

HIGHLIGHT THE VALUE OF YOUR ESRM PROGRAM WITH OBJECTIVE-CENTRIC RISK MANAGEMENT



Bruce McIndoe, President
McIndoe Risk Advisory LLC
Bruce@McIndoeRiskAdvisory.com

LEARNING OBJECTIVES...

- **#1:** Gain knowledge of and how to apply Objective-Centric Risk Management to clearly articulate the organizational objective linkage and value of your ESRM program
- **#2:** Explore how the multi-disciplinary risk assessment helps drive protective services (physical & cyber security) collaboration and clearly articulates investments and residual risk to the objective owner
- **#3:** Apply the 5-Step Objective Centric & Internal Audit Process within your ESRM program

OUR TIME TODAY...

- **The Backstory** – confluence of events and frustrations
- **Intro to Objective-Centric Risk Management** – clear linkage of our work & investments to the Organization's value-generating Objectives
- **Operational Resilience** – working together as a Joint Force, developing multidisciplinary personnel and continuous risk management, preparation & response
- **BONUS – PSMM** – Standardized approach to measuring and improving our combined operations – People, Physical and Information Protection.

THE BACKSTORY ...



Don't understand &
confused



What worked



What doesn't

ATTRIBUTES OF WHAT WORKED...

- Joint Team of multidisciplinary experts
- Common mission – clear objectives
- Sharing information – everyone on the same page
- Agile approach – test approach, implement or fix
- Rapid decision making
- Executive engagement
- Broad and consistent communications

Go Deeper: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/responding-to-coronavirus-the-minimum-viable-nerve-center>

OBJECTIVE-CENTRIC RISK MANAGEMENT

Common mission – clear objectives – joint effort

Go Deeper: <https://riskoversightsolutions.com/resources/>

WHAT IS RISK?

As per ISO 31000 - Risk Management, risk is
"The effect of uncertainty on **objectives**"

Per COSO, "...the possibility that events will occur and
affect the achievement of strategy and business
objectives."

Risk Management reduces UNCERTAINTY of achieving business objectives

"We are in the CERTAINTY management business"

ENTERPRISE RISK MANAGEMENT (ERM)

ERM is a process-driven tool that enables the board and senior management to visualize, assess, and manage significant risks that may adversely impact the attainment of **key organizational objectives**.

*“A process, effected by an entity’s board of directors, management, and other personnel, designed to **provide reasonable assurance regarding the achievement of objectives** relating to operations, reporting, and compliance.”*

COSO ERM

*“... a strategic business discipline that **supports the achievement of an organization’s objectives** by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.”*

RIMS ERM

ALIGNING ERM AND ESG



- Environmental, Social, & Governance (ESG)
- Governance, Risk & Compliance (GRC)
- Both sets of principles focus on identifying and addressing the risks to long-term organizational success

Go Deeper: <https://grc2020.com/2021/07/08/es-g-rc-the-role-of-grc-in-delivering-esg/>

OBJECTIVE-CENTRIC RISK MANAGEMENT (O-CRM)

The objective-centric approach facilitates better integration of risk and strategy, and their alignment with the organization's vision and mission.

“With the objective-centric approach, risk assessment is driven by the **Objectives** set from the top (the Board and Senior Management) ensuring the integration of risk and strategy, as well as their alignment with the organization's vision and mission.”

Go Deeper: <https://insterp.com/towards-an-objective-centric-approach-to-risk/>

THE LIST-BASED RISK REGISTER

Effects of Sample Treatments on Scoring in the Risk Register

	Risk Item	Rationale for Inherent Risk	Inherent Risk			Risk Treatment	Residual Risk		
			Likelihood	Impact	Risk Score		Likelihood	Impact	Risk Score
Accept the risk →	Laptops break down during their useful lives.	x% printer replacement cost attributable to replacements made ahead of schedule.	1.0	1.0	1.0	Scheduled replacement precludes the need to extend laptop lives. Accept the risk of the cost of premature failure and replacement.	1.0	1.0	1.0
Reduce the risk →	Injuries incurred during operations.	x% accident rate with \$y annual cost of claims.	3.0	2.0	6.0	Develop and implement tested, proven safety protocol X.	2.0	1.0	2.0
Reduce the risk →	A major supplier fails to deliver materials	X% of raw materials purchases concentrated in a single supplier.	4.0	3.0	12.0	Spread raw materials purchases over x suppliers with no more than y% of purchases concentrated in any one supplier.	1.0	3.0	3.0
Transfer the risk →	The organization experiences a flood.	Property coverage excludes flood coverage.	3.0	3.0	9.0	Extend property insurance to provide coverage for floods. (Residual impact is the additional premium.)	3.0	1.0	3.0
Transfer the risk →	Extra costs incurred due to installation difficulties.	Annual costs of \$x for installation remediation and \$y for installation administration.	3.0	3.0	9.0	Outsource installation service. (Residual impact is the outsource cost.)	2.0	1.0	2.0
Avoid the risk →	A new product does not prove to be profitable.	Anticipate x% market penetration for \$yy revenue versus \$YY operational cost and \$ZZZ capitalized cost.	5.0	4.0	20.0	Do not develop the product.	0.0	0.0	0.0

This is what Leadership and the Board traditionally get from the Risk Assessment process...

There is NO CONTEXT around the mission or objectives that these “Risk Items” relate to.

Difficult for leadership to frame and comment.

