Risk Culture Management Framework

A systematic methodology to develop and implement risk culture in an organisation.

Author: Adley John Fisher Mangkiu

Edition: 1st Publication

Date: September 2025

1. Introduction

The Risk Culture Management Framework (“RCMF”) was developed with the purpose of fortifying available risk management frameworks in the aspect of developing and implementing risk culture in a systematic manner. Referring to ISO31000:2018, COSO Framework, albeit discussed in these frameworks, there is still an **absence of a structured approach in tackling the dynamic nature of organizational culture.**

This framework addresses the crucial gap between the *principle* of a strong risk culture and the *practice* of achieving it.

Review of Foundational Frameworks:
ISO31000:2018

i. The standard implicitly and explicitly addresses the importance of culture within risk management, primarily under the principles and framework components.
ii. **On Principles - Clause 4:** It states that risk management "*creates and protects value*" and is "*integral to all organizational activities*." This highlights that a cultural foundation is necessary. Specifically, **Clause 4.6** states that risk management "*takes human and cultural factors into account*."
iii. **On Framework - Clause 5:** The integration of risk management into organizational processes is a core objective. **Clause 5.2 (Leadership and commitment)** mandates that top management must ensure "*the integration of risk management into all organizational activities*," which is indicative to shape culture.
iv. Furthermore, **Clause 5.3.4 (Organizational Context)** requires the organization to understand its external and internal context, which explicitly includes "culture."

COSO ERM Framework (2017)

i. COSO's Enterprise Risk Management – Integrating with Strategy and Performance framework places a significant and explicit emphasis on culture.
ii. On **Organizational Culture:** The entire framework is built upon five components, the first and most foundational of which is "*Governance and Culture*."
iii. The COSO ERM framework defines Enterprise Risk Management as "*the culture, capabilities, and practices... that an organization relies on to manage risk*." Here, culture is positioned as the very first element.
iv. The framework also dedicates an entire principle (**Principle 1**) to this: "*The organization establishes and operates risk management in a manner that demonstrates a commitment to risk management and a desirable culture*." It elaborates on the board's role in defining desired behaviours and the need to attract, develop, and retain capable individuals who embody the organization's values.

IRM ABC Framework (2025)

i. The IRM ABC (Advanced Behavioural & Cultural) Risk Framework was developed specifically to address the critical implementation gap in modern risk management, placing an unparalleled and practical emphasis on measurable cultural transformation.
ii. On **Organizational Culture**: The framework's entire design revolves around the idea that **"Culture Eats Strategy for Breakfast,"** formalizing it into three core pillars: **A**wareness, **B**ehaviour, and **C**onnection, with behavioural psychology as its foundation.
iii. The IRM ABC framework defines Enterprise Risk Management as "**the ecosystem of ingrained habits, shared accountability, and empowered decision-making that enables an organization to navigate uncertainty with confidence.**" Here, the outcome of a successful culture is positioned as the primary goal.

2. Basis of the Risk Culture Management Framework

It is *hypothesized* that while established frameworks (ISO31000:2018, COSO ERM Framework) and emerging frameworks (IRM ABC) undeniably recognize and mandate the critical importance of risk culture, they collectively point to a crucial gap: **the absence of a prescriptive, structured, and implementable approach to *developing* and *implementing* risk culture**.

Both ISO 31000 and COSO use high-level, principle-based language. They describe **"what"** and **"why"** it is important, but they deliberately avoid prescribing a detailed **"how."** The IRM ABC Framework, while a significant step forward in focusing on behavioural psychology, remains a conceptual model.

i. **ISO31000:** A standard of principles and guidelines, *not a set of requirements for a management system*. It provides the *"what"* but not a step-by-step *"how to"* for cultural change.
ii. **COSO:** A framework of components and principles. While more descriptive than ISO, it is still a governance framework, *not an implementation manual*. It sets the expectation for a strong culture but does *not provide a structured methodology* to build risk culture from the ground up or transform an existing risk culture.
iii. **IRM ABC:** A behavioural-focused framework that provides the philosophical "why" behind cultural mechanics. However, it does not provide a tangible, structured breakdown on "how" the specific processes, tools, and iterative cycles required to diagnose, design, execute, and perpetuate cultural change within an organization.

Framework	What it Provides	What it lacks	How RCMF improves this
ISO 31000:2018	"What" & "Why" (Principles & Guidelines)	A prescriptive, step-by-step methodology for cultural implementation.	**Provides the "How"**: A detailed 5-phase iterative process (Define, Asses, Design, Execute, Monitor) to build culture from the ground up.
COSO ERM (2017)	Governance Expectation (Components & Principles)	A structured implementation manual to operationalize culture and measure behavioural change.	**Provides tools & metrics:** Behavioural pillars, qualitative/quantitative targets, and a system to measure cultural gaps and progress.
IRM ABC	Behavioural Philosophy (Conceptual Model)	A tangible, actionable process to translate theory into sustainable practice and habit formation.	**Provides the mechanism for change:** A practical cycle of assessment, reinforcement, and adaptation to engineer and nurture target habits into culture.

