UK Resilience Academy

ORGANISATIONAL RESILIENCE GUIDANCE FOR UK GOVERNMENT DEPARTMENTS, AGENCIES AND ARM'S LENGTH BODIES (ALBs)

Version 1, August 2024

Contents

INTRODUCTION

1. **The resilience of an organisation is its ability to achieve intended outcomes through uncertainty, disruption and change.** Highly resilient organisations emphasise foresight, preparation and planning for adversity, can manage through disruption with minimised service impacts and expedited recovery, learn effectively from their own and others' experience, and can more smoothly adapt to challenges and change in the longer term.

2. This guidance is intended to support UK Government departments, agencies and Arms-Length Bodies (ALBs) in developing their resilience functions to meet the challenges and commitments set out in the 2022 UK Government Resilience Framework. It is not mandatory, but it sets out a common approach for UK government departments to increase their organisational resilience, working both individually and collectively.

3. The guidance has been developed by the Cross Government Business Continuity Forum, led by the Department for Work and Pensions. It draws on established guidance, recognised good practice from both the public and private sector and relevant British (BSI) and International (ISO) standards, notably the 2022 BSI Code of Practice on Organisational Resilience[1]. The guidance complements and should be considered alongside the 2023 version of The Orange Book: management of risk – principles and concepts.

4. Throughout the guidance the term 'departments' is used for brevity, but this should be read to include all UK government departments, agencies and ALBs. It adopts the consistent language used in Government Functional Standards, and specifically Government Functional Standard GovS 007: Security.

CONTEXT

Concept

5. The concept of resilience has evolved over time, both in general and in relation to organisations. In general terms it has shifted from a narrower and shorter-term preparedness, response and recovery frame of reference to a more strategic and forward-looking approach in which risk reduction and adaptation to future conditions are key elements.

6. This applies equally to organisational resilience, and a further important development has been the progressively tighter integration of all relevant functions, including but not limited to risk management, IT service and business continuity, supply chains, security and safety management. Resilience is now widely recognised as a strategic capability for departments that enables them to reliably achieve their objectives, and not just a technical, defensive activity that can be delegated to the operational level.

[1] BS 65000:2022. Organizational resilience. Code of practice, British Standards Institution.

Definitions

7. The general ISO definition of resilience is: 'the ability to absorb and adapt in a changing environment'[2]. While this is broad, it is helpful because it spans the ability to deal with both short-term, acute disruption and also adapt to longer-term, chronic challenges and change.

8. Organisational resilience is defined here in explicitly outcome-oriented terms: 'the ability of an organisation to achieve intended outcomes through uncertainty, disruption and change'. The overall resilience of an organisation has both operational and strategic dimensions:

    a. **Operational resilience** engages with the organisation as it is currently established, building progressively greater levels of foresight, preparedness, continuity, response, recovery and improvement capabilities into that organisation so that it can sustain its essential outcomes through all forms and scales of disruption.

    b. **Strategic resilience** focuses on building greater levels of resilience into the future of the organisation by means of risk reduction, further enhanced operational resilience and fostering adaptive capacity.

9. Definitions from relevant documents appear in Annex one.

Related functions

10. As introduced above, the progressively tighter integration of relevant functions has been a hallmark of resilience-progressive organisations in recent years. The relationship between risk, security, safety, business continuity, organisational and national resilience can be summarised as follows:

    a. **Risk**: risk management is concerned with the identification and assessment of hazards and threats and their treatment in a way that is consistent with an organisation's risk appetite, tolerance and intended outcomes. The risk management framework in a highly resilient organisation will be integrated with arrangements for incident and crisis response, recovery and renewal should risks materialise. Government's principal tool for identifying and assessing risks to the UK in the medium term is the National Security Risk Assessment (NSRA). This is owned by the Resilience Directorate in the Cabinet Office and should be used as a tool to support risk identification and assessment.

    b. **Security**: security is the application and management of measures to limit the likelihood and impact of threats, that is the causing of deliberate harm. It includes the protection of assets (people, property and information), threat and impact containment, consequence management and investigation and system improvement. Highly resilient organisations will have the capability to reduce risk, intercept, contain and mitigate disruption from all sources, manage adverse events and their consequences and recover and renew to better face future changes and challenges.

    c. **Safety**: safety management in organisations is the application and management of measures that protect people from harm arising from all risks and, at the same time,