Go Deeper: <https://normanmarks.wordpress.com/2021/01/10/what-is-wrong-with-a-typical-risk-register/>

CONNECTING OUR WORK TO OBJECTIVES IN 5 STEPS

1. Populate an Objectives Register

Top Value Creation & Preservation Objectives by the BoD & Executives

2. Assignment of Ownership

Objective Owner/Sponsors, ID “Risk Assessment Rigor” & Assurance Level Targets

3. Confirm Decisions

Objectives Register, Risk Assessment Rigor & Independent Assurance levels w/BoD

4. Integrated Risk Assessment & Independent Assurance

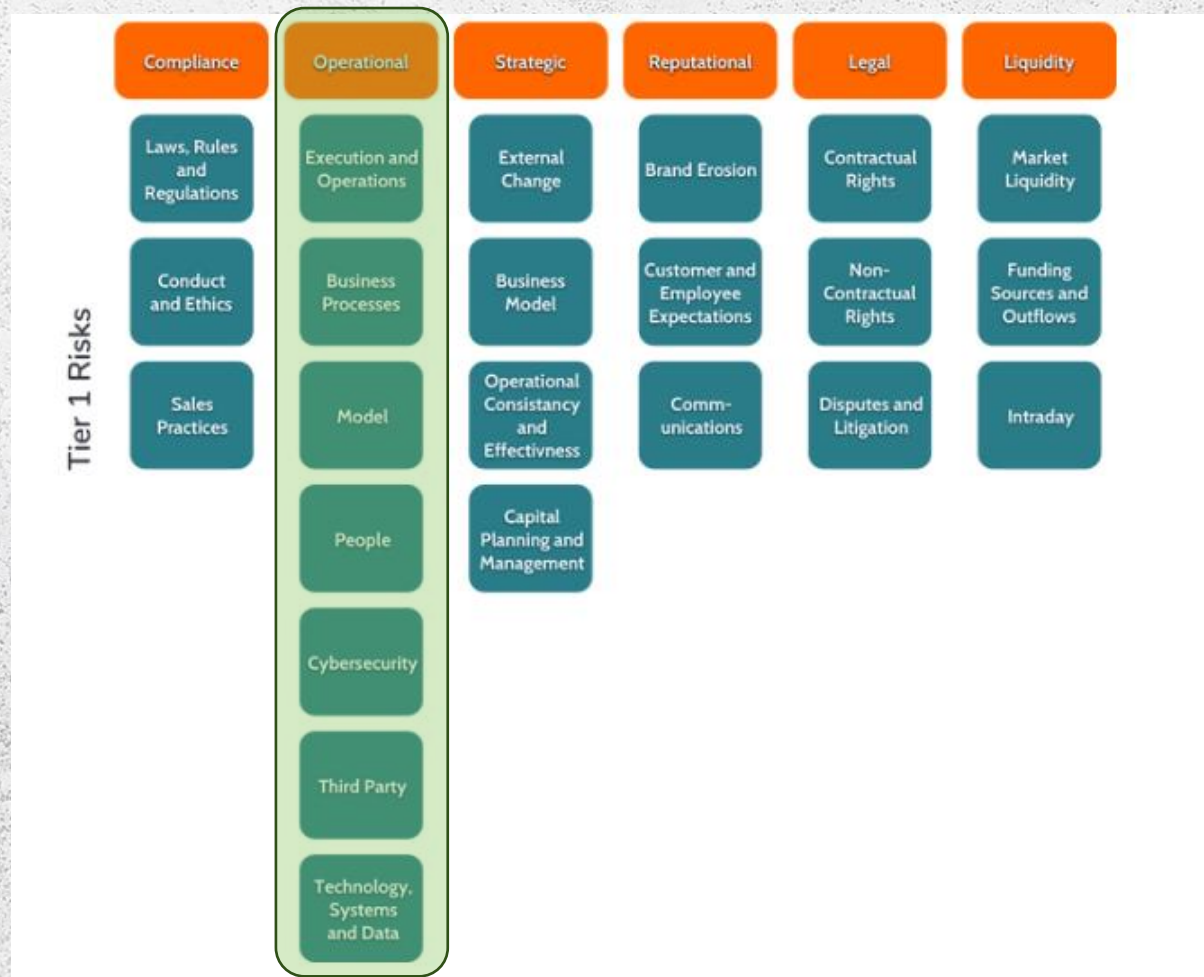
Complete integrated Risk Assessment and internal audit for independent assurance

