HM Government

The Orange Book

Management of Risk – Principles and Concepts

Term	Intention
shall	denotes a requirement: a mandatory element
should	denotes a recommendation: an advisory element
may	denotes approval
might	denotes a possibility
can	denotes both capability and possibility
is/are	denotes a description

References are shown in square brackets [] and listed in Annex 6.

The meaning of words is as defined in the Shorter Oxford English Dictionary, except where defined in Annex 5. It is assumed that legal and regulatory requirements shall always be met.

Produced by Mark Ripley, Government Finance Function

Alternative format versions of this report are available on request from GovFinance@hmtreasury.gov.uk

Contents

Introduction

In successful organisations, risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. If we are serious about meeting objectives successfully, improving service delivery and achieving value for money, risk management must be an essential and integral part of planning and decision-making. While risk practices have improved over time across government, the volatility, complexity and ambiguity of our operating environment has increased, as have demands for greater transparency and accountability for managing the impact of risks. This updated guidance builds on the previous Orange Book to help improve risk management further and to embed this as a routine part of how we operate.

Public sector organisations cannot be risk averse and be successful. Risk is inherent in everything we do to deliver high-quality services. Effective and meaningful risk management in government remains as important as ever in taking a balanced view to managing opportunity and risk. It must be an integral part of informed decision-making; from policy or project inception through implementation to the everyday delivery of public services. At its most effective, risk management is as much about evaluating the uncertainties and implications within options as it is about managing impacts once choices are made. It is about being realistic in the assessment of the risks to projects and programmes and in the consideration of the effectiveness of the actions taken to manage these risks.

This isn't about adding new processes; it is about ensuring that effective risk management is integrated in the way we lead, direct, manage and operate. As an integrated part of our management systems, and through the normal flow of information, an organisation's risk management framework harnesses the activities that identify and manage the uncertainties faced and systematically anticipate and prepare successful responses. Its importance and value to success should not be underestimated.

As with all aspects of good governance, the effectiveness of risk management depends on the individuals responsible for operating the systems put in place. Our risk culture must embrace openness, support transparency, welcome constructive challenge and promote collaboration, consultation and co-operation. We must invite scrutiny and embrace expertise to inform decision-making. We must also invest in the necessary capabilities and seek to continually learn from experience.

This updated guidance has benefited from discussions with stakeholders and practitioners across the public sector and with colleagues from the private sector. We are grateful for their time and their valuable insights.

Scope

The document updates the version published in 2004. Like the original, it sets out the main principles underlying effective risk management in all government departments and arm's length public bodies[1] with responsibility derived from central government for public funds.

This document may be useful to all parts of the UK public sector, as the same principles generally apply, with adjustments for context.

Purpose

This document is intended for use by everyone involved in the design, operation and delivery of efficient, trusted public services. Its primary audience is likely to be:

- executive and non-executive members of the board;
- Audit and Risk Assurance Committee members;
- risk practitioners;
- senior leadership;
- policy leads; and
- programme and project Senior Responsible Officers (SROs).

The board of each public sector organisation should actively seek to recognise risks and direct the response to these risks. It is for each accounting officer, supported by the board, to decide how. The board and accounting officer should be supported by an Audit and Risk Assurance Committee, who should provide proactive support in advising on and scrutinising the management of key risks and the operation of efficient and effective internal controls.

Attempting to define a one-size-fits-all approach to managing risks, or to standardise risk management practices, would be misguided because public sector organisations are different sizes, are structured differently and have different needs.

This document does not set out the procedure by which an organisation should design and operate risk management. It sets out a principles-based approach that provides flexibility and judgement in the design, implementation and operation of risk management, informed by relevant standards[1] and good practice. Where relevant, the reader is directed to other standards and guidance, including related functional and professional standards and codes of practice (see Annex 6). References throughout the document are shown in square brackets [].

The Management of Risk framework is available through AXELOS[2], who manage guides that comprise the recommended best practice for government project delivery and provide advice on their application.

Comply or Explain

The document sets out main and supporting principles for risk management in government. In considering the effectiveness of risk management arrangements, assessing compliance with *Corporate Governance Code*[2] requirements, and overseeing the preparation of the governance

1 Executive Agencies, Non Departmental Public Bodies and Non Ministerial Departments.

2 AXELOS is a company part owned by the UK government. Their guides are available by subscription or individual purchase.

statement, the board shall consider adherence with the main principles, which are mandatory requirements. The supporting principles, which are advisory, should inform their judgements. Departures may be justified if good risk management can be achieved by other means.

The main principles are the core of the document. The way in which they are applied should be the central question for a board as it determines how it is to operate in accordance with the Corporate Governance Code. Each government organisation is required either to disclose compliance or to explain their reasons for departure clearly and carefully in the governance statement accompanying their annual resource accounts. The requirement for an explanation allows flexibility, but also ensures that the process is transparent, allowing stakeholders to hold organisations and their leadership to account.

Structure

The core document is structured around Sections (A-E), based on principles that are designed to provide the "what" and the "why", not the "how", for the design, operation and maintenance of an effective risk management framework.

The principles can be applied within and across departments, arm's length bodies and organisations with linked objectives, and to activity at any level of decision-making.

The principles should be used to inform an organisation's approach to risk management and its own more detailed policies, processes and procedures – the "how". Implementing and improving the risk management framework should support an incremental approach to enhancing risk management culture, processes and capabilities over time, building on what already exists to achieve improved outcomes.

The primary roles and responsibilities for the risk management framework are set out in each Section. The responsibilities and expectations of the board, the accounting officer and the Audit and Risk Assurance Committee are also summarised at Annex 1.

Some explanation of, and guiding principles on, the design and operation of the "three lines of defence" model are provided in Annex 2.

Annex 3 contains questions that may assist in assessing how the principles are applied in defining clear responsibilities, promoting the risk culture, developing capabilities and supporting the effectiveness of the risk management framework.

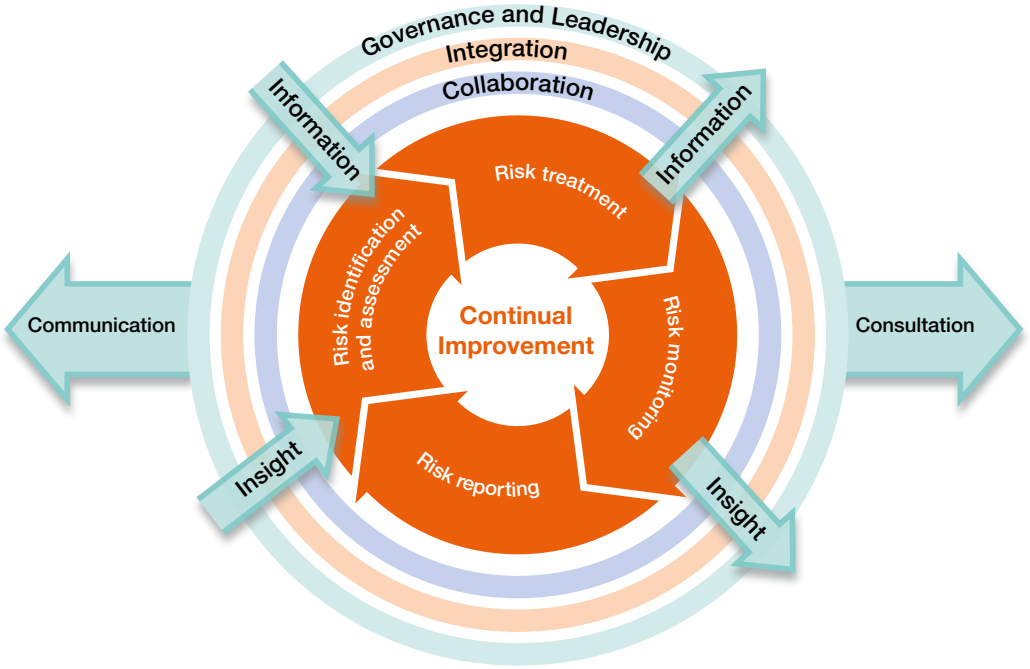
Some common categories or groupings of sources of risk are provided at Annex 4. These may help consider the range of potential risks that may arise; they are not intended to be comprehensive.

