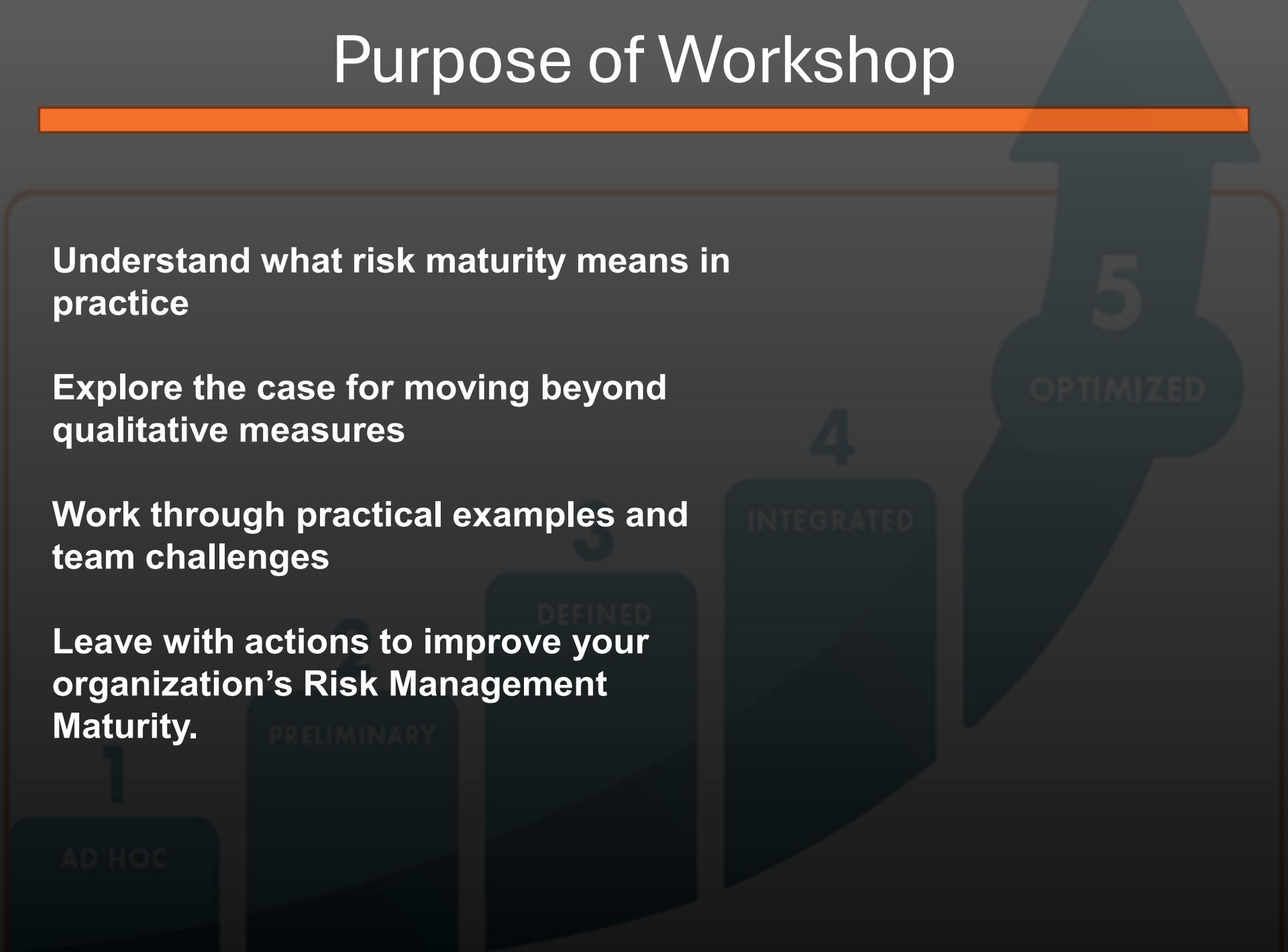


Advancing Risk Maturity through Practical Risk Profiling



Presented by: David Fox
Managing Director of Fox Risk Ltd

Purpose of Workshop



Understand what risk maturity means in practice

Explore the case for moving beyond qualitative measures

Work through practical examples and team challenges

Leave with actions to improve your organization's Risk Management Maturity.

