Risk Management Best Practice Guide

A practical governance and assurance framework for UK organisations

Prepared by Nadia Saleh

Copyright, Licensing and Permitted Use

Executive Summary (One Page)

Risk management is a fundamental component of effective governance and leadership. It enables organisations to protect value, support informed decision-making, and achieve strategic and operational objectives in an uncertain environment.

In the UK, boards and senior leaders are responsible for establishing and maintaining a sound system of risk management and internal control. This includes setting a clear risk appetite, identifying principal risks, ensuring appropriate controls are in place, and reviewing the effectiveness of those controls on a regular basis.

Effective risk management is not about eliminating risk, but about understanding uncertainty and making proportionate, well-informed decisions. Minimum expectations include up-to-date risk registers, clear ownership of risks, regular reporting to senior leadership and the board, and a culture that encourages openness and escalation.

Common failures include treating risk management as a compliance or “tick-box” exercise, outdated or overly complex risk registers, unclear accountability, and insufficient challenge at senior levels.

A strong risk management framework supports confident leadership, resilience, regulatory compliance, and sustainable success.

---

1. Definition of Risk Management

Risk management is the systematic process by which an organisation identifies, assesses, manages, monitors, and reports risks that could affect the achievement of its objectives.

In a business and governance context, risk management:

- Protects the organisation from financial, legal, operational, and reputational harm
- Supports informed strategic and operational decision-making

- Enables innovation by understanding and managing uncertainty
- Strengthens accountability, assurance, and governance

Risk management is not about avoiding all risk. It is about understanding risk in line with organisational objectives and risk appetite, and applying proportionate controls.

---

2. Legislative and Regulatory Framework (UK / EU)

Risk management in the UK and EU is shaped by a combination of legislation, regulation, and recognised governance standards rather than a single statutory requirement.

Key UK Legislation

- Health and Safety at Work etc. Act 1974

  Requires employers to assess and manage risks to employees and others.

- Management of Health and Safety at Work Regulations 1999

  Introduces mandatory risk assessments and preventive controls.

- Companies Act 2006

  Requires directors to exercise reasonable care, skill, and diligence and to consider principal risks.

- Corporate Manslaughter and Corporate Homicide Act 2007

  Links failures in risk management to criminal liability.

- Data Protection Act 2018 (UK GDPR)

  Requires identification and management of data protection and privacy risks.

Governance Codes and Standards

- UK Corporate Governance Code

Requires boards to maintain sound risk management and internal control systems and to identify principal risks.

- HM Treasury – Orange Book (Public Sector)

  Sets out risk management principles for government bodies.

- ISO 31000 – Risk Management Guidelines

  International best-practice framework applicable across sectors.

- COSO Enterprise Risk Management Framework

  Widely used in large and regulated organisations.

---

3. Core Principles of Effective Risk Management

Effective risk management should be:

- Integrated – embedded into strategy, planning, and daily operations
- Proportionate – focused on what matters most
- Clearly owned – with defined accountability at all levels
- Forward-looking – identifying emerging and future risks
- Regularly reviewed – reflecting changes in the organisation and environment
- Culturally embedded – supported by openness and transparency

---

4. Risk Management Process

A typical risk management process includes:

1. Establishing context

   Understanding objectives, operating environment, and risk appetite

2. Identifying risks

   Strategic, operational, financial, legal, reputational, people, and technology risks

3. Assessing risks

   Evaluating likelihood and impact (inherent and residual risk)

4. Treating risks

   Avoid, reduce, transfer, tolerate, or exploit

5. Monitoring and reviewing

   Assessing control effectiveness and changes in risk profile

6. Reporting and escalation

   Providing timely information to senior management and the board

---

5. Documentation Checklist

An effective risk management framework is supported by appropriate documentation. As a minimum, organisations should have:

Governance

- Risk Management Policy
- Risk Appetite Statement
- Defined roles and responsibilities (board, executive, management)

Risk Identification and Assessment

- Corporate Risk Register
- Departmental / project risk registers
- Risk scoring and assessment methodology
- Summary of principal risks

Controls and Assurance

- Internal control framework

- Key risk indicators (KRIs)
- Incident and near-miss reporting process
- Business Continuity Plan
- Disaster Recovery Plan
- Health and safety risk assessments
- Data Protection Impact Assessments (where applicable)

Monitoring and Reporting

- Regular risk reports to senior leadership and the board
- Risk review timetable
- Internal and external audit reports
- Lessons-learned logs

---

6. Common Mistakes in Risk Management

Organisations frequently weaken their risk management frameworks by:

- Treating risk management as a compliance or tick-box exercise
- Failing to link risks to strategic objectives
- Maintaining outdated or overly complex risk registers
- Lacking clear ownership and accountability
- Focusing only on low-level operational risks
- Discouraging escalation through blame or punitive cultures
- Failing to learn from incidents and near misses
- Providing risk reports without meaningful analysis or challenge

---

7. What Good Looks Like

A mature risk management framework:

- Supports confident, informed decision-making
- Protects organisational value and reputation
- Identifies and manages principal and emerging risks
- Is proportionate to organisational size and complexity
- Is embedded into governance, strategy, and culture
- Evolves continuously as the organisation changes