Definitions and supportive concepts are provided at Annex 5 of some terms used throughout this document to explain the scope and intended meaning behind the language used.

Annex 6 contains further details of other standards and guidance referenced throughout the document.

Risk Management Principles

Risk Management Framework



The risk management framework supports the consistent and robust identification and management of opportunities and risks within desired levels across an organisation, supporting openness, challenge, innovation and excellence in the achievement of objectives. For the risk management framework to be considered effective, the following principles shall be applied:

A. Risk management shall be an essential part of **governance and leadership**, and fundamental to how the organisation is directed, managed and controlled at all levels.

B. Risk management shall be an **integral** part of all organisational activities to support decision-making in achieving objectives.

C. Risk management shall be **collaborative and informed** by the best available information and expertise.

D. Risk management processes shall be **structured** to include:

   a. **risk identification and assessment** to determine and prioritise how the risks should be managed;

   b. the selection, design and implementation of **risk treatment** options that support achievement of intended outcomes and manage risks to an acceptable level;

   c. the design and operation of integrated, insightful and informative **risk monitoring**; and

   d. timely, accurate and useful **risk reporting** to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

E. Risk management shall be **continually improved** through learning and experience.

Section A: Governance and Leadership

Main Principle

A **Risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.**

Supporting Principles

A1 Each public sector organisation should establish governance arrangements appropriate to its business, scale and culture[3]. Human behaviour and culture significantly influence all aspects of risk management at each level and stage. To support the appropriate risk culture, the accounting officer should ensure that expected values and behaviours are communicated and embedded at all levels.

A2 The accounting officer, supported by the board, should periodically assess whether the leadership style, opportunities for debate and human resource policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours. Where they are not satisfied, they should direct and manage corrective actions and seek assurances that the desired risk culture and behaviours are promoted.

CS Code/Brilliant CS values

Brilliant CS

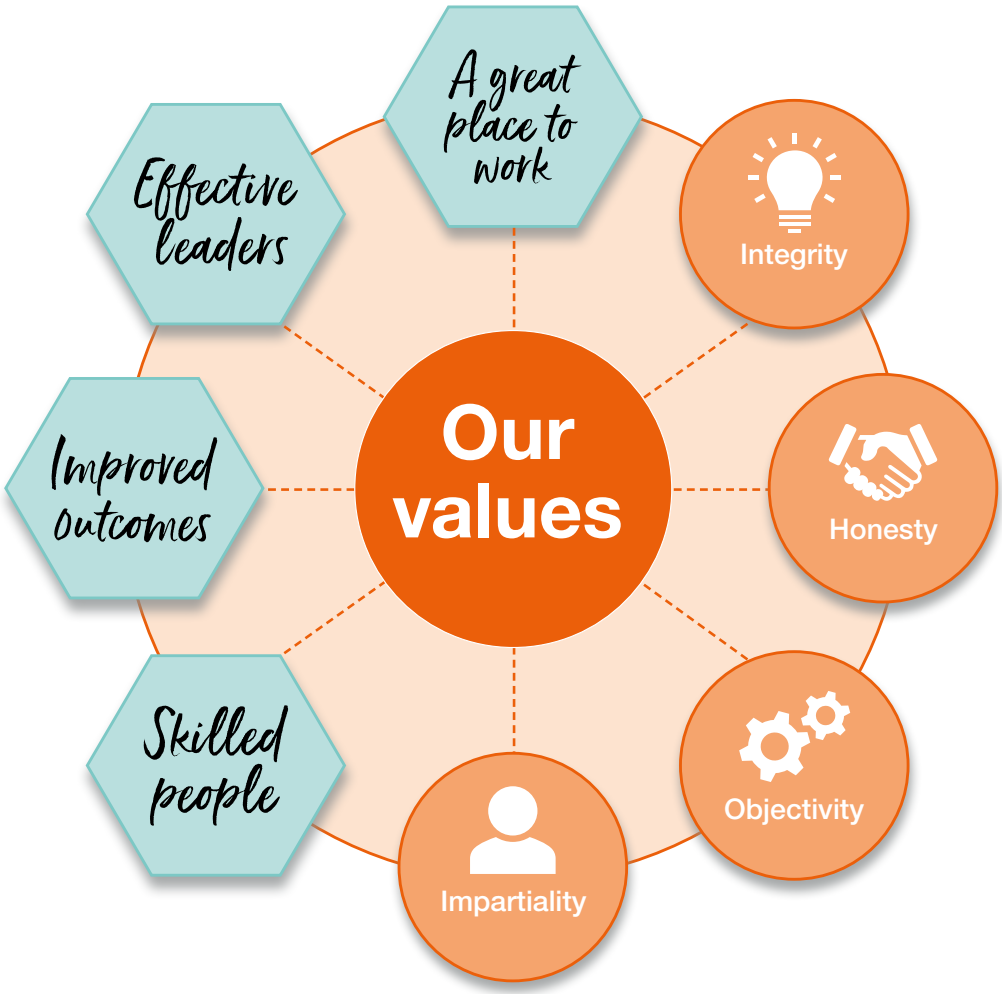
CS Code

'integrity' is putting the obligations of public service above your own personal interests

'honesty' is being truthful and open

'objectivity' is basing your advice and decisions on rigorous analysis of the evidence

'impartiality' is acting solely according to the merits of the case and serving equally well governments of different political persuasions



A3 The board should make a strategic choice about the style, shape and quality of risk management[4] and should lead the assessment and management of opportunity and risk. The board should determine and continuously assess the nature and extent of the principal risks[3] that the organisation is exposed to and is willing to take to achieve its objectives - its risk appetite – and ensure that planning and decision-making reflects this assessment. Effective risk management should support informed decision-making in line with this risk appetite, ensure confidence in the response to risks and ensure transparency over the principal risks faced and how these are managed.

3 A principal risk is a risk or combination of risks that can seriously affect the performance or reputation of the organisation.

A4 The board should ensure that roles and responsibilities for risk management are clear, to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation. The accounting officer should ensure that roles and responsibilities are communicated, understood and embedded at all levels. The "three lines of defence model" provides a systematic approach that may be used to help clarify the specific roles and responsibilities that are necessary for the effective management of risks within an organisation (see Annex 2).