A brief History

What is the current most widely used risk standard?

ISO 31000 – International standard for risk management.

First published on the **13th of November 2009**, revised in 2018.

None of these are aligned to the ISO standard risk management activities.

All were published prior to the current standard.

Published papers on Risk Maturity Models

- *Towards a risk maturity Model – Hilson (1997)*
- *The risk management process maturity model – Chapman (2006)*
- *Understanding and Improving you risk management capability: assessment model for construction organisations – Zou et al. (2010)*
- *Risk maturity model – Cienfuegos et al. (2013)*

Defining Risk Maturity

“Risk maturity is the extent to which an organisation applies structured, consistent, and data-informed approaches to risk management — from governance to operational delivery.”

Risk Maturity Model, correctly called – **Risk Management System Capability Maturity Model.**

Capability

Maturity

Model

- Specific attributes of an organisation, enabling it to collectively deliver organisation objectives in the face of threats and to leverage opportunities.
- The current or future state, fact or period of evolving development, quality, sophistication and effectiveness of attributes characteristic of that organisation.
- Model represents a simplified description of a system or process to assist evaluation, calculations or prediction. It is typically repeatable and testable over time.

Risk Management System

Why do we have the concept of risk management?

*To systematically improve our **organisation's capability** to identify and control the uncertainty that matters, which protects assets, improves performance and ensures long-term viability*



So how do we know if our organisation's capability in the Risk Management framework, matches our desired level of risk management?

Spot the difference

R M Logistic– risk heat map.



R M Logistics latest audit highlighted a very low risk management capability.

A to Z Logistic – risk heat map.



A to Z Logistics latest audit highlighted a high competency in risk management capability.

How Maturity Is Typically Measured

- **1–5 Scale (Ad hoc → Optimised):**

- This scale ranges from 1 (Ad hoc) to 5 (Optimised), indicating the level of maturity in risk management practices.

- **Focus Areas:**

- Governance, process, culture, and data are the key areas assessed to determine maturity.

- **Common Method:**

- Qualitative, self-scored checklists are the most frequently used method for assessing maturity.



Challenges: These models are often used without calibration or strategic linkage, leading to inconsistencies and a lack of alignment with organisational goals.

Why Quantify?

Clear evidence of progress over time.

- Quantified measurements provide a clear and objective way to track progress, ensuring that improvements are visible and measurable.

Builds Trust with Executives, Auditors, and Stakeholders

- Quantified data builds credibility and trust, as it provides concrete evidence that can be easily verified and audited.

Enables Benchmarking Across Teams, Functions, and Sectors

- Quantitative metrics allow for consistent benchmarking, making it possible to compare performance across different teams, functions, and sectors.

Supports Focused Investment and Targeted Uplift

- With clear metrics, you can identify areas that need improvement and allocate resources more effectively to achieve targeted uplift.

Quote: “Measurement systems drive behaviour — maturity tools should too.”

Case Example – Infrastructure Client

Problem: All teams scoring themselves as 3–4, despite rising incidents.

Approach: Applied quantitative measures against ISO-aligned model attributes.

Sample of Metrics used: % of risks reviewed quarterly, % of leadership decisions supported by risk analysis, % of treatments with assigned owners.

Result: Risk capability dashboards introduced in each team's report, maturity tracked, audit confidence improved, measurable uptick in performance.

If control effectiveness is measured via assurance reviews, why do you not measure your biggest risk control... the Risk Management System itself?