The frameworks focus on integrating risk management into the existing culture and processes. For example, ISO 31000's direction is to "**integrate**" risk management assumes a pre-existing risk culture structure into which risk management must be embedded. It does not provide a structured approach to first develop a risk culture.

Risk culture is dynamic and should be accepted as such. ISO31000, COSO, and IRM ABC acknowledge this as a contextual or conceptual factor but **do not provide a comprehensive methodology** to continuously measure, nurture, and adapt the risk culture in response to this constant change.

Culture is a mandated and foundational concept in these frameworks. However, the nature of these documents leans more towards high-level guidance and conceptual models rather than a structured, practical methodology for the active

development, implementation, and maintenance of risk culture creating the definitive need for a resolute RCMF.

3. Philosophy of the Risk Culture Management Framework

The RCMF is developed under one core philosophy: ***Risk culture is not a set of rules, but a living system of relationships*.** It is the major determinant of the effectiveness of all formal risk management processes.

i. **View of Culture:** Culture is the totality of shared attitudes, values, beliefs, and behaviours related to risk awareness, risk-taking, and risk management. It is transmitted primarily through social learning and is rooted in the psychological safety of a population.

ii. **Guiding Principle:** The framework is not a linear project but an **iterative, evolutionary process.** It is a cycle of assessment, corrective action, reinforcement, and re-assessment.

"Repetitive action makes a practice.
Continuous practice makes a behaviour.
Consistent behaviour makes a habit.
Collective habit makes a culture."

4. Risk Culture Management Framework

The RCMF is structured around five iterative phases which must be supported with continuous activities.

- *Phase 1: Define Target Culture*
- *Phase 2: Asses Current Culture*
- *Phase 3: Design Action Plan*
- *Phase 4: Execute & Implement*
- *Phase 5: Monitor & Reinforce*

4.1. Phase 1: Define Target Culture

Phase 1 objective: *To establish a relevant, detailed and ideal "target" risk culture for the organization.*

Step 1: Specify Behavioural Pillars

- Conduct workshops/brainstorming with operational function experts, Senior Management and the board using high relevance data & information such as:
  - Strategic Objectives
  - Organizational Values
  - Risk Appetite Statement
  - Geographical-specific beliefs and lifestyles

- Conduct multiple sessions as necessary and come up with 3-5 high relevance behavioural pillars. It is recommended to keep the number of behavioural pillars concise, prioritising quality over quantity.
- Example output of high relevance behavioural pillars as below:

  - Pillar 1: Transparency
    (willingness to report any type of issue without fear of ramifications)

  - Pillar 2: Risk Intelligence
    (able to elaborate cause and impact, how each risk interacts with each other)

  - Pillar 3: Risk Awareness
    (able to detect potential risk autonomously)

  - Pillar 4: Ownership & Accountability
    (clear understanding on responsibilities and the absence of blame)

- Once Behavioural Pillars have been decided, begin listing down target behaviours in relation to each pillar.
- Example target behaviours as below:

		Pillars	
		Transparency	**Risk Intelligence**
Target Behaviours	**1**	Willingness to report any type of issue, error, or near-miss without fear of negative ramifications.	Ability to clearly articulate the root cause of a risk event.
	2	Proactive and open sharing of information that could be critical to managing risk.	Ability to explain the potential operational and financial impact of a risk.
	3	Encouraging and valuing honest communication from all levels of the organization.	Understanding how different risks are interconnected and can influence one another.
	4	Creating an environment where questions are welcomed and answered openly.	Using understanding of risk interactions to make more informed decisions and mitigate cascading effects.

Step 2: Define Target Behaviours (Qualitative)

- For each behaviour, define in detail:
  - If the behaviour is in practice (positive target behaviour)
  - If the behaviour is not practiced (negative target behaviour)

- It would be best to use a “narrative” and “cautionary tales” when defining a behaviour.
- Example output of a well-crafted behaviour is as the statement below:

Positive Target Behaviour

"A *Junior Internal Auditor immediately highlight a mistake in the audit report albeit reviewed by Internal Audit Manager, stating 'I might be wrong, but I wanted to ensure the quality of our work. I wanted us to check.'"*

Negative Target Behaviour

"A *Junior Internal Auditor notices a mistake in the audit report but stays silent due to fear of ramifications stating 'the Internal Audit Manager have reviewed this report meaning this is not an issue. If I bring it up, I might be scolded.' "*

Step 3: Translate to Metrics (Quantitative)

- All target behaviours that have been determined qualitatively must then be defined quantitatively to enable numeric analysis.