A5 The board should agree the frequency and scope of its discussions to review how management is responding to the principal risks and how this is integrated with other matters, including planning and performance management processes. Risk should be considered regularly as part of the normal flow of management information about the organisation's activities and in significant decisions on strategy, major new projects and other prioritisation and resource allocation commitments. Risk management should anticipate, detect, acknowledge and respond to changes and events in an appropriate and timely manner. Risks can crystallise quickly; the board and Audit and Risk Assurance Committee should ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so as a part of risk reporting (see Section D).

A6 Regular reports to the board should provide a balanced assessment of the principal risks and the effectiveness of risk management. The accounting officer, supported by the Audit and Risk Assurance Committee, should monitor the quality of the information they receive and ensure that it is sufficient to allow effective decision-making.

A7 The accounting officer, supported by the Audit and Risk Assurance Committee, should establish the organisation's overall approach to risk management. An effective risk management framework will differ between organisations depending on their purpose, objectives, context and complexity. The risk management framework should be periodically reviewed to ensure it remains appropriate (see Section E).

A8 The accounting officer should designate an individual to be responsible for leading the organisation's overall approach to risk management, who should be of sufficient seniority and should report to a level within the organisation that allows them to influence effective decision-making. They should be proactively involved with and influence governance and decision-making forums and should establish, and be supported through, effective communication and engagement with the accounting officer, senior management, the board and the chair of the Audit and Risk Assurance Committee. They should also exhibit a high level of objectivity in gathering, evaluating and communicating information and should not be unduly influenced by their own interests or by others in forming and expressing their judgements.

A9 The accounting officer should ensure the allocation of appropriate resources for risk management, which can include, but is not limited to, people, skills, experience and competence.

A10 The accounting officer, supported by senior management, must demonstrate leadership and articulate their continual commitment to, and the value of, risk management through developing and communicating a policy or statement to the organisation and other stakeholders, which should be periodically reviewed.

Section B: Integration

Main Principle

B Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

Supporting Principles

B1 The assessment and management of opportunity and risk should be an embedded part of, and not separate from:

- setting strategy and plans;
- evaluating options and delivering programmes, projects or policy initiatives;
- prioritising resources;
- supporting efficient and effective operations;
- managing performance;
- managing tangible and intangible assets;[5] and
- delivering improved outcomes.

The accounting officer, supported by senior management, should ensure that risks are transparent and considered as an integral part of appraising options, evaluating alternatives and making informed decisions.

B2 Effective appraisal supports the assessment of the costs, benefits and risks of alternative ways to meet objectives.[6] When conducting an appraisal, consideration should be given to the identification and analysis of risks in the design and implementation of options, including: analysis of varying scenarios, sensitivity in forecasts, the objective or subjective basis of assumptions, optimism or status quo bias, dependencies and the inter-relationships between risks. This analysis and evaluation should provide the foundation to understand the risks arising through chosen options and how these will be managed, including how these will be subject to effective and on-going monitoring (see Section D).

B3 Delivery confidence should be supported through the transparent identification of the principal risks faced and how those risks will be managed within business and financial plans.

B4 The board, and those setting strategy and policy, should use horizon scanning and scenario planning collectively and collaboratively to identify and consider the nature of emerging risks, threats and trends. The Government Office for Science ensures that government policies and decisions are informed by the best scientific evidence and strategic long-term thinking.[7] Some other common horizon scanning issues are informed by the Civil Contingencies Secretariat through the National Risk Assessment (NRA).[8]

B5 Government has an inherent role in protecting and assuring the public, which includes taking cost-effective action to reduce risk to a tolerable level and providing accurate and timely information about risks to the public.[9] Policy leads should take explicit steps to involve the public, understand what they are concerned about and why and communicate good information about risk that is targeted to the needs of the audiences involved. Government will:

- be open and transparent about its understanding of the nature of risks to the public and about the process it is following in handling them;
- seek wide involvement of those concerned in decision-making processes;
- act proportionately and consistently in dealing with risks to the public;
- base decisions for intervention on relevant evidence, including expert risk assessment; and
- place responsibility for managing risks to those best able to control them.

Section C: Collaboration and Best Information

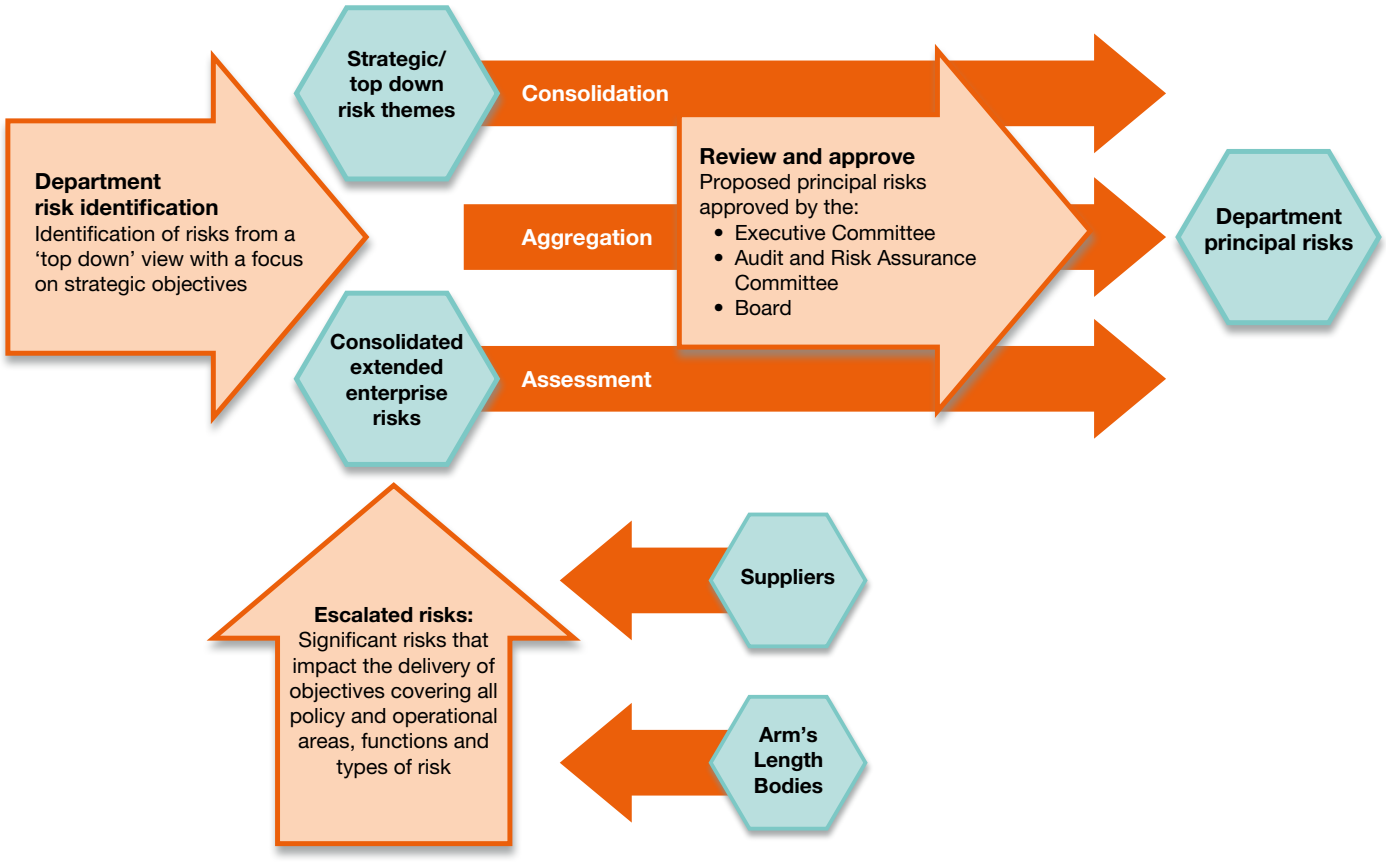
Main Principle

C Risk management shall be collaborative and informed by the best available information and expertise.