Where We Measure Maturity

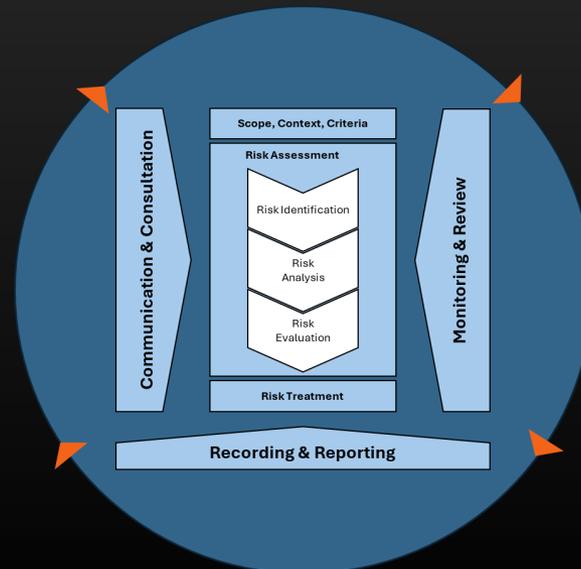
ISO 31000-2018: Framework

Leadership, Integration, Design, Implementation, Evaluation, Improvement.

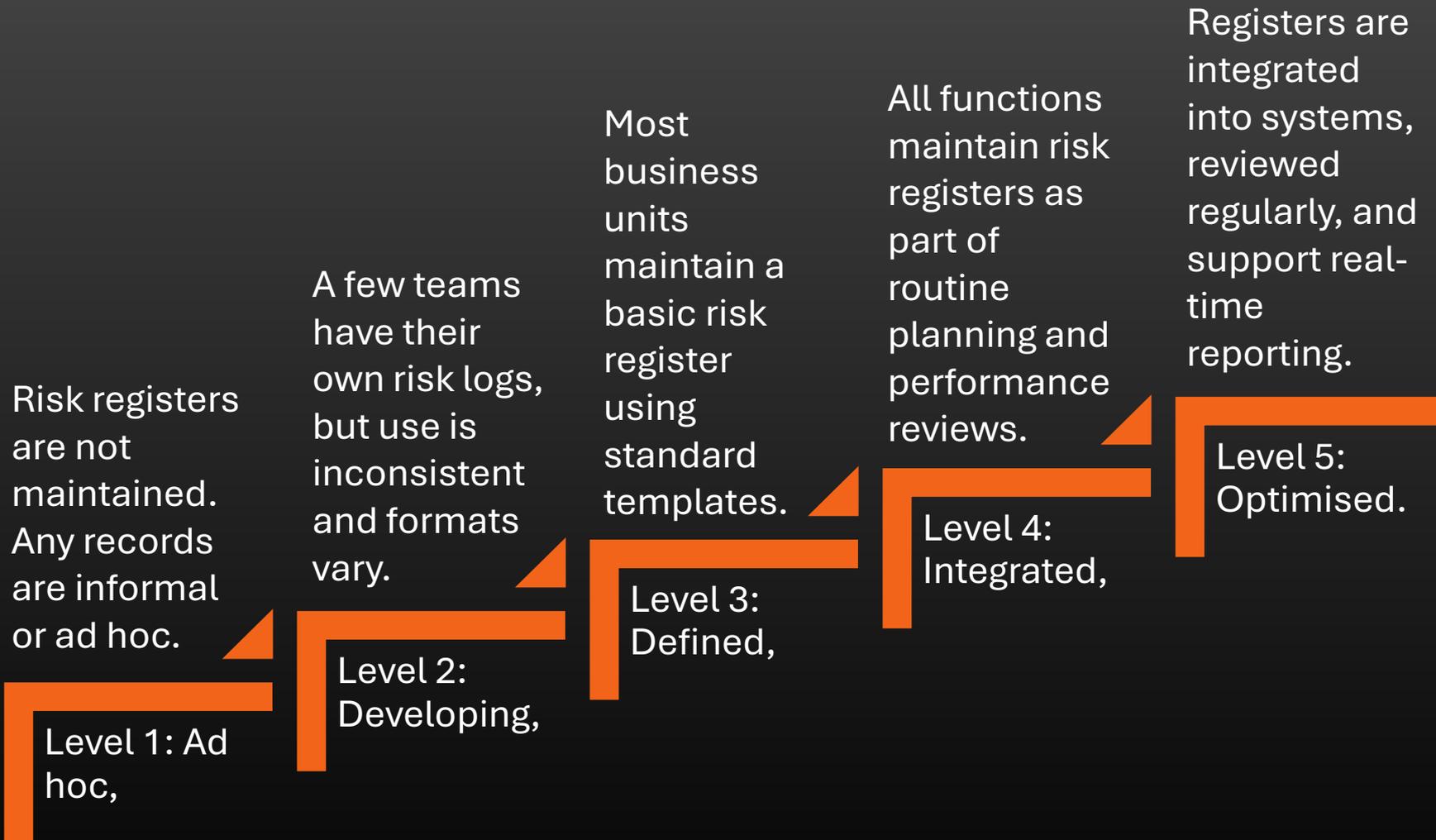


ISO 31000-2018: Risk Process

Communication, Context, Assessment, Treatment, Monitoring, Recording.