  Note: It is understood in practice that not all findings can be measured Quantitatively. In this case, relying on Qualitative or Semi-Quantitative measures would be ideal.

- The numeric analysis will facilitate a realistic progression tracking of the risk culture implementation.
- There are several methodologies to transform qualitative to quantitative, meaning a singular pillar can have several measures which is beneficial in the implementation of risk culture.
- Example output of quantitatively defined behaviours as below:

  From the "Transparency" Pillar

  Qualitative Target Behaviour (Positive): "A Junior Internal Auditor immediately highlights a mistake in the audit report albeit reviewed by Internal Audit Manager..."

Qualitative Target Behaviour (Negative): "A Junior Internal Auditor notices a mistake... but stays silent due to fear of ramifications..."

a) Metric: Employee Speak-Up Rate

Definition: The percentage of employees who report an issue, error, or near-miss within a defined period (e.g., number of reported cases per quarter – Zero cases is a cause of concern).

How to Measure: (Number of unique employees submitting reports / Total number of employees) * 100

Target Behaviour: Increase the speak-up rate from a baseline of 20% to 70% within a quarter.

b) Metric: Anonymous Reporting Tool Usage

Definition: The number of submissions made through an anonymous reporting channel (e.g., web portals, hard copy forms) per 100 employees.

How to Measure: (Total anonymous reports / Total number of employees) * 100

Target Behaviour: Maintain or increase the current rate of 5 reports per 100 employees, indicating support on risk reporting behaviour a sustained psychological safety.

c) Metric: Manager Response Index

Definition: An anonymous 5-point scale score from employee surveys assessing the statement: "When I raise a concern, my manager responds constructively and without retaliation."

How to Measure: Regular anonymous pulse surveys

Target Behaviour: Increase the average score from 2.8 to 4.5.

Step 4: Determine Ideal Target Risk Culture

- After all pillars have been qualified and subsequently quantified, an ideal target behaviour can be determined.
- As slightly mentioned in the process of defining quantitative risk behaviours, an ideal target behaviour must be the last output of *Phase 1*.
- Example Ideal target behaviour as below:

Behavioural Pillar	Qualitative Target Behaviour (Positive Example)	Quantitative Metric & Definition	Ideal Target Behaviour (Quantified Goal)
Transparency	"A Junior Internal Auditor immediately highlights a mistake in the audit report, stating 'I might be wrong, but I wanted to ensure the quality of our work.'"	Metric: Employee Speak-Up Rate Definition: % of employees who report an issue/error within a quarter.	Increase the organization's quarterly Speak-Up Rate from a baseline of 20% to 70%.
Risk Intelligence	"A project manager can clearly articulate how a delay in one department creates financial, operational, and reputational risks for the entire project."	Metric: Risk Intelligence Score Definition: Average score from a mandatory risk assessment quiz following project reviews, testing understanding of risk interdependencies (scale 1-5).	Achieve an average Risk Intelligence Score of 4.5 or higher across all project teams within two quarters.

Ownership & Accountability	"A team leader, upon a project setback, initiates a blameless post-mortem focused on 'what went wrong with the process' rather than 'who made the error.'"	Metric: Blameless Post-Mortem Rate Definition: % of significant risk events or project setbacks that result in a documented, blameless review process.	Ensure 90% or more of significant risk events are followed by a blameless review process to reinforce a culture of accountability without fear.

Step 5: Acknowledgement & Approvals

- A list of all ideal target behaviours will be the sum of all work done in *Phase 1*.
- The target behaviours will then be presented to the Risk Committee / Top Management / Board of Governance for acknowledgement and approval.

Realistic Outcomes:

a) Risk Committee / Top Management / Board of Governance approves all ideal target behaviours – proceed with Top-Bottom implementation.
b) Risk Committee approves ideal target behaviours; Top Management / Board of Governance does not approve – Bottom-Top implementation.
c) Risk Committee / Top Management / Board of Governance does not approve ideal target behaviours – Infiltrative Implementation

Note:

i. There are some cases that the presented ideal target behaviours are approved partially (not all listed are approved).
ii. For those approved, the risk practitioner will proceed with Top-Bottom Implementation.

iii. The risk practitioner is advised to do infiltrative implementation of the remaining ideal targeted risk cultures based on relevance.

4.2. Phase 2: Asses Current Culture

Phase 2 objective: *To determine a holistic and accurate representation of the current risk culture by combining quantitative and qualitative, formal and informal assessment measures.*

Step 1: Asses current behaviours

- Collect information on current behaviours in a risk perspective.
- There are no limitations on the methods used to collect information, but it is highly suggested that any behaviour assessment to be done considering 3 criteria:

(a) Discreet

i. Target sample should not be aware of an ongoing assessment to ensure no change in behaviours happens during the assessment.
ii. Awareness of observation will create restrains which alters the raw behaviours practiced.
iii. Example: Knowing an audit is coming will alert an auditee. An auditee, regardless of compliance or non-compliance will strive to align with actual practices to “appear” complaint.