5. Consolidated Report

Include “Composite Residual Risk Ratings” prepared for Executives & BoD

Go Deeper: <https://insterp.com/towards-an-objective-centric-approach-to-risk/>

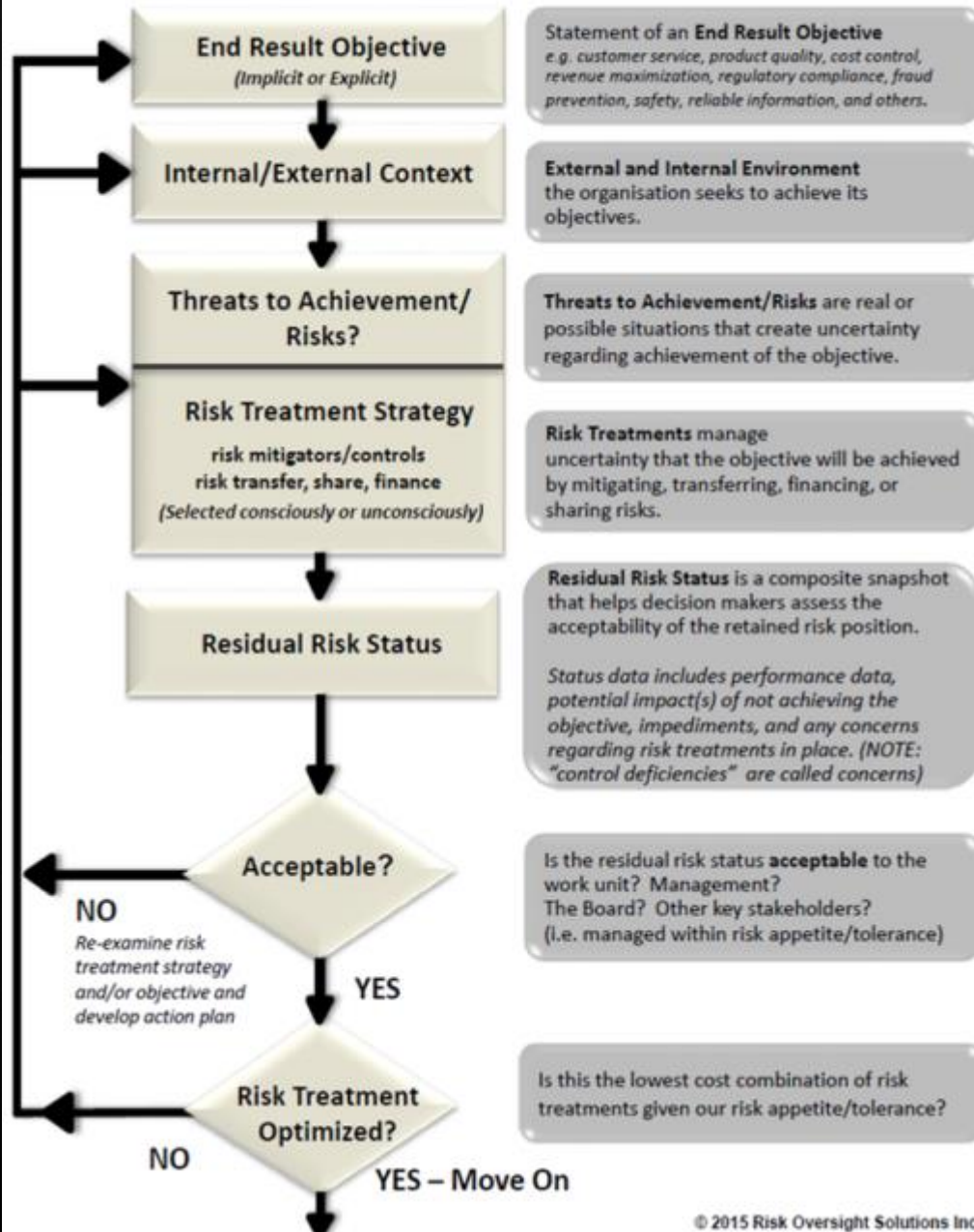
EXAMPLE ERM RISK TAXONOMY



360-Degree Risk Assessment

- 6 Risk Categories
- Tier 1 - Subcategories are organization specific

Our focus is on Operational Risk within the 360-degree ERM Risk Assessment for an Objective.



Each Objective gets a Risk Assessment

- End Result Objective “Owner/Sponsors” are the primary risk assessor/reporters not risk specialists or internal audit
- **Risks are assessed collectively** in terms of their composite effect on achieving the objective
- **Agree on current retained risk** acceptability
- **Determine if risk treatment is optimized** – lowest possible cost combination that would still provide an acceptable residual risk

COMPOSITE RESIDUAL RISK RATING DEFINITIONS

- 0 Fully acceptable** Composite residual risk status is acceptable. No changes to risk treatment strategy required at this time. (NOTE: this could mean that one or more significant risks are being accepted. Information on accepted concerns is found in the residual risk status information)
- 1 Low** Inaction could result in very minor negative impacts. Ad hoc attention may be required to adjust composite residual risk status to an acceptable level
- 2 Minor** Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust composite residual risk status to an acceptable level
- 3 Moderate** Inaction could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust composite residual risk status to an acceptable level
- 4 Advanced** Inaction could allow continuation of/or exposure to serious negative impacts. Senior management attention required to adjust composite residual risk status
- 5 Significant** Inaction could result in or allow continuation of very serious entity level negative impacts. Senior management attention urgently required to adjust composite residual risk status to an acceptable level
- 6 Major** Inaction could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately
- 7 Critical** Inaction virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately
- 8 Severe** Inaction virtually certain to result in or allow continuation of very severe negative impacts. Senior management/board-level attention urgently required to adjust composite residual risk status
- 9 Catastrophic** Inaction could result in or allow the continuation of catastrophic proportion impacts. Senior management/board level attention urgently required to adjust composite residual risk status and avert a catastrophic negative impact on the organisation
- 10 Terminal** The current composite residual risk status is already extremely material and negative and having disastrous impact on the organisation. Immediate top priority action from the board and senior management required to prevent the demise of the entity

Residual Risk Ratings are a key input to assessing & prioritizing Risk Appetite by Management and the BOD.

OBJECTIVES RISK REGISTER

An Objectives Risk Register with top value creation/strategic objectives and top value preservation objectives provides the foundation for all ERM and internal audit work.

Gives the Board and Executives much needed context.

Corporate	Description	End Result Objective Owner / Sponsor(s)	Composite Residual Risk Rating (CRRR)	CRRR Update Date	Potential to Increase Entity Value	Potential to Erode Entity Value	Current Risk Assessment Rigor (RAR)	Independent Assurance Level (IAL)
	Ensure that financial statements are reliable and in compliance with GAAP.	CEO	6 - Major	6/12/2014	Medium	Low	Medium (M)	LOW
	Safeguard and enhance ABC's reputation	CEO	4 - Advanced	6/10/2014	High	High	Very Low (VL)	MEDIUM

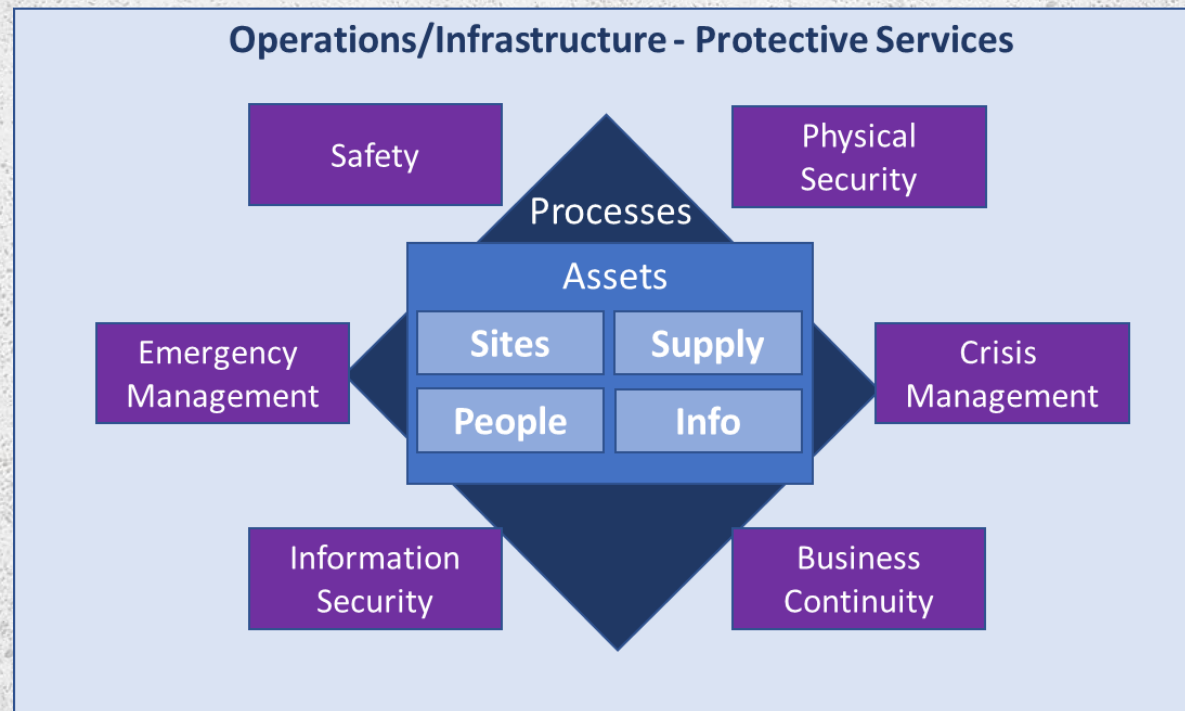
Drives an informed conversation around Risk Appetite