Supporting Principles

C1 The accounting officer, supported by the Audit and Risk Assurance Committee, should establish risk management activities that cover all types and source of risk (see Annex 4). There may be many different, but aligned, risk management processes that are applied at different levels within an organisation and across those involved in the end to end delivery of public services. The management of risks and the operation and oversight of internal control should be considered and aligned across this extended enterprise. This requires collaboration and cross-organisational working through a range of public sector, private sector and third-sector partnerships. The risk management framework should be designed to support a comprehensive view of the risk profile, aggregated where appropriate, in support of governance and decision-making requirements.

Risk escalation, consolidation and aggregation



C2 Nearly all government departments sponsor arm's length bodies for which they take ultimate responsibility, while allowing a degree of (or sometimes considerable) independence. Effective relationships and partnership working between departments and arm's length bodies, a mutual understanding of risk, and a proportionate approach to monitoring and reporting are critical. The principal accounting officer[4] should consider the organisation's overall risk profile, including the risk management within arm's length bodies, who should have their own robust and aligned arrangements in place. Informative and transparent management information should enable departments and arm's length bodies to promote transparency and understanding in achieving the effective management of risks, including the timely escalation of risks, as necessary, based on agreed criteria.

C3 Risk management processes (see Section D) should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of experts and stakeholders. Information and perspectives should be supplemented by further enquiry as necessary, should reflect changes over time and should be appropriately evidenced. Expert risk assessment methodologies may be highly specialised and may vary depending on the context.

C4 Those assessing and managing risks should consult with appropriate external and internal stakeholders to facilitate the factual, timely, relevant, accurate and understandable exchange of information and evidence, while considering the confidentiality and integrity of this information. Communication should be continual and iterative in supporting dialogue, providing and sharing information and promoting awareness and understanding of risks.

C5 Communication and consultation should also assist relevant stakeholders in understanding the risks faced, the basis on which decisions are made and the reasons why particular actions are required and taken. Communication and consultation should:

- bring together different functions and areas of professional expertise in the management of risks;
- ensure that different views are appropriately considered when defining risk criteria and when analysing risks (see Section D);
- provide sufficient information and evidence to facilitate risk oversight and decision making; and
- build a sense of inclusiveness and ownership among those affected by risk.

Complicated and ambiguous risk scenarios are inherent given the dynamic and/or behavioural complexity in public service delivery, often with no simple, definitive solutions. These risks require whole-system-thinking, aligned incentives, positive relationships and collaboration, alongside relevant technical knowledge, to support multi-disciplinary approaches to their effective management.

4 The Treasury appoints the permanent head of each central government department to be its accounting officer. Where there are several accounting officers in a department, the permanent head is the principal accounting officer.

C6 Functions[5] within and across organisations should play an integral part in identifying, assessing and managing the range of risks than can arise and threaten successful delivery against objectives. Function leads should provide expert judgement to advise the accounting officer to:

- set feasible and affordable strategies and plans;
- evaluate and develop realistic programmes, projects and policy initiatives;
- prioritise and direct resources and the development of capabilities;
- identify and assess risks that can arise and impact the successful achievement of objectives;
- determine the nature and extent of the risks that the organisation is willing to take to achieve its objectives;
- design and operate internal controls in line with good practice; and
- drive innovation and incremental improvements.

5 Functions are embedded in government departments and arm's length bodies, helping to deliver departmental objectives and better outcomes across government.

Section D: Risk Management Processes

Main Principle

D **Risk management processes shall be structured to include:**

a. **risk identification and assessment to determine and prioritise how the risks should be managed;**

b. **the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;**

c. **the design and operation of integrated, insightful and informative risk monitoring; and**

d. **timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.**

Risk Management Processes

Supporting Principles

D1 The accounting officer, supported by their nominated individual responsible for leading the organisation's overall approach to risk management, should ensure the adequate design and systematic implementation of policies, procedures and practices for risk identification and assessment, treatment, monitoring and reporting. Although risk management processes are often presented as sequential, in practice they are iterative.

Risk identification and assessment

D2 Risk identification activities should produce an integrated and holistic view of risks, often organised by taxonomies or categories of risk (see Annex 4). The aim is to understand the organisation's overall risk profile. The organisation can use a range of techniques for identifying specific *risks* that may potentially impact on one or more objectives. The following factors, and the relationship between these factors, should also be considered:

- tangible and intangible sources of risk;
- changes in the external and internal context;
- uncertainties and assumptions within options, strategies, plans, etc;
- indicators of emerging risks;
- limitations of knowledge and reliability of information; and
- any potential biases and beliefs of those involved.

Risks should be identified whether or not their sources are under the organisation's direct control. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity.

D3 While each risk identified may be important, some form of measurement is necessary to evaluate their significance to support decision-making. Without a standard for comparison, it is not possible to compare and aggregate risks across the organisation and its extended enterprise. This prioritisation is supported by risk assessment[10], which incorporates risk analysis and risk evaluation.

D4 The purpose of risk analysis is to support a detailed consideration of the nature and level of risk. The risk analysis process should use a common set of risk criteria to foster consistent interpretation and application in defining the level of risk, based on the assessment of the *likelihood* of the risk occurring and the *consequences* should the *event* happen (see Annex 5).

D5 Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of evidence and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use. Limitations and influences associated with the information and evidence bases used, and/or the analysis techniques executed, should be explicitly considered. These should be correctly sourced, appraised and referenced within risk reporting to decision-makers. All business critical analytical models in government should be managed within a framework that ensures appropriately specialist staff are responsible for developing and using the models as well as their quality assurance[11].

D6 Risk evaluation should involve comparing the results of the risk analysis with the nature and extent of risks that the organisation is willing to take - its risk appetite - to determine where and what additional action is required. Options may involve one or more of the following:

- avoiding the risk, if feasible, by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- retaining the risk by informed decision;
- changing the likelihood, where possible;
- changing the consequences, including planning contingency activities;
- sharing the risk (e.g. through commercial contracts[12]).

The outcome of risk evaluation should be recorded, communicated and validated at appropriate levels of the organisation. It should be regularly reviewed and revised based on the dynamic nature and level of the risks faced.