(b) Face-Level

i. Assessment should be done without justifying the behaviours observed.
ii. Every risk practitioner will have different understanding and different views. As much as possible, avoid justifying the observed behaviour to suit preferred understanding/agenda.

iii. Example:

Behaviour observed: Individuals are sharing ID & Password for critical weighbridge operations in a milling factory.

× Justified observation: "Due to lack of staff availability and ease of transition, the employees are sharing ID & Password".

✓ Proper risk-based observation: "Sharing of ID & Password is a critical risk that may cause pilferage which is highly impactful to the company's cashflow. This also impacts audit traceability should there be any pilferage cases uncovered".

(c) Relevance

i. Behaviour assessment must be relevant to the organizations respective business model considering internal and external context.

ii. It is not optimal to force a behaviour without considering the relevance of the behaviour to the organization.

iii. Example 1: In the context of an IT security company, reporting of errors is highly relevant as the impact if a "bug" is discovered by a customer is significant.

iv. Example 2: In the context of Legal firms, a junior lawyer publicly reporting a minor citation error might be seen as undermining the partner's authority and damaging the firm's reputation reflecting a lack of expertise.

- Behaviours observed will be considered as raw data to be the used for Qualitative/Quantitative output.

Step 2: Consolidate assessment findings.

- As the assessed behaviour are collected using multiple methods, all sources of information must be consolidated into a singular list.
- Example output as below:

i. Openly discussing crucial information.
ii. Company laptops/desktops are not password locked.
iii. Allowing external parties to enter premises without logging entry or supervision.
iv. "Blame-game" during cross departmental meetings.
v. Fear/hatred towards audits.

- The risk practitioner will then elaborate this risk further and transform the assessed behaviour into a Qualitative format.
- Example of the transformed behaviour into a qualitative format is as below:

i. Openly discussing crucial information.

Positive Target Behaviour

"An employee, before leaving their desk for a meeting, consistently locks their computer workstation as a standard practice, understanding that it is a fundamental step in protecting client and company data from unauthorized access."

Negative Target Behaviour

"An employee walks away from their desk for an extended period, leaving their computer unlocked and their sensitive emails and files fully accessible to anyone passing by, believing 'it's just for a minute' or 'no one would look anyway'."

- Once all assessed behaviours have been transformed to a Qualitative format, the next step would be to translate the Qualitative to a Quantitative measure.
- This step will be entirely the same step as described in: *"Phase 1: Define Target Culture > Step 3: Quantitatively Define Behaviours".*

Step 3: Compare findings against Target Culture

- At this point, there should be 3 main resources prepared which are:

  i. Behavioural Pillars
     - This iterative document will be the guideline for risk practitioners to align to when implementing Risk Culture.

  ii. Qualitative/Quantitative Ideal Target Behaviour
     - This iterative document is the goal of the Risk Culture implementation.
     - It reflects what behaviours should be habitual in the organization for Risk Culture to be effectively embedded in the organization.

  iii. Qualitative/Quantitative Current Behaviour
     - This iterative document are the observed behaviours that shaped the current organization's Risk Culture.
     - This document will be the core variable in ensuring proper Risk Culture implementation.

- The current behaviours will then be compared against the ideal targeted behaviours to determine the actual gaps and weakness that the organization is realistically facing in the process of Risk Implementation.

Step 4: Prioritize Gaps

- Based on current available information prepared, a realistic comparison will be done between ideal target behaviour vs current behaviour.
- The simplest method to do this is by comparing the Quantitative aspects of both ideal target behaviour and current behaviour.
- Example comparison as below:

Ideal Target Behaviour (Quantified Goal)	Current Rating	Goal Rating	Realistic Gap
Increase the organization's quarterly Speak-Up Rate from a baseline of 20% to 70%.	2%	70%	68%
Achieve an average Risk Intelligence Score of 4.5 or higher across all project teams within two quarters.	1.3	>4.5	3.2

Note: *Realistic Gap = Goal Rating – Current Rating*

- As illustrated in the table above, this comparison methodology is straightforward and effective to measure the "room for improvement" in the risk culture implementation.
- Based on the Realistic Gap, the risk practitioner will arrange based on severity (as per general risk evaluation practice).
- Action plan and resource allocation should be executed based on priority.

4.3. Phase 3: Design Action Plan

Phase 3 objective: *To develop action plans to address root causes of cultural gaps using data and information gathered.*

- A widespread practice for cultural initiatives is the urgency of implementing action plans.