WHY IS OC-RM DIFFERENT/BETTER?

- **Management/business units are the primary risk assessor/reporters** – establishes clear accountability for risk acceptance decisions, “embeds” risk management in the business, and leads to better decisions
- **Technically superior** in terms of identifying the true residual/retained risk position linked to top objectives
- **Links all risk assessment & treatment work to top strategic and value preservation objectives**, current performance being achieved, and impact information

THE INTEGRATED RISK ASSESSMENT DRIVES COLLABORATION

**Collaborative Joint Force with Multi-Capable
Protective Personnel all aligned to ONE joint mission**



OPERATIONAL RESILIENCE

Operational resilience is both a process and a characteristic of an organization to adapt rapidly to changing environments and needs.

It is an organizational trait that allows an organization to carry out its mission or business despite the presence of operational stress and disruption.

It is not...

“initiatives that expand business continuity management programs”

ORGANIZATIONAL TRAITS

- Prepared
- Adaptable
- Collaborative
- Trustworthy
- Responsible



Go Deeper: <https://hbr.org/sponsored/2021/03/5-traits-of-resilient-organizations>



Organizational Objectives

Enterprise Risk Management

Operational Risk Management

POWERED BY
ASIS
INTERNATIONAL

Creating a straight line from Objectives to investments and on-going risk management to ensure the certainty of achievement.

Operational Resiliency

People

Sites

Supply

Info

Assets

Processes

EM/CM
Communications

Safety &
Physical Security

Business
Continuity

Information
Systems

HR & Training

Mobility

Operations/Infrastructure (Protective Services)

OUR TRIBAL IDENTITIES

POWERED BY
ASIS
INTERNATIONAL



**Enterprise
Risk Management**



Operational Resilience

BUSINESS RESILIENCE



**Enterprise Security
Risk Management**



WE CAN NO LONGER OPERATE IN SILOS

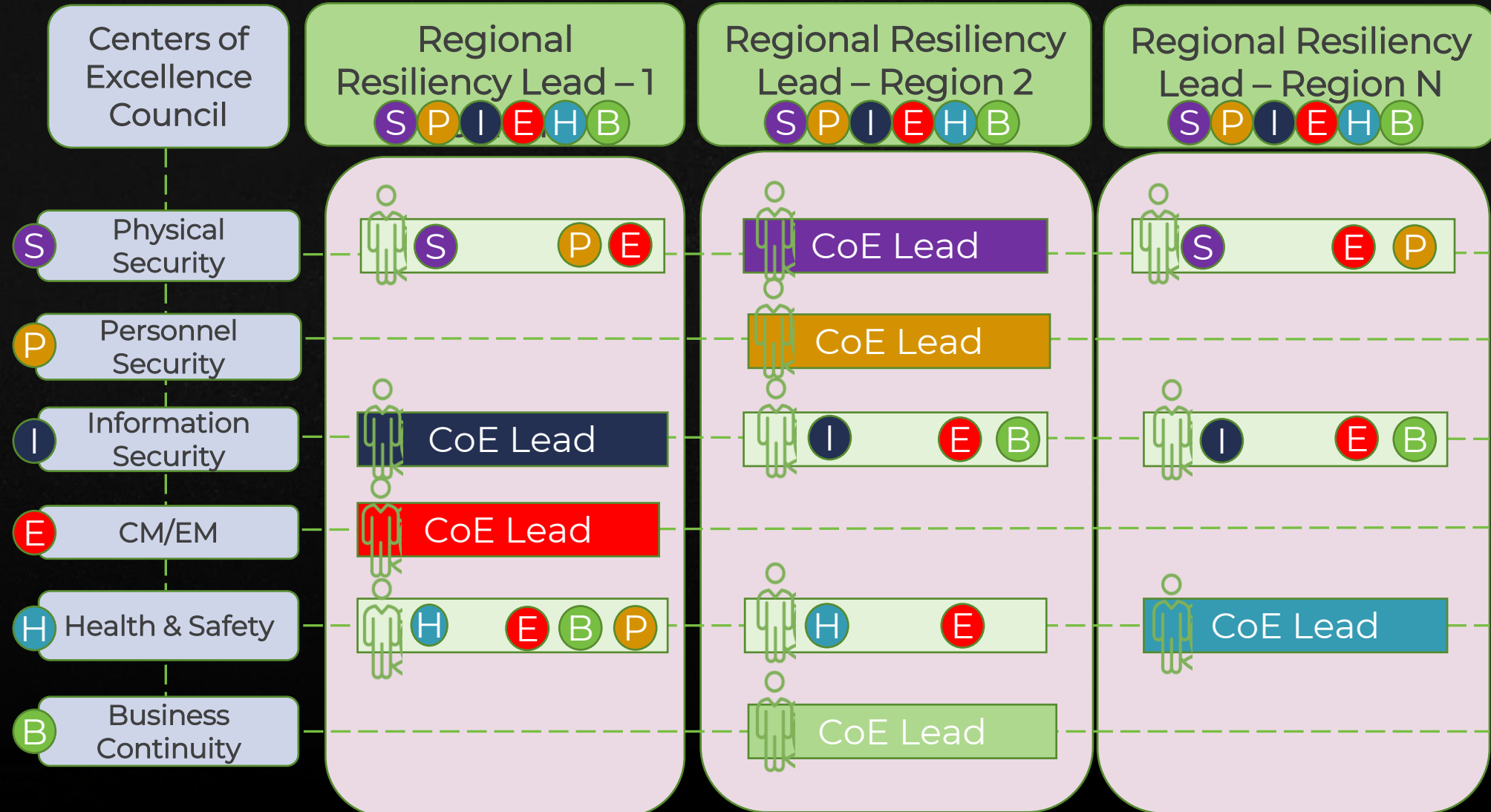
- **Multi-Capable Protective Personnel (MCPPE):** Protective Personnel trained in protective discipline skills and capable of accomplishing tasks outside of their core protective discipline specialty.
- **Primary Classification:** Primary protective discipline matrixed to respective Center of Excellence (CoE).
- **“Badging” System:** Based on additional discipline skill achievement and/or certification. Required for leadership positions and linked to promotion and pay.