[2] ISO 22300:2021. Security and resilience - Vocabulary. International Standards Organization.

protect the future success of those organisations[3]. While safety management is a specific and separate discipline, its coherence with risk, security and continuity is a critical element of an organisation's resilience.

d. **Business continuity** is the capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following a disruptive incident. Resilience is the strategic ability to survive and thrive, which requires the integration of a range of functions and capabilities including risk management, business continuity, security, incident and crisis and recovery management.

e. **National resilience:** national resilience is the collective resilience of institutions, infrastructure, communities and the varied networks that bind us together. The ability of organisations, public, private and third sector, to maintain the delivery of their functions and services through uncertainty and disruption, and to adapt to challenge and change in the longer term, is a critical element of national resilience.

Existing Standards

11. This guidance reflects the expectations and good practice set out in the British and International Standards which are summarised in Annex two. These standards have a number of common threads: the need for deep understanding of context and risks; the importance of preparation as a basis for response to disruption; a step-by-step approach that emphasises continuous improvement; the importance of robust assurance; and the idea that disruption can present opportunities for renewal, not just recovery.

12. While individual standards should be considered and implemented as appropriate by departments, the effective integration of those functions is of equal importance as their implementation in isolation. To illustrate, effective security management will not in itself deliver a highly resilient organisation, but an organisation cannot be highly resilient without effective security management. The whole is greater than the sum of its parts.

Key considerations and benefits

13. Departments should work through how their approach to organisational resilience is informed by each of the following:

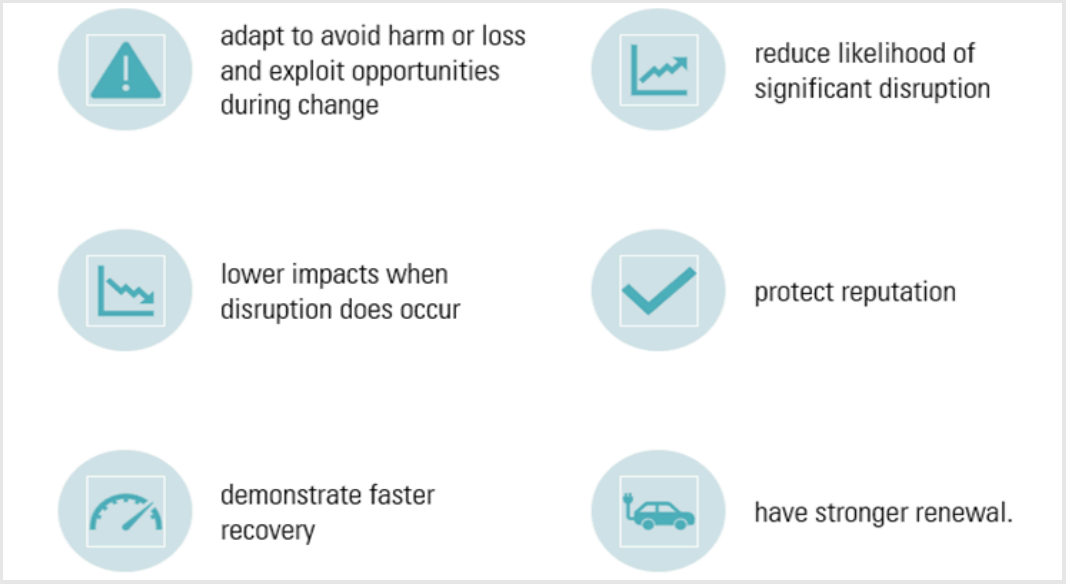
    a) **Against what?** Assets, services and outcomes should be resilient against defined risks, whether specific or wider 'bundles' of risks. While much can be done to develop capabilities that will enable response, recovery and renewal in the face of unforeseen events and circumstances, departments cannot be equally resilient against all possible eventualities, and this necessitates choices about priorities.

    b) **Why?** Resilience protects and enables what organisations and their partners, customers and stakeholders value – their essential outcomes. A lack of resilience will place statutory obligations, tangible (e.g. physical, financial and digital assets) and non-tangible (e.g. welfare and reputation) resources at increased risk of erosion, interruption, damage or loss. Departmental leaders should determine the value of that and invest commensurately.