- "One must crawl before they can walk" should give an idea on Risk Culture implementation ideology.
- The critical point of failure in implementing a Risk Culture is taking a direct jump from "We have a problem" immediately to "let's stop this action / let's do training / let's enforce this policy with penalties".
- Risk Culture implementation is lesser about the "activities of change" and more about the "mechanisms of change".

i. Activities of change: It is the *"what"* of risk culture implementation.
   - It is the specific actions, initiatives, and interventions done to ***influence risk culture*** (e.g., training programs, communication campaigns, workshops, revised incentive structures).

ii. Mechanisms of change: It is the *"how"* of a functioning risk culture.
   - It is the underlying psychological and social processes through which the activities produce a ***sustainable cultural shift*** (e.g., creating psychological safety, fostering social learning, new behaviours).

<u>Step 1: Determine suitable action plan.</u>

- Categorize the cultural gaps using MINDSPACE framework (*by the UK Institute for Government and the Cabinet Office*)
  i. **M**essenger (who communicates the risk holds the same weight as what is communicated)
     - Humans are heavily influenced by who communicates information.
     - Humans are prone to trust or to be persuaded more easily by authority figures, experts, and people we like or close with.
     - "The right message from the right person"

  ii. **I**ncentives (social recognition, time savings, authority)
     - Humans a wired to be "loss-adverse" and more sensitive to immediate gratification.

- It is recommended that to frame incentives in all risk culture implementations.

iii. **N**orms (our perception on what others are doing)
- Humans are significantly influenced by what others do and put emphasis on the approval/disapproval of others.
- Risk practitioners must leverage on social norm for better risk culture implementation.

iv. **D**efaults (the pre-set option)
- Humans are technically “ritualistic” and indirectly “systematic” with a strong sense to stick to a pre-set option.
- Risk practitioners should present optimal risk behaviour choices as default, especially in the perception.

v. **S**alience (how obvious and attention-grabbing the risk is)
- Humans are attracted to things that are new, interesting, relevant and simple.
- Risk practitioners leverage on this for risk behaviour implementation.

vi. **P**riming (subtle cues that influence behaviour)
- Human actions are often influenced by sub-conscious cues in our environment.
- These are considered as sub-conscious “triggers” to certain mental associations.
- The goal is to prevent “don’t tell us what to do” response upon implementation. Risk practitioners should aim to nudge and inject (or prime) risk optimal behaviours.
- Targeted outcome should be an automated “this is wrong, let me do something about it”.

vii. **A**ffect (emotional response)

- Humans are driven by immediate emotional reactions and gut feelings, which often override logical, analytical thinking when making decisions.
- Risk practitioners must design risk communications and training impacts emotionally, using narratives and imagery to make risk feel real and urgent.

viii. **C**ommitments (the power of public or written pledges)

- Humans have a powerful psychological desire to be consistent with their past actions and public agreements.
- Risk practitioners should obtain voluntary and public commitments to safe practices to increase accountability especially in shaping a risk culture.

ix. **E**go (how the action makes us feel about ourselves)

- Humans act in ways that align with their self-identity and that make them feel good about themselves, often seeking to avoid actions that cause internal guilt or shame.
- Risk practitioners can frame compliant behaviour as "what a professional/safe/responsible person like you does," appealing to individuals' self-concept to encourage better risk optimal behaviour.

- Once cultural gaps have been categorised, risk practitioners should match the categorised behaviour to a proven behavioural technique.
- Example Gap: Low "Speak-Up Rate" (Current: 2%, Target: 70%).
- Root cause: Fear of retaliation (**Affect**), perception that "no one else reports" (**Norms**).

i. **Action 1 (Addressing Norms): Use social proof.** Instead of a generic email from HR, have a respected team leader/manager (the right **M**essenger) share a brief story: *"Last month, John in production*

reported a near-miss with a conveyer belt. Because he spoke up, we fixed the process for everyone. Thank you, John." This makes the desired behaviour visible and normal.

ii. **Action 2 (Addressing Affect): Re-frame the incentive**. Guarantee and loudly promote a "no retribution, only gratitude" policy. Implement a "Lesson of the Month" award for the best-submitted risk insight, voted on by peers.

Step 2: Design Habit to Culture milestone

- Breakdown the task of implementing a risk culture into a series of tangible and measurable milestones.

i. **Milestone 1: Practice**
   - All measures in this stage are siloed/individualistic/departmental.
   - This milestone is achieved when most of the individuals in the pilot group consistently demonstrate new behaviours.
   - Example: *"80% of individuals in the Operations Control department voice out at least 1 insight during the monthly operational risk meeting".*

ii. **Milestone 2: Behaviour**
   - At this stage, automation should be apparent.
   - Behaviours are automatically demonstrated without any push/reminder.
   - Example: *"The Operations Control department initiates internal risk meetings for 3 consecutive months with 90% of attendees providing insight during the monthly operational risk meeting"*.

iii. **Milestone 3: Habit**
   - At this stage, a behaviour goes beyond automation and becomes a "need" even without official authority/policy implementation.

