ACCURATE AND RELIABLE

INSIGHT PAPER · ENTERPRISE RISK MANAGEMENT

Risk Governance and Resilience

What a successful enterprise risk management framework contains — from culture and ownership through to key risk indicators and operational resilience.

IN THIS PAPER

PUBLISHED BY
EDRAK Global

SUBJECT
ERM frameworks, policy and operational resilience

PREPARED FOR
Boards, risk officers and internal audit

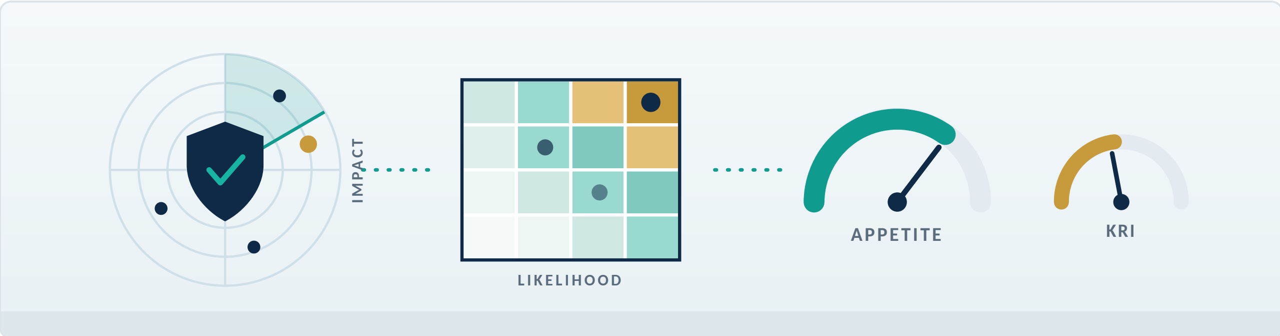
ENQUIRIES
info@edrakglobal.com
edrakglobal.com

01 — THE FRAMEWORK

Risk governance structures

A successful ERM framework allows an organisation to detect future risks and opportunities.

By using the right **KPIs and KRIs**, organisations not only optimise the decisions they make about risk appetite and future strategy, but also measure the effectiveness of ERM itself.



Detection, assessment and monitoring: an ERM framework is only as good as the indicators that feed it.

02 — CULTURE

The single greatest hurdle

The single greatest hurdle to successful ERM is **articulating and integrating risk management into the organisation's culture**. In one sense risk management is part of the culture no matter what is articulated in policy — an organisation can have a cavalier approach to risk taking, a structured approach to risk taking and oversight thereof, or anywhere in between. The organisation needs to clearly spell out how it approaches risk taking, ownership, management, and ongoing monitoring of risk.

Risk governance and policies

How good you are at overseeing risk taking. A risk governance structure is critical for organisations to establish the right governance for risk management, and specifically how it is aligned with strategic planning and objective/performance management.

> ### A common point of failure
>
> This is a big area of failure for most ERM programmes, when it is often the case that risk management operates as an island with very little interaction with the board and executives, or with organisational strategy and objectives. A solid ERM policy will identify how the board and its committees interact with ERM as well as senior executives.

Roles and responsibilities

Once the governance structure is in place, the policy should get into specific roles and responsibilities for ERM. This includes a clear understanding of the roles of:

- A Chief Risk Officer
- Executive management
- Business operations
- Risk owners across the business
- Risk management staff
- The role of audit in the assurance oversight of risk management

Risk strategy

Following on the heels of risk culture, the ERM policy should next deal with **how ERM aligns and integrates with corporate performance, objective, and strategy management**.

03 — BOUNDARIES

Appetite, tolerance and ownership

?

Risk tolerance and appetite

How much risk are we willing to take? The next logical sequence in the ERM policy is to establish the boundaries of risk taking. In articulating the organisation's approach and boundaries to risk tolerance and appetite, the policy should discuss what is acceptable and unacceptable risk.