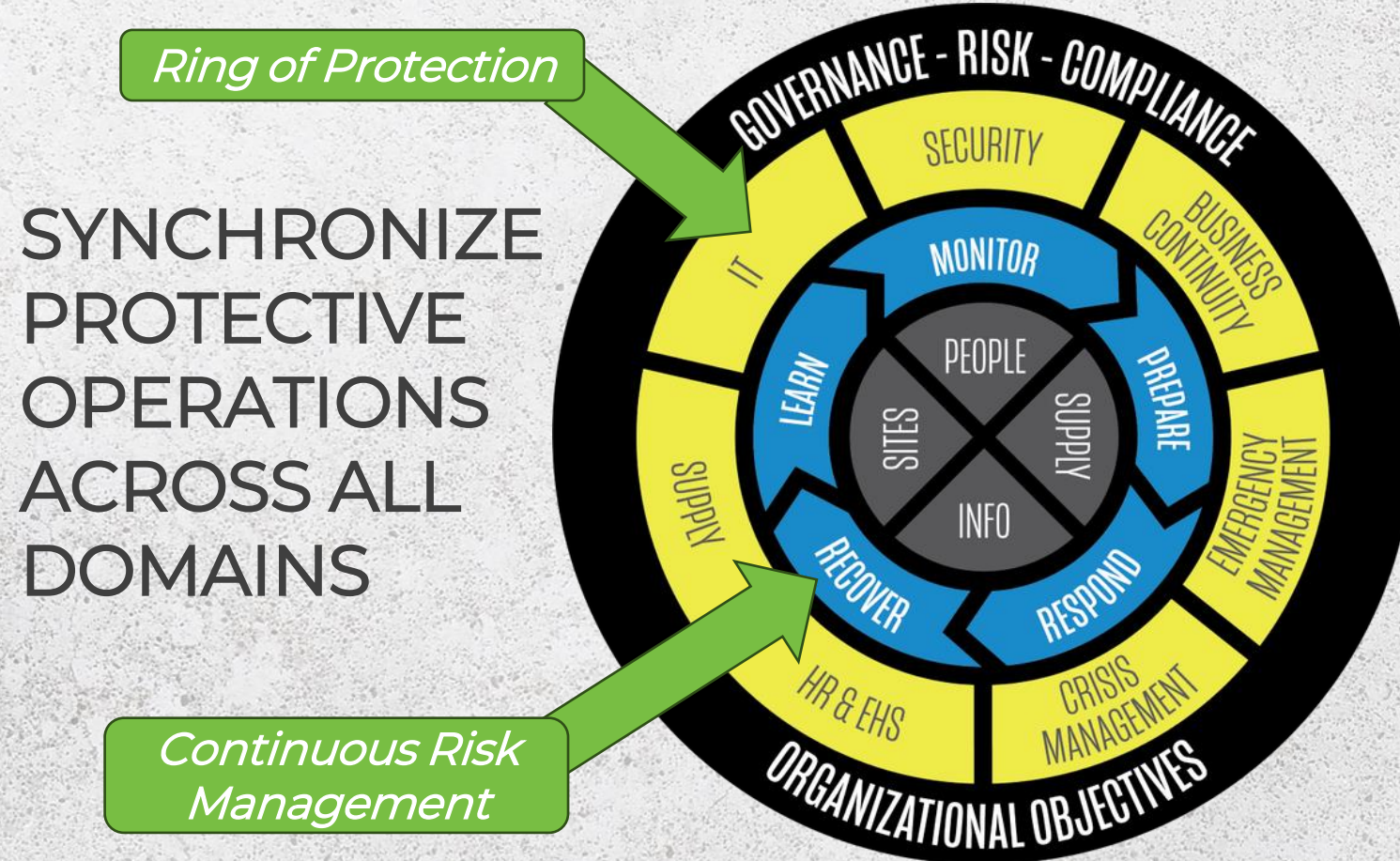
REGIONAL MODEL – PS JOINT FORCE

POWERED BY
ASIS
INTERNATIONAL

GLOBAL OPERATIONAL RESILIENCE



AGILE OPERATIONAL RESILIENCY™



Agile Operational Resiliency is the ability of an organization to adapt and thrive during times of stress, disruption and uncertainty.

AOR is a wholistic strategy that protects assets, objectives and reputations by empowering multi-disciplinary personnel to develop and continuously manage a 360-degree view of risk.