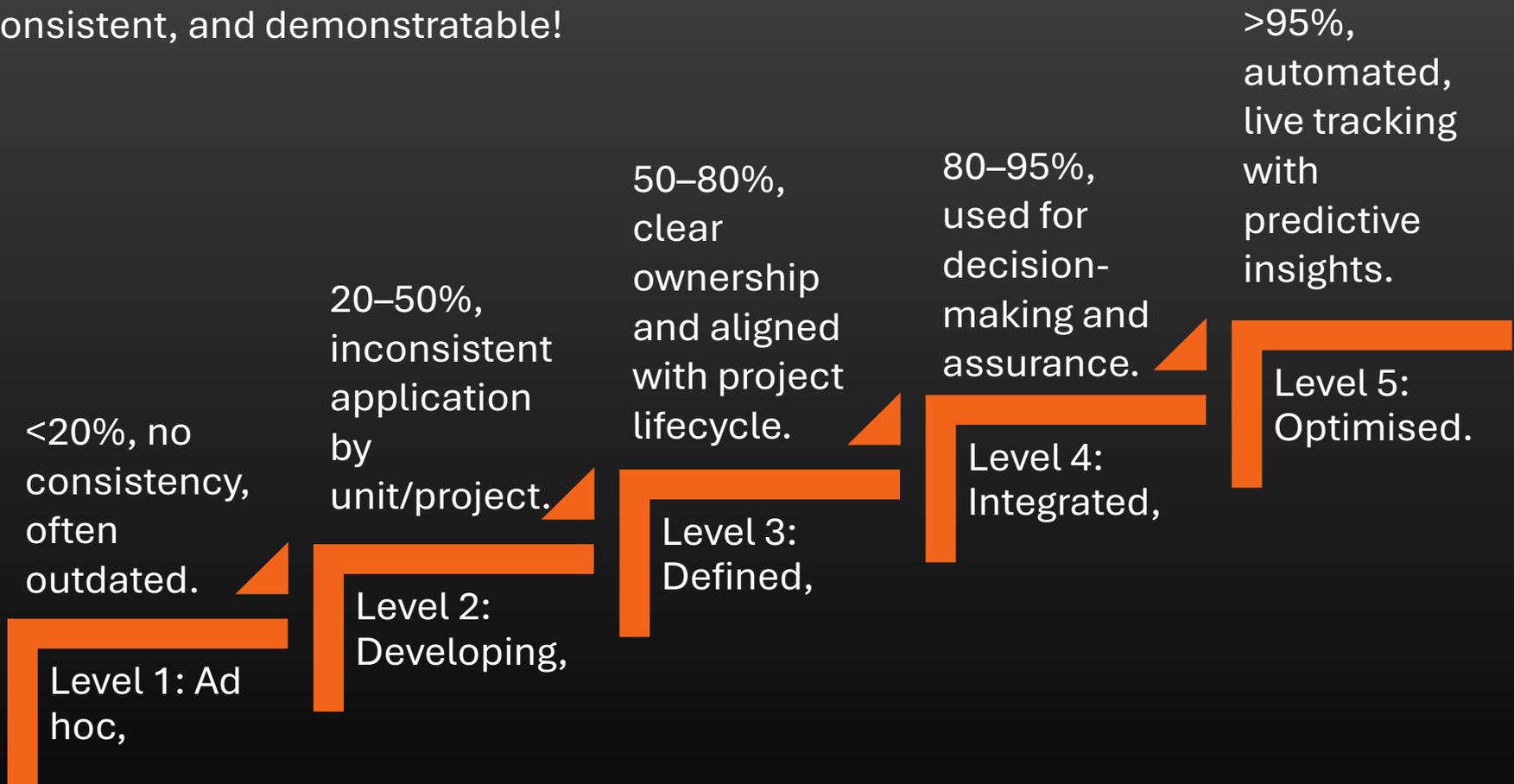
From Metrics to Maturity



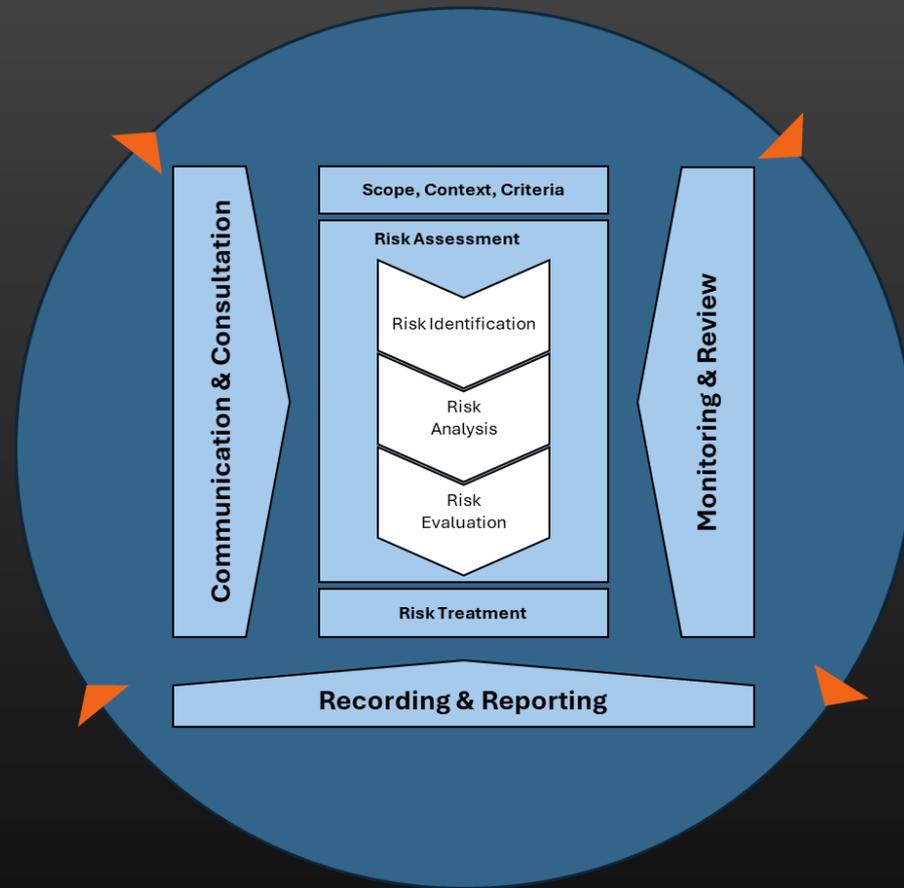
Example: Application of Risk Registers in Business Units.

From Metrics to Maturity

Making Progress objectively measurable, consistent, and demonstratable!