Risk ownership

You cannot hold anyone accountable for risk unless clear ownership of risk is defined. While specific ownership of individual risks is found in supporting risk management policies — vendor risk, privacy, credit risk, information risk — the ERM policy should state the ownership of risk at the high-level categories.

The risk function does not own risk

It should be clear on the point that the risk management function does not own risk: **the business and process owners are the ones that own risk**. The ERM process is there to communicate and provide the infrastructure to manage and monitor risk to support the risk owners across the business.

Risk assessment process

The ERM policy is to authorise the formation of risk assessment processes in the organisation. The policy itself should outline the expectations of required periodic assessments — such as an annual ERM assessment process — and authorise the establishment of more specific risk assessments in supporting risk management policies. This section should identify the approval needed to establish a risk assessment, what structure is provided, and how the assessment gets communicated and integrated into the ERM structure.

04 — RESPONSE

Mitigation, indicators and documentation

1. **Mitigation and response**

   The ERM policy should articulate the proper response plans to risk — risk transfer, risk acceptance, risk mitigation, and risk avoidance — while much of the detail is worked out in supporting risk policies.

2. **Key risk indicators**

   Ongoing monitoring for risk is critical to a successful ERM programme. This involves the authorisation and establishment of a process to gather metrics on Key Risk Indicators that are further defined in supporting policies. The ERM policy should provide guidance on how KRI information is collected, how often, and establish that KRIs are to be relevant to the business and mapped to Key Performance Indicators of the business.

3. **Risk documentation and communication**

   Documentation of risk, risk taking, risk acceptance and ownership, as well as assessment, management, and monitoring activities for risk, are critical to a successful ERM programme. An organisation cannot hold individuals accountable for risk taking if there is not clear documentation on the risk.

FOUR RESPONSES	KRIS	ACCOUNTABILITY
Transfer, accept, mitigate, avoid	**Mapped to KPIs**	**Requires documentation**
Set out in the ERM policy	Relevant to the business, collected on a defined cycle	No record, no accountability

Four responses to risk

- Risk transfer
- Risk acceptance
- Risk mitigation
- Risk avoidance

05 — RESILIENCE

Operational resilience

The operational challenges brought on by the COVID-19 crisis have forced companies to rethink what it means to be resilient.

It is imperative that organisations address emerging risks that can hinder the business from fulfilling its commitments to customers and other stakeholders. Accountants are trained to understand how business models work, so they should make sure the necessary measures are in place and the right questions asked.

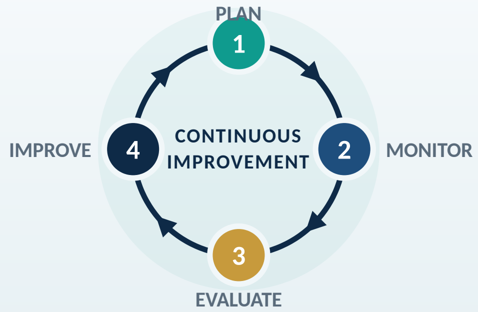
Operational risks depend on the organisation's activities but require **constant assessment, analysis and adaptation** if the organisation is to be able to address the unique challenges of every type of disruption. Operational resiliency is another risk journey that must be defined from the top, by the board, and include the engagement of all business units and the people working within them.

> **The lesson learned is that operational resilience demands long-term investment of resources and time.**

By focusing on critical activities and testing their processes, controls and documentation, organisations can start laying valuable foundations for a more resilient future. Accountants can help their organisations with this by creating **specific metrics for the tolerable levels of operational disruption**.

Governance, resilience, risk and control

Together these ensure effective and appropriate governance, allowing evaluation, monitoring and implementation of appropriate risk identification procedures — by designing and implementing effective internal audit and control systems.



Assessment, analysis and adaptation: resilience is maintained rather than achieved.

Reviewing your ERM framework?

To learn more about risk governance structures, ERM policy and operational resilience, please contact us.

info@edrakglobal.com

EDRAK Global · Accurate and Reliable · edrakglobal.com