- A behaviour becomes a “standard” in a group where measure become more qualitative than quantitative.
- In this stage, most measures will be inverted from “How many risk meetings a month” to “How many risk meeting was not conducted in a month”.
- Peers will openly remind each other to prepare for the meeting and discuss on risk without even being in an official meeting or venue.

iv. **Milestone 4: Culture**

- At this stage, the habit of a group starts to influence other groups, mostly due to cross departmental activities and engagements.
- The behaviours practiced become a default on “how we do things here”.
- Example: *“The Finance department initiates financial risk meetings after joining several of Operations Control department’s risk meeting”*.

➢ Below is the simplest breakdown on how these milestones can be implemented:

i. Milestone 1: Practice (Learning the Basics)

- Goal: Get people to try the new behaviour, even just once.
- What to Do:
  - ✓ Train them: Show them how. "Here's how to report a risk."
  - ✓ Make it easy: Give them a simple controls/measures like forms or a clear checklist.
  - ✓ Keep it safe: Pilot test on a small team first. Branch out if it works.

ii. Milestone 2: Behaviour

- Goal: Make the behaviour a normal, a routine.
- What to Do:
  - ✓ Add reminders: Put a "Report a Risk" button where everyone can see it.

- ✓ Show appreciation: Say “Thank you” openly. When someone does it right, praise them.
- ✓ Share proudly: "Due to his insight and the team’s efforts, the company is now more resilient." This makes it seem normal.

iii. Milestone 3: Habit

- Goal: Make the behaviour so normal that the team expects it from each other.
- What to Do:
  - ✓ Talk about it: Make risk discussion a fixed agenda on every meeting.
  - ✓ Let the team lead: Have team members run the risk meetings themselves.
  - ✓ Build pride: Say things like, "It would be hard for my team to fail since we prepare for mistakes."

iv. Milestone 4: Culture

- Goal: The behaviour is now standard everywhere in the company.
- What to Do:
  - ✓ Positive Infection: Include un-initiated departments in mature risk implementations.
  - ✓ Share success: Have your successful team tell other teams how they did it.
  - ✓ Entry Implementation: Tell new hires from day one, "This is how we work here."
  - ✓ Document: Make it part of the official rules and job descriptions.

Step 3: Design Relapse prevention

- Culture is dynamic and by nature prone to revert to old, familiar patterns.
- As all risks, there should a mechanism of resilience to automate “counter-regression”.
- Proposed strategy to design relapse prevention as below:
    i. Identify Relapse Triggers
        - Begin with the question, *“What could make us go back to our old ways?”* There are many ways to get an output to this simple question.
        - Risk practitioners could use any preferred method of identification as long as it aligns with a singular goal, which is to *critically and objectively list down all possible historical behaviours that could cause a relapse*.
        - Example of relapse triggers as below:

          Leadership Change: New management may not value the cultural initiative.

          Performance Pressure: Under tight deadlines, "shortcuts" (old behaviours) become tempting.

          Initiative Fatigue: The "next big thing" draws attention and resources away.

          Crisis Mode: A major incident can cause an automatic reaction towards blame and secrecy.

    ii. Fortify Defence against Triggers
        - There are no specific rules or standards on how to compile and arrange identified relapse triggers, but it is strongly recommended to **consider all triggers as significant**.

- One significant mistake that risk practitioners do for Risk Culture Implementation is considering some relapse triggers are less significant than others.
- As portrayed throughout the framework, **culture is viral**. One small lapse in practice will make a behaviour, which in time will avalanche into a negative culture.
- Risk practitioners must determine root cause of each triggers identified and setup a mechanism to defend/address triggers from happening or impacting the newly implemented culture.
- Example of defence mechanisms as below:

For Leadership Change: Formalize the culture.

- ✓ Embed the target behaviours and their metrics into formal performance reviews, promotion criteria, and board reporting dashboards.
- ✓ Inject the target behaviours into the "biology" of the company from the smallest level of operations to the highest level of decision making.

For Performance Pressure: Make old behaviours "uncomfortable".

- ✓ If the old culture was "blame", implement a mandatory "Lesson Learned" field in every incident report that must be completed before the report can be closed.
- ✓ Should there be any individual that voluntarily revert to old behaviour, that individual must make a departmental/company-wide presentation on their action.
- ✓ This forces uncomfortable association with the behaviour.

For Initiative Fatigue: Automate reinforcement. Use nudges.

- ✓ Instead of a big annual training, set up a quarterly, automated pulse survey that measures psychological safety and sends

results directly to the highest relevant authority in the company.

For Crisis Mode: Create a "Cultural Mandate".

- ✓ This is a pre-written, pre-approved statement for communications during a crisis that mandates phrases like "Our focus is on understanding the process failure, not assigning blame," signed by the Board.

iii. Review Defence Mechanism

- Relapse triggers will change as the risk culture matures.
- Risk practitioners must consider how the risk culture will evolve in the company.
- Not all implementations will be relevant as time progresses; thus, it is highly advisable to review relapse triggers in intervals.