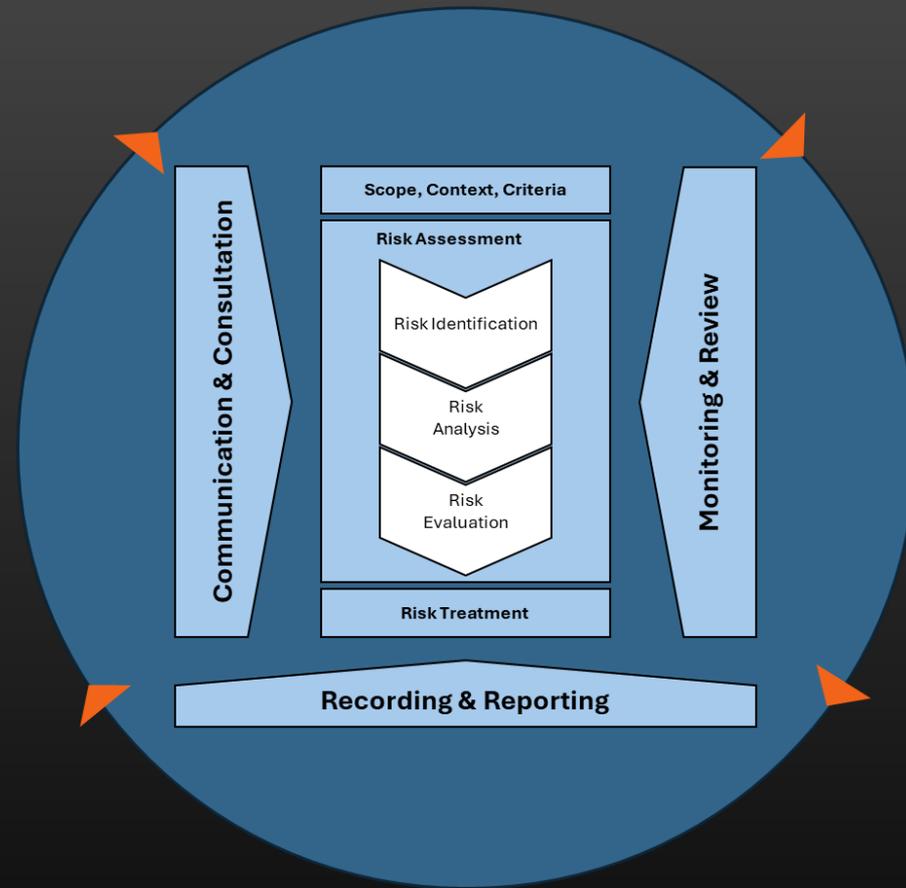


Group Exercise 1.



Pick two ISO 31000 attributes and identify a quantifiable measurement for each, and scale it for a 1–5 maturity scale.

Group Exercise 2.



Pick an organisation and score it on your scale (can be imaginary),
Identify one strength, one gap based on the score,
Be honest — not everything is a 3!

Turning Maturity Into Action

What low maturity tells you:



Identifies gaps, risk blind spots, opportunity cost

What high maturity enables:



Provides foresight, agility, trust

Start with a key area:



Focus such as monitoring, integration, or treatment

Key Question: “Which attribute do we most need to lift?”

Scenario: What If You Scored a 2?



: Developing

You've just been scored a 2 for Implementation of your ERM Framework Implementation. **The Board wants it raised to level 3 in the next quarter.**

How will you improve this in 90 days?

Team Task:

- Define two metrics to measure ERM Implementation for level 2 & 3 only.
- Decide on 3 actions to move from a level 2 to the level 3.
- Which executive stakeholder should lead this plan?

Examples:

% of management staff who can articulate their role in the ERM framework

% of business units reporting risk metrics (tracking their own risk KRIs)

What Will You Take Back?



Risk maturity is a catalyst for continuous improvements



Quantitative models bridge strategy, behaviour, and measurable outcomes.



Reflect: What actionable insight can I implement tomorrow to enhance my organisations Risk Management Capability Maturity?”

Remember: *Quantified measurements provide clear evidence of progress and build trust, while subjective qualifications can lead to inconsistencies and lack of accountability.*

Thank you

NEW ZEALAND

**RISK & RESILIENCE
SUMMIT**



TOGETHER WE SHAPE OUR FUTURE