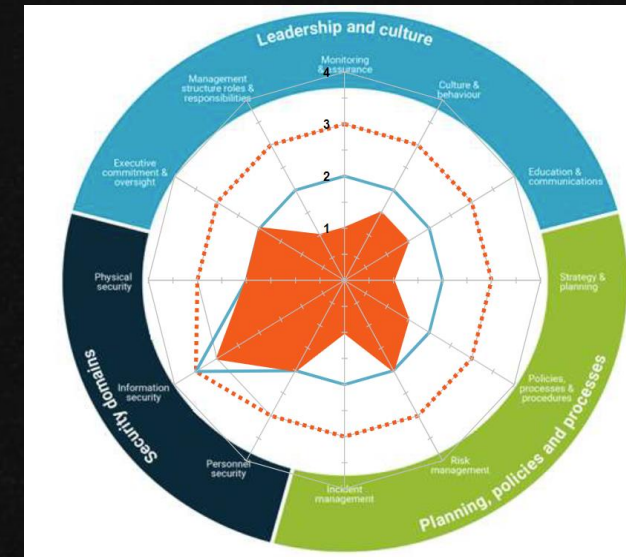
Go Deeper: <https://mcindooriskadvisory.com/aor-whitepaper>

PROTECTIVE SECURITY - CAPABILITY MATURITY MODEL (PS-CMM)

Go Deeper:

Capability Maturity Model for Protective Security, July 2022, NZ
Government

<https://protectivesecurity.govt.nz/self-assessment-and-reporting/capability-maturity-model/>



MODEL COVERAGE – OPERATIONAL ASSETS & SECURITY

- Each organization has a unique combination of:
 - People, information, and physical assets it needs to protect
 - Types and levels of security risks to manage
- Security Domains across Asset Classes
 - Personnel Security
 - Physical Security
 - Information Security
- Evaluates the Program Maturity across 12 dimensions
Resulting in 4 maturity levels (Informal, Basic, Managed, Enhanced)

12 EVALUATION DIMENSIONS

Leadership & Culture

- Executive Commitment
- Management Structure
- Monitor & Assurance
- Culture & Behaviors
- Education & Communications

Planning, Policies & Procedures

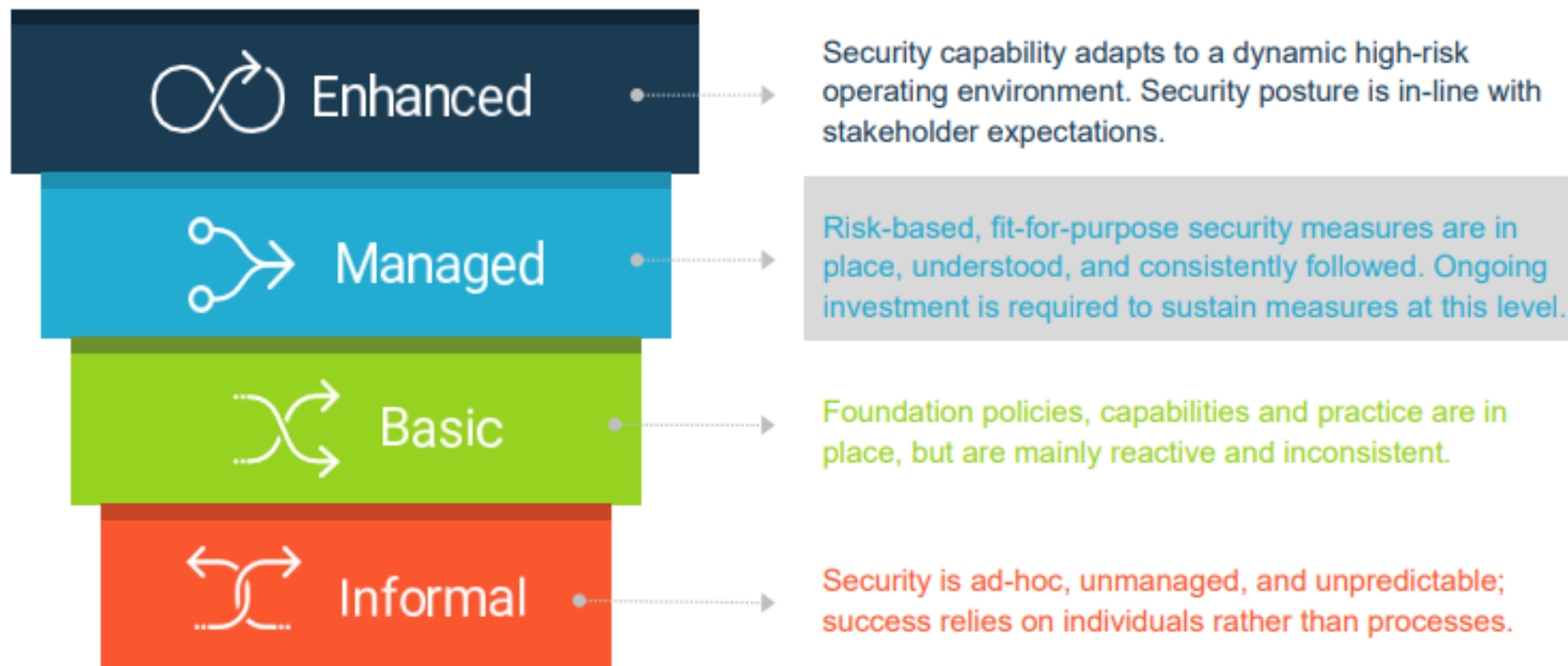
- Strategy & Planning
- Policies, Processes, Procedures
- Risk Management
- Incident & Crisis Management