4.4. Phase 4: Execute & Implement

***Phase 4 objective**: To implement action plan in a way that builds momentum and broad organisational impact.*

Top-Bottom Implementation:

- ➢ This is the best-case scenario for risk culture implementation. This is where the Top Management & the Board acknowledges and approves of the proposed RCMF.

Step 1: Assemble authoritative, cross functional team to lead implementation.

- ➢ Using authority approved by Top Management & the Board, mandate several key individuals in all areas of operations to begin implementation.

Step 2: Communicate the truth (Current vs Target)

- Using data & information collected, elaborate the truth to all the relevant key individuals.
- Tell them what the issue is, how changing can benefit them, how the behaviours are impacting their respective operational processes.

Step 3: Empowerment

- Determine action plan and execute.
- Give the key individuals independence and authority to make decisions and changes.
- Provide reasonable support using authority approved by Top Management & the Board.

Step 4: Incremental wins.

- Simply announce wins proudly.
- Even minor impacts should be celebrated.

Bottom-Top Implementation

- In which case the RCMF is only partially acknowledged and approved (e.g., approved by Risk Committee but not by Top Management & the Board), this will be the 2nd best option for implementation.

Step 1: Pick a pilot group.

- Pick a pilot group for the RCMF.
- Determine key individual that holds a significant authority and impact in the pilot group.
- Initiate risk culture implementation with the key individual.

Note: If the key individual refuses, move on to a different pilot group with different key individuals.

Step 2: Communicate the truth (Current vs Target) – pilot group specific.

- Using data & information collected, elaborate the truth to the key individuals.
- Elaborate what the issue is, how changing can benefit the pilot group, how the behaviours are impacting the pilot group's operational processes.

Step 3: Empowerment

- Determine action plan and execute.
- Give the key individuals independence and authority to make decisions and changes.
- Provide reasonable support using available resources and be ready to discuss with Top Management & the Board for further support for additional resources.

Step 4: Incremental wins.

- Announce wins proudly and make a "display' on how the win impacted the department and the company.
- Strive to branch out to multiple groups until the coverage can be considered "company-wide".

Infiltrative Implementation

- Due to "infantile risk maturity", all level of authority will be against any new initiative or implementations.
- This is most common for companies that treat Risk Management as "compliance only" initiative (establishing risk department and hiring risk practitioners not for progress but to simply meet regulatory requirements).
- In this case, infiltrative implementation will be the most optimal option to shape a risk culture.

Step 1: Inject subtle risk-based awareness.

- Most cases, risk practitioners will be discouraged due to push-back from all sides, however, this can be strategically tackled by using a "Prolonged Exposure Theory".

- For context, “Prolonged Exposure Theory” is derived from the practice of psychology. This theory is a method where individuals **face a feared stimulus repeatedly and safely**, instead of avoiding it.
- Risk practitioners can leverage this theory for the implementation of Risk Culture.

Use of Prolonged Exposure Method

i. Deriving from the “Prolonged Exposure Theory”, Prolonged Exposure method is devised for the sake of infiltrative risk culture implementation.

ii. How to do it?

- This is a “no-noise” subconscious method to expose individuals to align to certain behaviours.
- Pick a target group for infiltrative implementation. Once determined, the risk practitioner will begin with visual & audio exposure.
- Risk practitioner may provide risk awareness materials *indirectly* such as:
  - ✓ Including non-related individuals on unofficial risk related discussions.
  - ✓ Use repetitive humour to non-risk related interactions with conversations like:
    “Join us for badminton?” > “You all go ahead. *Risk Management*, I don’t want to keep winning”.

    “Lunch” > “I’m good. *Risk Management*, I don’t want to be broke by the end of the month”.

  - ✓ Stick tangible risk advice (posters, leaving risk notes on whiteboards, email background) indirectly within the line of sight of non-related individuals.

Step 2: Focus on task-based risk training.

- After some time implementing Prolonged Exposure Method, there should be an initiated risk aware pilot group.
- Risk practitioners may begin to convince the pilot group to attend risk training for their specific role/departments/operational functions.
- It is advised to set what training and how many sessions would be sufficient to improve a group's risk behaviour maturity.
- Once a group's risk behaviour matures, begin infiltrative implementation on a new group.

Step 3: Push for Top-Bottom/Bottom-Top implementation

- Once infiltration reach 80% of total departments, risk practitioners should collect information, consolidate and present to highlight impact.
- Using this information, risk practitioner will make another attempt to get approval for RCMF by presenting to the Risk Committee / Top Management / Board of Governance.
- Based on the outcome, risk practitioner can proceed with Top-Bottom/Bottom-Top implementation (subject to outcome of presentation).