Risk treatment

D7 Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in enhancing the achievement of objectives against the costs, efforts or disadvantages of proposed actions. Justification for the design of risk treatments and the operation of *internal control* is broader than solely economic considerations and should take into account all of the organisation's obligations, commitments and stakeholder views.

D8 As part of the selection and development of risk treatments, the organisation should specify how the chosen option(s) will be implemented, so that arrangements are understood by those involved and effectiveness can be monitored. This should include:

- the rationale for selection of the option(s), including the expected benefits to be gained;
- the proposed actions;
- those accountable and responsible for approving and implementing the option(s);
- the resources required, including contingencies;
- the key performance measures and control indicators, including early warning indicators;
- the constraints;
- when action(s) are expected to be undertaken and completed; and
- the basis for routine reporting and monitoring.

D9 Where appropriate, contingency, containment, crisis, incident and continuity management arrangements should be developed and communicated to support resilience and recovery if risks crystallise.

Risk monitoring

D10 Monitoring should play a role before, during and after implementation of risk treatment. Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of organisational objectives.

D11 The results of monitoring and review should be incorporated throughout the organisation's wider performance management, measurement and reporting activities. Recording and reporting aims to:

- transparently communicate risk management activities and outcomes across the organisation;
- provide information for decision-making;

- improve risk management activities; and
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

D12 The "three lines of defence" model sets out how these aspects should operate in an integrated way to manage risks, design and implement internal control and provide *assurance* through ongoing, regular, periodic and ad-hoc monitoring and review (see Annex 2). When an organisation has properly structured the "lines of defence", and they operate effectively, it should understand how each of the lines contributes to the overall assurance required and how those involved can best be integrated and mutually supportive. There should be no gaps in coverage and no unnecessary duplication of effort. Importantly, the accounting officer and the board should receive unbiased information about the organisation's principal risks and how management is responding to those risks.

Risk reporting

D13 The board, supported by the Audit and Risk Assurance Committee, should specify the nature, source, format and frequency of the information that it requires. It should ensure that the assumptions and models underlying this information are clear so that they can be understood and, if necessary, challenged. Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting; and
- relevance of information to organisational objectives and decision-making.

D14 The information should support the board to assess whether decisions are being made within its risk appetite to successfully achieve objectives, to review the adequacy and effectiveness of internal controls, and to decide whether any changes are required to re-assess strategy and objectives, revisit or change policies, reprioritise resources, improve controls, and/or alter their risk appetite.

D15 Clear, informative and useful reports or dashboards should promote key information for each principal risk to provide visibility over the risk, compare results against key performance/risk indicators, indicate whether these are within risk appetite, assess the effectiveness of key management actions and summarise the assurance information available. Reports should include qualitative and quantitative information, where appropriate, show trends and support early warning indicators. Understanding and decision-making should be supported through the presentation of information in summary form and the use of graphics and visualisation.

D16 Principal risks should be subject to “deep dive” reviews by the board and Audit and Risk Assurance Committee, with those responsible for the management of risks and with appropriate expertise present at an appropriate frequency depending on the nature of the risk and the performance reported.

Section E: Continual Improvement

Main Principle

E Risk management shall be continually improved through learning and experience

Supporting Principles

E1 The organisation should continually monitor and adapt the risk management framework to address external and internal changes. The organisation should also continually improve the suitability, adequacy and effectiveness of the risk management framework. This should be supported by the consideration of lessons based on experience and, at least annually, review of the risk management framework and the performance outcomes achieved. Annex 3 contains questions that may assist in assessing the efficient and effective operation of the risk management framework.

E2 All strategies, policies, programmes and projects should be subject to comprehensive but proportionate evaluation[13], where practicable to do so. Learning from experience helps to avoid repeating the same mistakes and helps spread improved practices to benefit current and future work, outputs and outcomes. At the commencement, those involved and key stakeholders should identify and apply relevant lessons from previous experience when planning interventions and the design and implementation of services and activities. Lessons should be continually captured, evaluated and action should be taken to manage delivery risk and facilitate continual improvement of the outputs and outcomes. Organisation leaders and owners of standards, processes, methods, guidance, tools and training, should update their knowledge sources and communicate learning as appropriate.

E3 Process/capability maturity models or continuum may be used to support a structured assessment of how well the behaviours, practices and processes of an organisation can reliably and sustainably produce required outcomes. These models may be used as a benchmark for comparison and to inform improvement opportunities and priorities.

E4 As relevant gaps or improvement opportunities are identified, the organisation should develop plans and tasks and assign them to those accountable for implementation.

Annex 1 – Roles and Responsibilities - Board, Accounting Officer and Audit and Risk Assurance Committee

Board

The board of each public sector organisation, informed and advised by their Audit and Risk Assurance Committee, should:

- lead the assessment and management of risk and take a strategic view of risks in the organisation.
- ensure that there are clear accountabilities for managing risks and that officials are equipped with the relevant skills and guidance to perform their assigned roles effectively and efficiently.
- ensure that roles and responsibilities for risk management are clear to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation.
- determine and continuously assess the nature and extent of the principal risks that the organisation is willing to take to achieve its objectives - its "risk appetite" - and ensure that planning and decision-making appropriately reflect this assessment.
- agree the frequency and scope of its discussions on risk to review how management is responding to the principal risks and how this is integrated with other matters considered by the board, including business planning and performance management processes.
- specify the nature, source, format and frequency of the information that it requires.
- ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so.
- use horizon scanning to identify emerging sources of uncertainty, threats and trends.
- assure itself of the effectiveness of the organisation's risk management framework.
- assess compliance with the Corporate Governance Code[2] and include explanations of any departures within the governance statement of the organisation's annual report and accounts.

Accounting Officer

The accounting officer of each public sector organisation, supported by the Audit and Risk Assurance Committee, should:

- periodically assess whether the organisational values, leadership style, opportunities for debate and learning, and human resource policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours.
- ensure that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture.
- designate an individual to be responsible for leading the organisation's overall approach to risk management, who should be of sufficient seniority and should report to a level within the organisation that allows them to influence effective decision-making.
- establish the organisation's overall approach to risk management
- establish risk management activities that cover all types of risk and processes that are applied at different organisational levels.
- ensure the design and systematic implementation of policies, procedures and practices for risk identification, assessment, treatment, monitoring and reporting.
- consider the organisation's overall risk profile, including risk management within arm's length bodies and the extended enterprise.
- demonstrate leadership and articulate their continual commitment to and the value of risk management through developing and communicating a policy or statement to the organisation and other stakeholders, which should be periodically reviewed.
- ensure the allocation of appropriate resources for risk management, which can include, but is not limited to people, skills, experience and competence.

- monitor the quality of the information received and ensure that it is of a sufficient quality to allow effective decision-making.
- ensure that risk is considered as an integral part of appraising option choices, evaluating alternatives and making informed decisions.
- be provided with expert judgements through functions to advise on:
  - the feasibility and affordability of strategies and plans;
  - the evaluation and development of realistic programmes, projects and policy initiatives;
  - prioritisation of resources and the development of capabilities;
  - the design and operation of internal control in line with good practice and the nature and extent of the risks that the organisation is willing to take to achieve its objectives; and
  - driving innovation and incremental improvements.
- clearly communicate their expectation that risk management activities are coordinated and that information is shared among across the 'lines of defence' where this supports the overall effectiveness of the effort and does not diminish any of the 'lines' key functions.