Security Domains

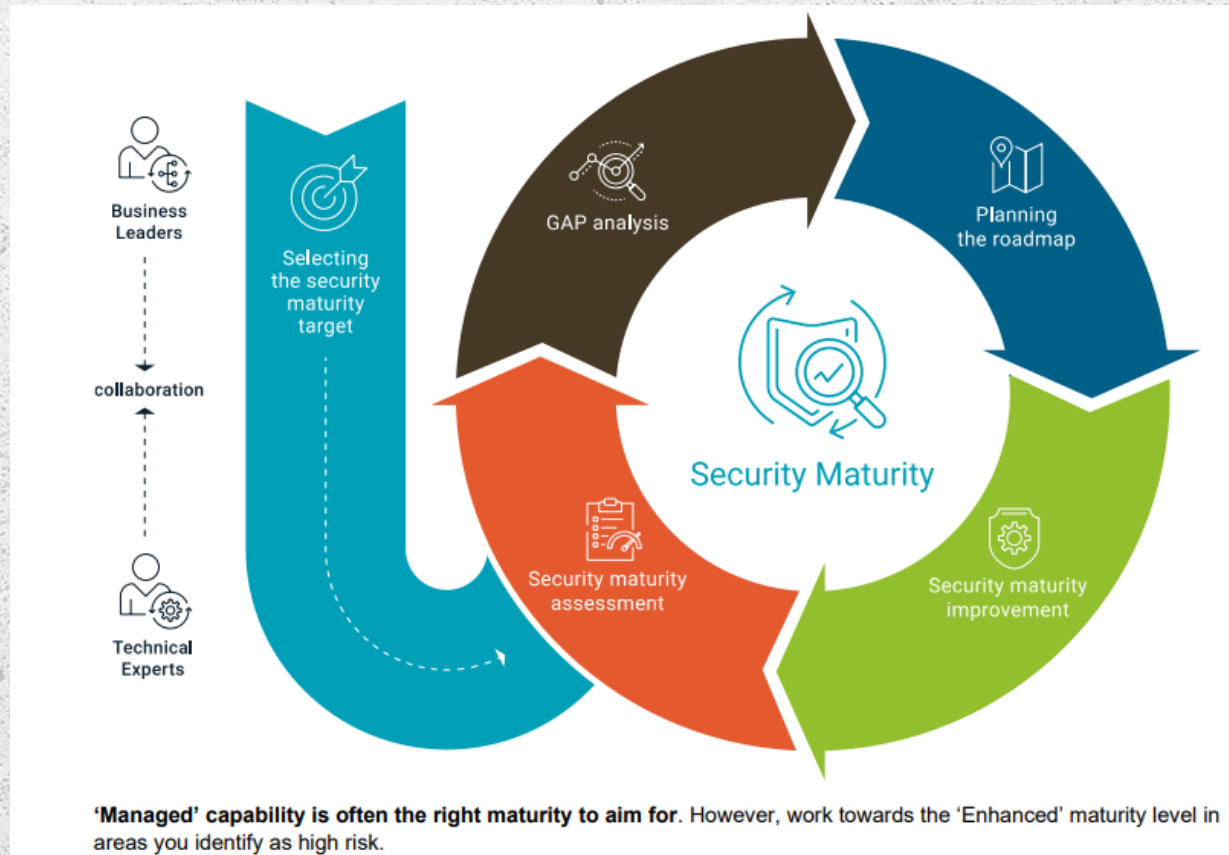
- Personnel Security
- Information Security
- Physical Security

4 MATURITY LEVELS

Security capability maturity levels



THE FULL LIFE-CYCLE IMPROVEMENT PROCESS

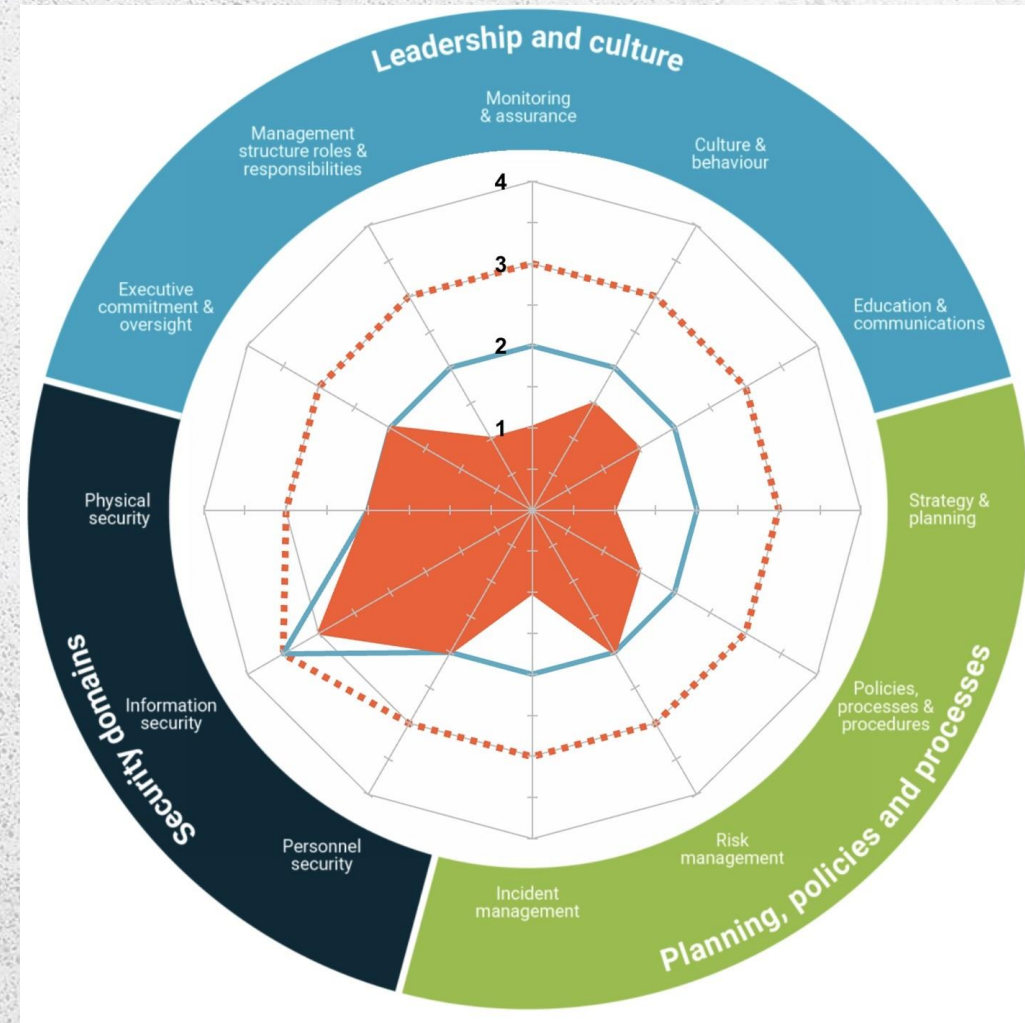


Provides clear metrics to the team & management on the Current state of maturity, the desired Target maturity and Improvement Plans to get there.