4.5. Phase 5: Monitor & Reinforce

Phase 5 objective: *To create a feedback loop that ensures the risk culture implemented remains relevant, dynamic, and prevents relapsing.*

Step 1: Measure Leading & Lagging Indicators

- A complete monitoring mechanism must balance both retrospective (lagging) and predictive (leading) indicators to provide a complete picture of risk culture maturity.

Lagging Indicators:

i. Lagging indicators are typically easier to measure but it leans more towards past trends, the *results* of cultural behaviours.

ii. Examples of lagging indicators:

- **Number and severity of risk events / operational losses:** A strong culture should see a reduction in frequency and impact, especially of those caused by human error or misconduct.
- **Risk Culture Maturity Score:** An index derived from periodic assessments (e.g., surveys, interviews) that tracks progress against the defined Behavioural Pillars.
- **Employee Turnover:** High turnover is a pre-cursor of a toxic culture, including blame, or lack of psychological safety.
- **Audit & Regulatory Findings:** A reduction in repeated audit non-compliance/findings signals that issues are being addressed at a cultural level, not just procedurally.

Leading Indicators:

i. Leading indicators lean towards future possibilities. They provide early warning signals and measure the *drivers* of cultural health.

ii. Examples of leading indicators:

- **"Speak-Up Rate" & Anonymous Reporting Tool Usage** (as defined in Phase 1): A leading indicator of psychological safety.
- **Employee Sentiment Analysis:** Using natural language processing on internal communications (e.g., pulse surveys, feedback tools) to estimate the growth of risk-aware language vs. blame-oriented language.
- **Training Completion Rates & Competency Scores:** Measures the input of knowledge, which is a precursor to behavioural change.
- **Response Time to Identified Issues:** The speed with which teams mobilize to address a near-miss or a control weakness indicates cultural prioritization and ownership.
- **Leadership Actions:** Quantifying the frequency and quality of leadership behaviours that reinforce the target culture (e.g., number of times executives publicly reward transparency, mention risk in decision-making contexts).

Step 2: Setup a Risk Culture Assessment Interval

- Culture cannot be measured with a single implementation using a singular tool.
- A sustainable frequency of assessment must be established to create a reliable time-series for trend analysis.
- The proposed methods and frequency for measuring the organization's risk culture is as follows:

i. **Continuous Monitoring:**
   - **Tool:** Automated dashboards tracking quantitative metrics (e.g., speak-up rate, report usage).
   - **Frequency:** Real-time or daily/weekly refresh.

ii. **Pulse Checks:**
   - **Tool:** Short, anonymous, focused surveys (3-5 questions) on specific cultural pillar (e.g., "I feel safe reporting a mistake.").
   - **Frequency:** Quarterly.

iii. **Deep-Dive Assessment:**
   - **Tool:** A comprehensive review combining the annual employee engagement survey (with embedded risk culture questions), focus groups, behavioural observation, and interviews.
   - **Frequency:** Annually, aligned with the strategic planning cycle.

iv. **Trigger-Based Assessment:**
   - **Tool:** Full cultural diagnostic as outlined in Phase 2.
   - **Frequency:** Initiated automatically after a significant organizational event (e.g., major crisis, merger/acquisition, CEO change, major strategic shift).

- Note: the proposed methods are suggestive. And may be expanded to meet with the Risk Culture objectives.

Step 3: Adapt RCMF to Ensure Relevance

➢ Enforcement is key. Monitoring data will be useless without a mandated process to act on enforcement. This step closes the feedback loop.

i. **Formal Review Cycle:**

- Conduct an annual **Risk Culture Review** chaired by the Chief Risk Officer (or equivalent) with mandatory attendance from HR, Internal Audit, Risk Management and relevant operational leaders.
- Agenda:
  - ✓ **Review Performance:** Analyse the year's data on leading and lagging indicators against targets.
  - ✓ **Identify Root Causes:** Why are certain metrics improving or deteriorating?
  - ✓ **Assess External & Internal Context:** Has the company's strategy, risk appetite, or operating environment changed? Will the target culture need revision?
  - ✓ **Update the Framework:** Based on the findings, formally approve adjustments to impacted areas.
  - ✓ **Re-Communicate and Re-Calibrate:** The updated RCMF must be re-socialized across the organization, just as the original was. This demonstrates that risk culture is not static and that leadership is committed to its evolution.

BIBLIOGRAPHY

1. International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO.
2. IEC 31010, Risk management — Risk assessment techniques
3. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. COSO.
4. Institute of Risk Management (IRM). (2025). *IRM ABC: Advanced Behavioural & Cultural Risk Framework*. IRM.
5. Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINDSPACE: Influencing behaviour for public policy*. Institute for Government and Cabinet Office, UK.
6. Foa, E. B., Hembree, E. A., & Rothbaum, B. O. (2007). *Prolonged Exposure Therapy for PTSD: Emotional Processing of Traumatic Experiences*. Oxford University Press.