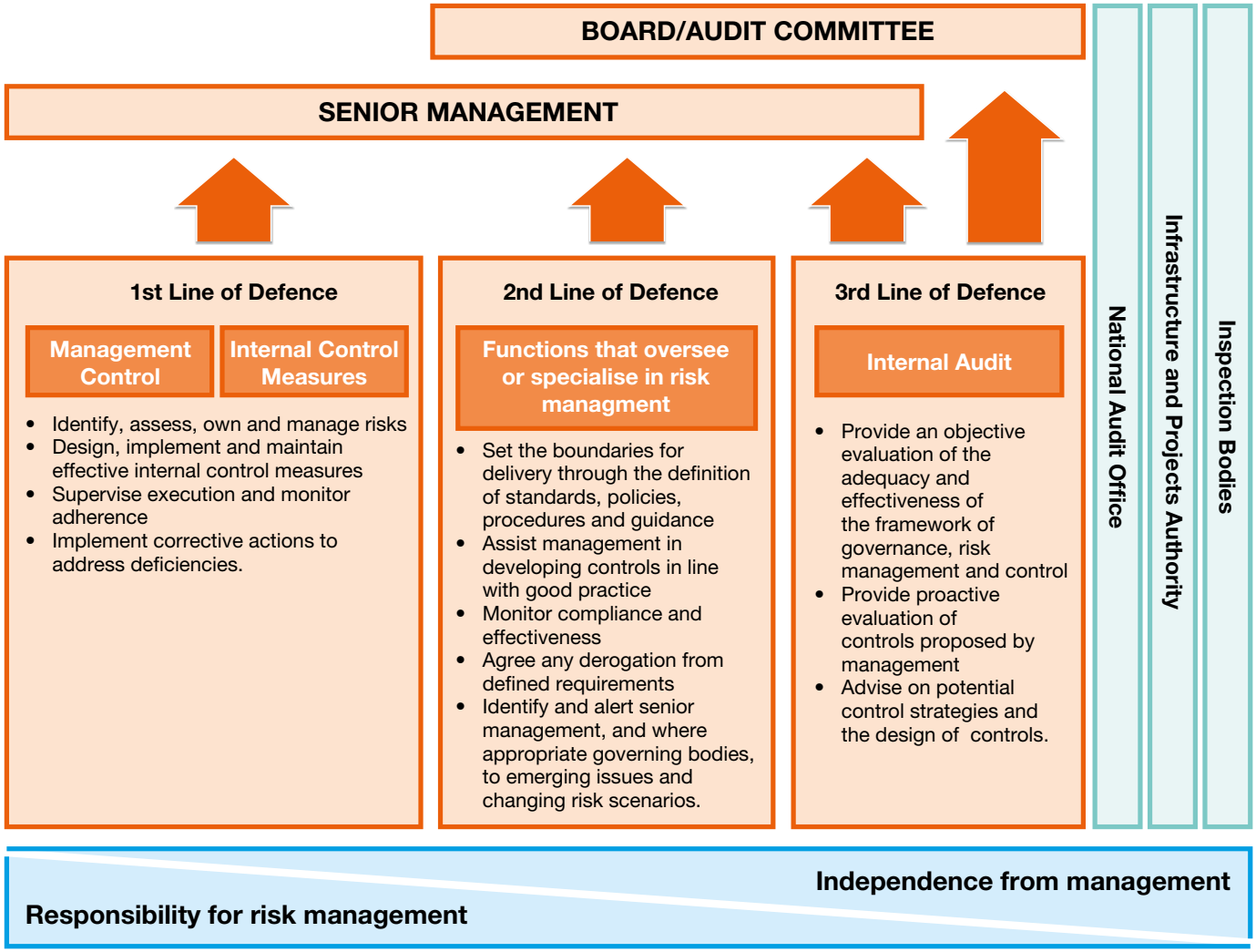
Audit and Risk Assurance Committee[14]

Leading the assessment and management of risk is a role for the board. The Audit and Risk Assurance Committee should support the board in this role. It is essential that the Audit and Risk Assurance Committee:

- understands the organisation's business strategy, operating environment and the associated risks, taking into account all key elements of the organisation as parts of an "extended enterprise";
- understands the role and activities of the board (or equivalent senior governance body) in relation to managing risk;
- discusses with the board its policies, attitude to and appetite for risk to ensure these are appropriately defined and communicated so that management understands these parameters and expectations;
- understands the risk management framework and the assignment of responsibilities;
- critically challenges and reviews the risk management framework, without second guessing management, to evaluate how well the arrangements are actively working in the organisation; and
- critically challenges and reviews the adequacy and effectiveness of control processes in responding to risks within the organisation's governance, operations, compliance and information systems.

Assurance should be obtained on risks across the departmental group. The group should focus on assurances over the management of cross organisational governance, risk and control arrangements to supplement departmental or entity level assurances. Similarly, assurance over the risk and control environment should also encompass services outsourced to external providers, including shared service arrangements, and risks that cross organisational boundaries, for example, in major projects.

Annex 2 – The Three Lines of Defence



Everyone in an organisation has some responsibility for risk management. The "three lines of defence" model provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities within and across the organisation.

The model is not intended as a blueprint or organisational design, but may provide a flexible structure that can be implemented in support of the risk management framework. Functions within each of the "lines of defence" may vary from organisation to organisation and may operate differently.

Neither governance bodies nor senior management are considered to be among the "lines" in this model. They are the primary stakeholders served by the "lines of defence", as they collectively have responsibility and accountability for setting the organisation's objectives, defining strategies to achieve those objectives, and establishing roles, structures and processes to best manage the risks in achieving those objectives successfully.

First line of defence

Under the "first line of defence", management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. Their activities create and/or manage the risks that can facilitate or prevent an organisation's objectives from being achieved.

The first line 'own' the risks, and are responsible for execution of the organisation's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies. Through a cascading responsibility structure, managers design, operate and improve processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risks and supervise effective execution. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, variations in or inadequate processes and unexpected events, supported by routine performance and compliance information.

Second line of defence

The second line of defence consists of functions and activities that monitor and facilitate the implementation of effective risk management practices and facilitate the reporting of adequate risk related information up and down the organisation. The second line should support management by bringing expertise, process excellence, and monitoring alongside the first line to help ensure that risk are effectively managed.

The second line should have a defined and proportionate approach to ensure requirements are applied effectively and appropriately. This would typically include compliance assessments or reviews carried out to determine that standards[6], expectations, policy and/or regulatory considerations are being met in line with expectations across the organisation.

Third line of defence

Internal audit form the organisation's "third line of defence". An independent internal audit function[15] will, through a risk-based approach to its work, provide an objective evaluation of how effectively the organisation assesses and manages its risks, including the design and operation of the "first and second lines of defence". It should encompass all elements of the risk management framework and should include in its potential scope all risk and control activities. Internal audit may also provide assurance over the management of cross-organisational risks and support the sharing of good practice between organisations, subject to considering the privacy and confidentiality of information.