SAMPLE PS-CMM ASSESSMENT

PS-CMM Assessment “Spider Graph”

- Shows 4 Levels of Achievement
- Depicts across 12 Dimensions
 - Current Assessment Level
 - Target Assessment Level
 - Previous Assessment Level (optional)



SIMPLE & CLEAR PS PROGRAM MATURITY REPORTING

- Integrates all Protective Security Domains
- Clear identification of gaps that need improvement
- Ability to tie activities and investment to achievement of maturity
- Designed for “*One size does not fit all*” and can be tailored
- Supports Classified Security Environments & Supply Chain Security
- **Free Materials:** Handbook, Excel Assessment Workbook, Education Website, Case Studies

Handbook: <https://protectivesecurity.govt.nz/assets/Classification/Capability-Maturity-Model-2022.pdf>

KEY TAKEAWAYS

- **Objective-Centric Risk Management** – aligns the organization and investments to objectives
- **360-Degree Risk Assessment** – ensures collaboration and awareness
- **Combined Operational Model** – ensures information sharing, synchronization, rapid decision-making
- **Multidisciplinary Protective Personnel** – better solutions, adaptive to demand, personal growth and flexibility
- **Protective Services Maturity Model** – common language, measures and improvement process



RELATED RESOURCES



- *COVID-19 brought all hands on deck: Why we need to keep it that way*
 - <https://www.securitymagazine.com/articles/95623-covid-19-brought-all-hands-on-deck-why-we-need-to-keep-it-that-way>
- *Why an Objective-Centric Security Strategy Matters (20:14)*
 - <https://open.spotify.com/episode/2sKT9rOFcqE7ATVpp2xI1J>
- *Circuit Podcast (45:00) Creating the Unified Protector*
 - <https://podcast.circuit-magazine.com/episode/creating-the-unified-protector-bruce-mcindoe>
- *Talk'n TRM (30:48) with Bruce McIndoe*
 - <https://talkntrm.podbean.com/e/talk-n-trm-with-bruce-mcindoe/>

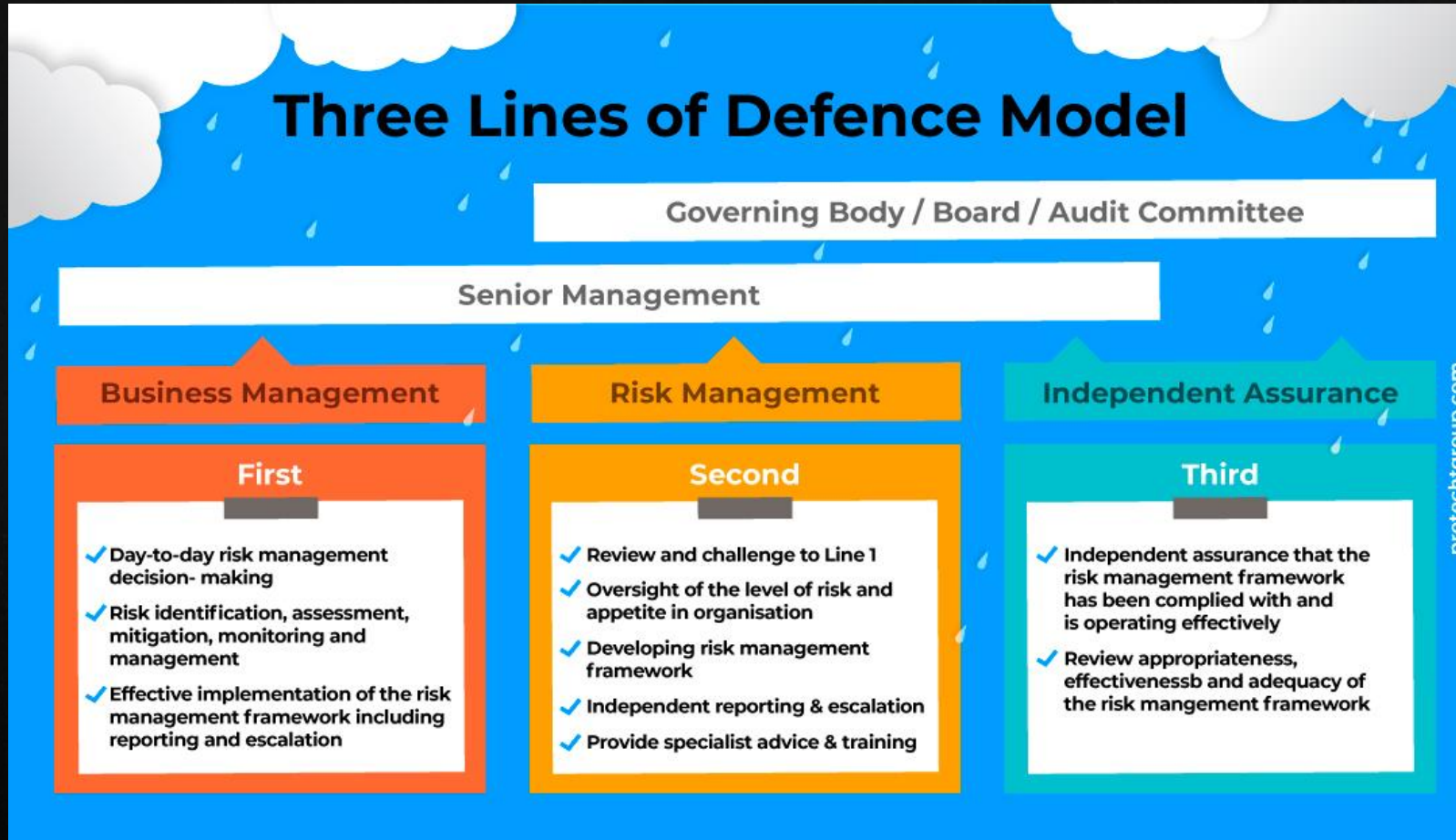


11-13 SEPTEMBER 2023
DALLAS, TEXAS, USA

POWERED BY



3 LINES OF DEFENSE MODEL



- **Board**
 - Understand Risk Profile/Appetite
 - Know effective ERM in place
 - Review portfolio of risk against key objectives & residual risk
 - Review most important risks
- **CEO**
 - Participate with ERM Team
 - Assign Key Objective responsibility
 - 1st Line of Defense
- **Directors/Departments/LOB**
 - Understand risks & decisions
 - Implement risk management processes
- **Staff**
 - Understand ERM/Compliance
 - Maintain risk aware culture
 - Alert management to risks

Traditional Methods

Objective Centric Self-Assessment

