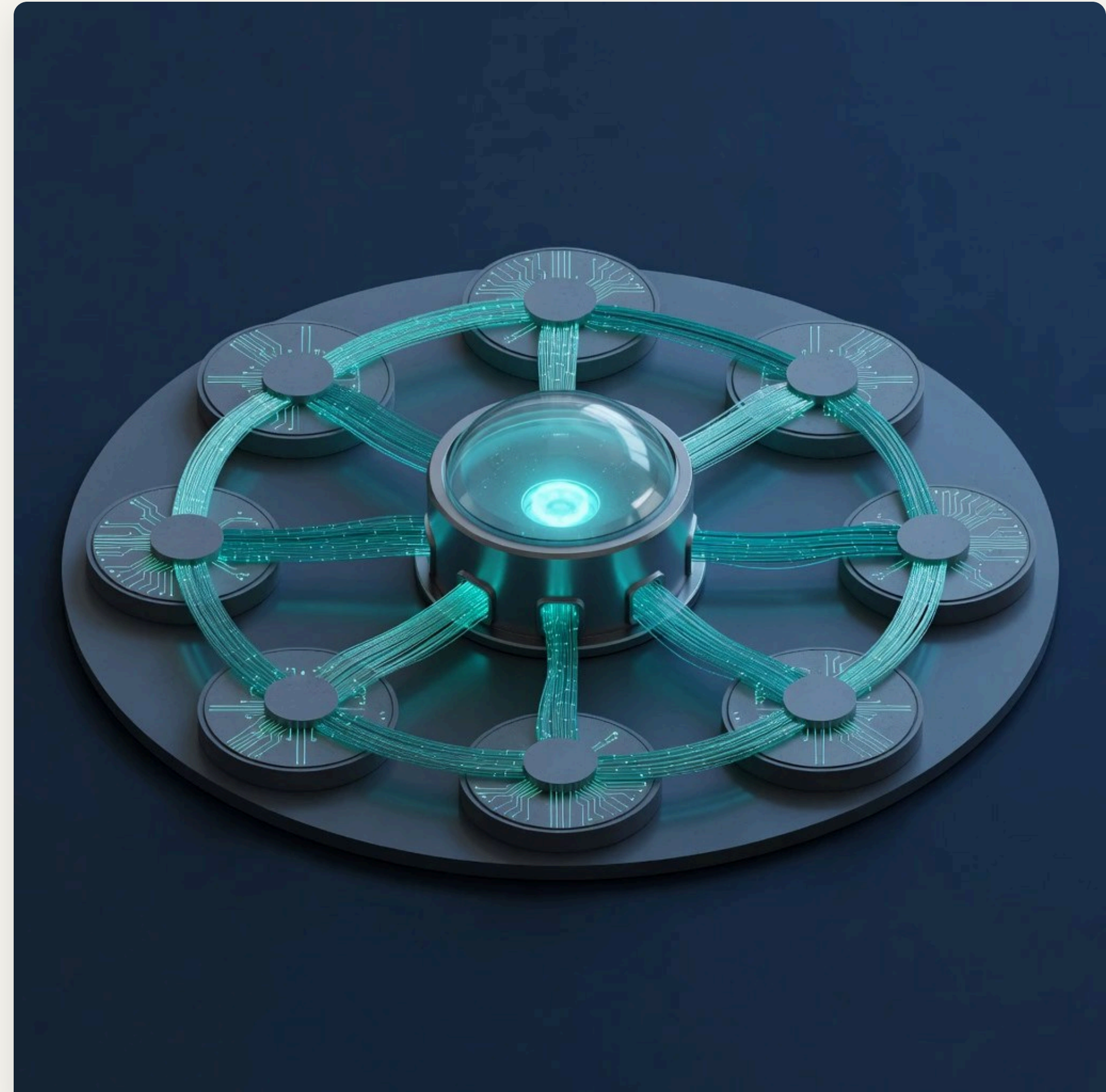
The CSF does not impose one approach.

# Six concurrent Functions organise cybersecurity outcomes.

## GOVERN INFORMS ALL.

**Govern** sits at the centre of Identify, Protect, Detect, Respond, and Recover.

Address all Functions together, not in sequence.



# Govern turns unique risks into organisational direction.



## **Organisational context.**

Understand mission, stakeholders, dependencies, and requirements.



## **Risk strategy.**

Set objectives, appetite, tolerance, and response options.



## **Accountability.**

Establish roles, responsibilities, authorities, and resources.



## **Policy and oversight.**

Communicate, enforce, review, and adjust direction.



## **Supply chain risk.**

Manage supplier and third-party cybersecurity exposure.

# Leaders should test whether governance is actionable.

Ask whether risk objectives, appetite, tolerance, accountability, resources, policy, oversight, and supply chain risk management are established and communicated.