External assurance

Sitting outside of the organisation's own risk management framework and the three lines of defence, are a range of other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls, including:

6 In addition to professional standards, functional standards guide people working in and with the UK government. They exist to create a coherent and mutually understood way of doing business across organisational boundaries, and to provide a stable basis for assurance, risk management, and capability improvement.

- external auditors, chiefly the National Audit Office (NAO)[7], who have a statutory responsibility for certification audit of the financial statements;
- value for money studies undertaken by the NAO, which Parliament use to hold government to account for how it spends public money; and
- the Infrastructure and Projects Authority (IPA), who arrange and manage independent expert assurance reviews of major government projects that provide critical input to HM Treasury business case appraisal and financial approval points.

Other sources of independent external assurance may include independent inspection bodies, external system accreditation reviews/certification (e.g. ISO), and HM Treasury/Cabinet Office/ Parliamentary activities that support scrutiny and approval processes.

Coordination, cooperation and communication

The lines of defence have a common objective: to help the organisation achieve its objectives with effective management of risks. They often deal with the same risk and control issues. The accounting officer and the board should clearly communicate their expectation that information be shared and activities co-ordinated across each of the 'lines' where this does not diminish the effectiveness or objectivity of any of those involved.

Careful coordination is necessary to avoid unnecessary duplication of efforts, while assuring that all significant risks are addressed appropriately. Coordination may take a variety of forms depending on the nature of the organisation and the specific work done by each party. It is likely to be helpful to adopt a common 'language' or set of definitions across the 'lines of defence' to ease understanding, for example, in defining risk categories, risk criteria and what is an acceptance level of control or a significant control weakness.

Internal audit and external audit should work effectively together to the maximum benefit of the organisation and in line with international[16] and public sector standards.[17]

7 Some executive NDPBs may have private sector external auditors (either appointed by the relevant Secretary of State or by the Body's Executive) with a reporting line directly to the Secretary of State or to the body rather than through NAO to Parliament.

Annex 3 – Questions to Ask

These questions may assist in assessing how the risk management principles are applied to support the efficient and effective operation of the risk management framework. They should be read in conjunction with the principles set out in this document. The questions are not intended to be exhaustive and not all will be applicable in all circumstances. If the answers to the questions raise concerns, consideration should be given to whether action is needed to address possible areas for improvement.

Governance and Leadership

1. How is the desired risk culture defined, communicated, and promoted? How is this periodically assessed?

2. How do human resource policies and performance systems encourage and support desired risk behaviours and discourage inappropriate risk behaviours?

3. How has the nature and extent of the principal risks that the organisation is willing to take in achieving its objectives been determined and used to inform decision-making? Is this risk appetite tailored and proportionate to the organisation?

4. How are the board and other governance forums supported to consider the management of risks, and how is this integrated with discussion on other matters?

5. How effective are risk information and insights in supporting decision-making, in terms of the focus and quality of information, its source, its format and its frequency?

6. How are authority, responsibility and accountability for risk management and internal control defined, co-ordinated and documented throughout the organisation?

7. How is the designated individual responsible for leading the overall approach to risk management positioned and supported to allow them to exercise their objectivity and influence effective decision-making?

8. How are the necessary skills, knowledge and experience of the organisation's risk practitioners assessed and supported?

9. How has the necessary commitment to risk management been demonstrated?

Integration

10. How are risks considered when setting and changing strategy and priorities?

11. How are risks transparently assessed within the appraisal of options for policies, programmes and projects or other significant commitments?

12. How are emerging risks identified and considered?

13. How are risks to the public assessed and reflected within policy development and implementation?

14. How are National Risk Register risks, that are particularly pertinent to the organisation, recognised in risk assessments and discussions?

Collaboration and Best Information

15. How is an aggregated view of the risk profile informed across the organisation, arm's length bodies and the extended enterprise supporting the delivery of services?

16. How are the views of external stakeholders gathered and included within risk considerations?

17. How does communication and consultation assist stakeholders to understand the risks faced and the organisation's response?

18. How is function and professional expertise used to inform strategies, plans, programmes, projects and policies?

19. How do expert functions and professions inform the identification, assessment and management of risks and the design and implementation of controls?

20. How are functional standards communicated and their adherence monitored across the organisation?

Risk Management Processes

21. How are risk taxonomies or categories used to facilitate the identification of risks within the overall risk profile?

22. How are risk criteria set to support consistent interpretation and application in assessing the level of risk? How effective are these in supporting the understanding and consideration of the likelihood and consequences of risks?

23. How are limitations and influences associated with the information and evidence used with risk assessments highlighted?

24. How are interdependencies between risks or possible combinations of events ('domino' risks) identified and assessed?

25. How dynamic is the assessment of risks and the consideration of mitigating actions to reflect new or changing risks or operational eficiencies?

26. How are exposures to each principal risk assessed against the nature and extent of risks that the organisation is willing to take in achieving its objectives – its risk appetite – to inform options for the selection and development of internal controls?

27. How are decisions made in balancing the potential benefits of the design and implementation of new or additional controls with the costs, efforts and any disadvantages of different control options?

28. How are contingency arrangements for high impact risks designed and tested to support continuity, incident and crisis management and resilience?

29. How is the nature, source, format and frequency of the information required to support monitoring of risk management and internal control defined and communicated?

30. How are new and changing principal risks highlighted and escalated clearly, easily and more rapidly when required?

31. How comprehensive, informative and coordinated are assurance activities in helping achieve objectives and in supporting the effective management of risks?

32. How do disclosures on risk management and internal control contribute to the annual report being fair, balanced and understandable?

Continual Improvement

33. How are policies, programmes and projects evaluated to inform learning from experience? How are lessons systematically learned from past events?

34. How is risk management maturity periodically assessed to identify areas for improvement? Is the view consistent across differing parts or levels of the organisation?

35. How are improvement opportunities identified, prioritised, implemented and monitored?

Annex 4 – Example Risk Categories

Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

Operations risks – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

Legal risks – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

Property risks – Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

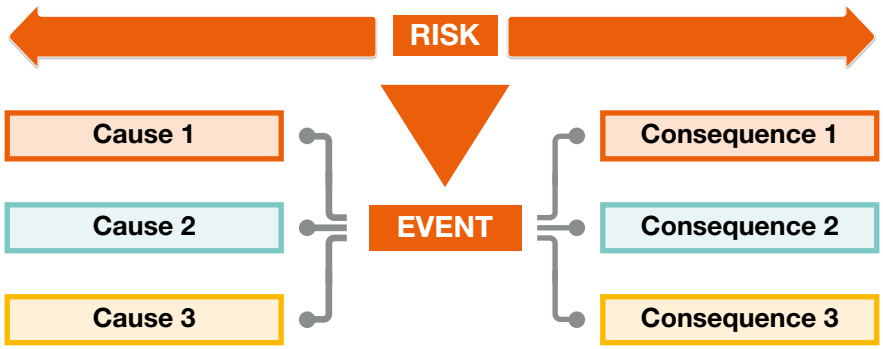
Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

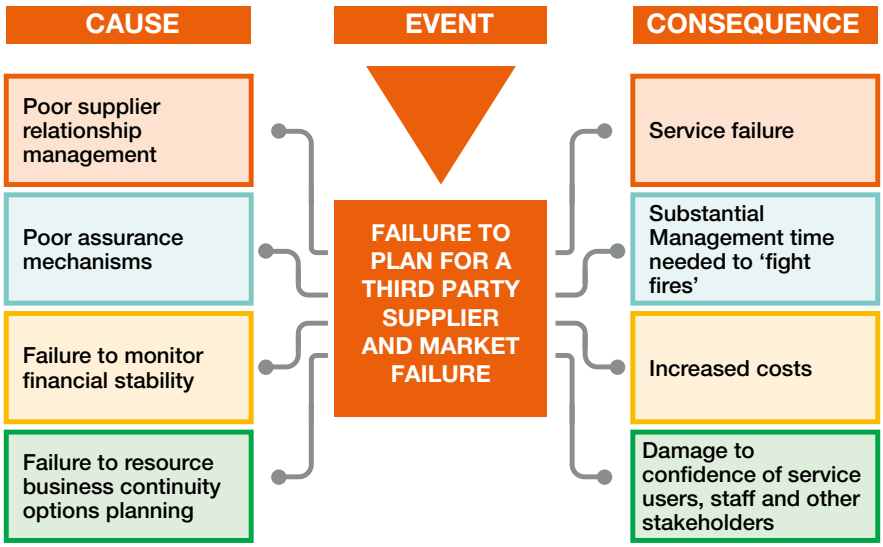
Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

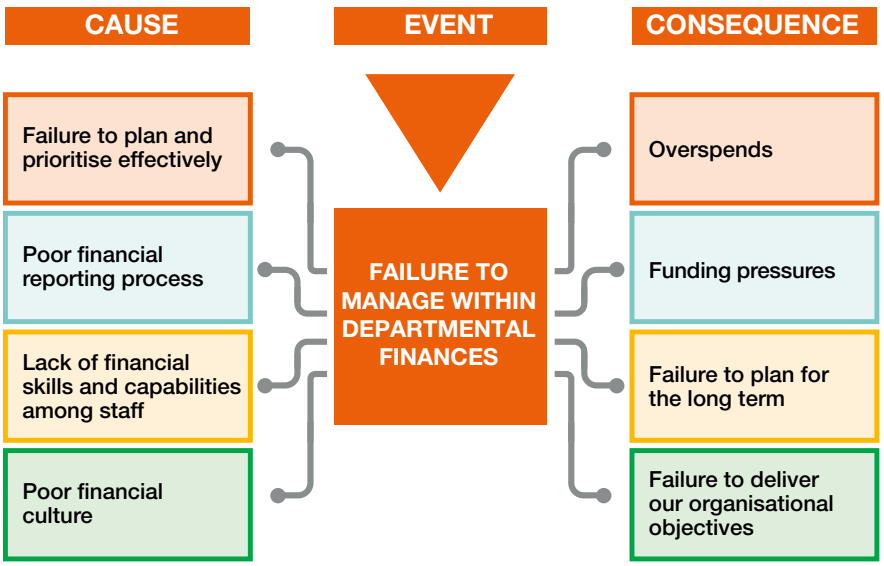
Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Annex 5 – Definitions and Supportive Concepts

Stating risks: causes, events and consequences







In stating risks, care should be taken to avoid stating consequences that may arise as being the risks themselves, i.e. identifying the symptoms without their cause(s). Equally, care should be taken to avoid defining risks with statements that are simply the converse of the objectives, i.e. failure to achieve the intended output/outcome.

Organisations typically assess consequences using a combination of criteria, which commonly include financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational effects. The criteria used should be dynamic and should be periodically reviewed and amended, as necessary. Scales should allow meaningful differentiation for ranking and prioritisation purposes based on assigning values to each risk using the defined criteria.

When assigning a consequence rating to a risk, the rating for the highest, most credible worst-case scenario should be assigned.

The risk analysis process defines the level of risk, based on the assessment of the ***likelihood*** of the risk occurring and the consequences should the event happen. Likelihood is the assessment of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Risk analysis should also consider:

- sensitivity and confidence levels, based on the information available;
- complexity and connectivity;
- time-related factors and volatility; and
- the effectiveness of existing internal control.

Internal Control is the dynamic and iterative framework of processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risk. Internal controls permeate and are inherent in the way the organisation operates and are affected by cultural and behavioural factors.

Where additional action is required to bring the levels of risk within the nature and extent that the organisation is willing to take to achieve its objectives, the organisation should select, develop and implement options for addressing risk through preventive, directive, detective, and/or corrective controls that manage risks to an acceptable level. These might be manual or automated. This involves an iterative process of:

- planning and implementing internal control;
- assessing the effectiveness of internal control;
- deciding whether the nature and extent of the remaining risk after the implementation of internal controls is acceptable; and
- if not acceptable, reassessing options and taking further action where appropriate.

Internal control, even if carefully designed and implemented, might not produce the intended or expected outcomes. Internal control can also introduce new risks that need to be managed.

Assurance is a general term for the confidence that can be derived from objective information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements, and the production of insightful and credible information to support decision-making. Confidence diminishes when there are uncertainties around the integrity of information or of underlying processes.

Annex 6 – References

ID	Description
1	BS ISO 31000:2018(E) - Risk management – Guidelines
2	Corporate governance code for central government departments https://www.gov.uk/government/publications/corporate-governance-code-for-central-government-departments
3	Managing Public Money – Section 4 Governance and Management https://www.gov.uk/government/publications/managing-public-money
4	Managing Public Money – Annex 4.3 Risk
5	Budget 2018: 2.18 The Balance Sheet Review – https://www.gov.uk/government/publications/budget-2018-documents/budget-2018 and Getting smart about intellectual property and intangible assets https://www.gov.uk/government/publications/getting-smart-about-intellectual-property-and-intangible-assets
6	Central Government Guidance on Appraisal and Evaluation - The Green Book https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf
7	The Future Toolkit provides guidance on horizon scanning and outlines how scenarios can be used to further investigate emerging risks https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf
8	The National Risk Assessment (NRA) - a strategic medium-term planning tool that captures examples of civil emergencies that could plausibly affect the UK within its territorial boundaries and should be used to inform integrated emergency management decisions
9	The Principles of Managing Risks to the Public https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191518/Managing_risks_to_the_public_appraisal_guidance.pdf
10	ISO 31010:2009 is a supporting standard for BS ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment
11	Guidance on producing quality analysis for government – The Aqua Book https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/416478/aqua_book_final_web.pdf
12	The Outsourcing Playbook - Central Government Guidance on Outsourcing Decisions and Contracting https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/780361/20190220_OutsourcingPlaybook_6.5212.pdf
13	Guidance for evaluation – The Magenta Book https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/220542/magenta_book_combined.pdf
14	HM Treasury Audit and Risk Assurance Committee Handbook, March 2016 https://www.gov.uk/government/publications/audit-committee-handbook
15	Public Sector Internal Audit Standards https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641252/PSAIS_1_April_2017.pdf
16	International Standards on Auditing - ISA 315 and 610