*Expect answers in the organisation's own risk-management terms.*

# Ask teams for evidence that risk decisions reach operations.

- **Mission:** What objectives and services are critical?
- **Risk:** How are risks calculated, prioritised, and tracked?
- **Resources:** Are resources commensurate with the risk strategy?
- **Oversight:** How are performance results used to adjust strategy?

**Profiles show the gap between today's posture and desired outcomes.**

---

## **CURRENT PROFILE**

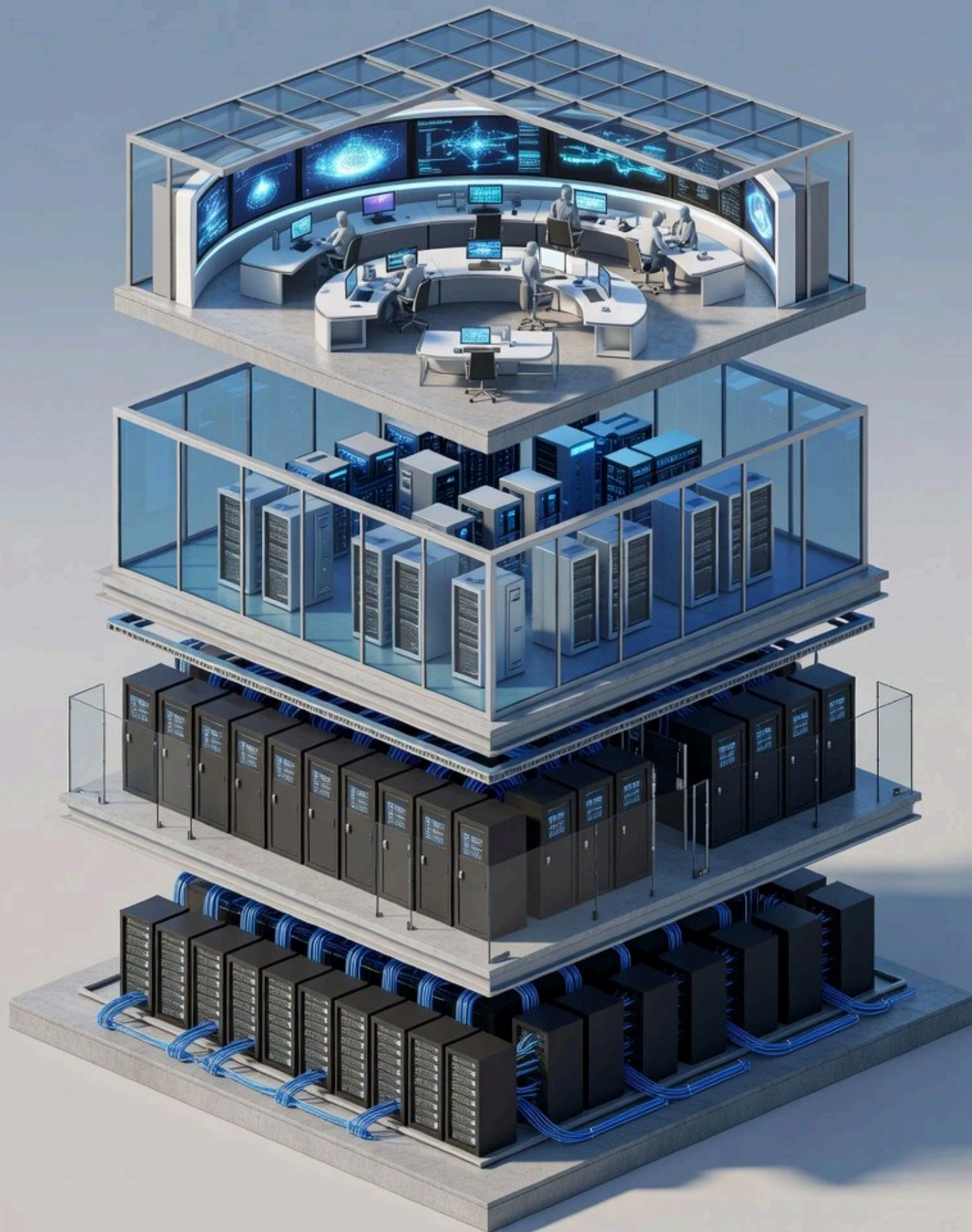
Describes outcomes currently achieved or being attempted.

---

## **TARGET PROFILE**

Prioritises desired outcomes for risk management objectives.

# Tiers characterise the rigor of risk governance and management.



## FOUR CHARACTERISATIONS.

Partial, Risk Informed, Repeatable, and Adaptive describe progression from ad hoc practices to continuous improvement.

Choose rigor that fits risk and organisational context.

# Ask for the profile.

Request Current and Target Profiles, gaps, action plan, and Tier context.