[3] HSE (2023) Risk assessment: Steps needed to manage risk - HSE Health and Safety Executive.

c) **How and how much?** There is no single path to high levels of resilience and what is proportionate and effective for one department may be a weak fit for another. Departments should however adapt and adopt authoritative frameworks, guidance, standards and established good practice to fit their specific context.

14. While highly resilient departments will secure better outcomes during disruption, there is substantial evidence that they can also realise various benefits during periods of stability. The BSI Code of Practice on Organisational Resilience describes how they are able to:



15. The following sections set out a framework comprised of guiding principles, practices and cultural attributes that will enable these benefits to be realised and which departments should consider when designing their approach to resilience.

FRAMEWORK

Guiding principles

16. Guiding principles, in this context, are overarching considerations which should inform departments' decisions about: leadership, management and culture; prioritisation and resourcing; structure and design; and the conduct and governance of resilience activities. The principles for organisational resilience are summarised below.

17. **Purpose** – resilience arrangements should reflect departmental objectives and senior leaders should provide suitably specific direction for resilience arrangements to be in proportion to their tolerance for impacts on essential outcomes.

18. **Risk-based** – while departments should have a general ability to respond and recover from unexpected events and the common consequences of 'bundles' of risks, they should also prepare for specific risks with horizon scanning, contingency planning and the validation of their risk-specific arrangements.

19. **Design** – resilience arrangements should reflect the established design principles of redundancy, diversity, modularity and adaptability[4].

[4] BS 65000:2022 - Organizational resilience. Code of practice, British Standards Institution.

20. **Embedded** – resilience should not be considered as a 'bolt on' function, rather it should be understood and normalised within the practices and culture of the organisation.

21. **Coherent** – silos, gaps and weak information flows undermine resilience and leaders should ensure joined-up working across functional, organisational and geographical boundaries.

22. **Reciprocal** – resilience is systemic and an individual organisation's continuity and resilience arrangements should make a conscious and meaningful contribution to the resilience of its wider network.

23. **Progressive** – departments should routinely scan for and reflect changes in the risk environment, lessons identified and good and leading practice.

24. The table below cross-references these to the Orange Book risk management principles. A highly resilient department will be able to demonstrate leading practice in risk management, but a high level of resilience will ultimately be achieved by the coherence and combined effect of all relevant functions.

Organisational resilience principles	**Orange Book risk management principles**
Purpose	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. Risk management processes shall be structured to include risk identification and assessment to determine and prioritise how the risks should be managed.
Risk-based	Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives. Risk management processes shall be structured to include the design and operation of integrated, insightful and informative risk monitoring and timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.
Design Embedded Coherent Reciprocal	Risk management processes shall be structured to include the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level.
	Risk management shall be collaborative and informed by the best available information and expertise.
Progressive	Risk management shall be continually improved through learning and experience.

Practices

25. Practices, in this context, are the things that organisations should do, have and be able to demonstrate, and the key practices for organisation resilience are summarised below.

26. **Oversight and accountability** – departmental governance arrangements should demonstrate clear accountability for risk management and resilience capabilities.
27. **Assess risk** – departments should have a heightened awareness of risk, change and emergent disruption, achieved through arrangements and suitable expertise for both short and longer-range horizon scanning. Risk assessment should inform the development of proportionate resilience capabilities.
28. **Assess impact** – the relative contribution and criticality of assets, capabilities and systems in enabling the achievement of essential outcomes should be understood and tested through business impact analyses.
29. **Reduce** – departments should consider relevant ways and means to reduce the likelihood of risks materialising, balancing risk-reducing and impact-mitigating measures in line with risk exposure and appetite.
30. **Protect** – suitable, sufficient and proportionate risk controls should be agreed and implemented to protect essential outcomes. Departments should regularly assess the effectiveness of controls and their proportionality to the department's risk appetite[5].
31. **Prepare** – preparation for disruption that either evades or overwhelms risk controls should span the following elements of capability:
    a. Doctrine, powers, plans and procedures.
    b. Equipment, infrastructure, supplies and logistics.
    c. Information and communications.
    d. Suitably Qualified, Experienced and Empowered Personnel (SQEEP).
32. **Assure** – departments should establish an ongoing programme to validate their resilience arrangements and capabilities and their specific preparedness for key risks. This should go beyond compliance checks into rigorous testing against reasonable worst-case scenarios. Capabilities and arrangements should be tested against the three lines of assurance[6].
33. **Respond** – response to disruption is built on *capability* (the components of the ability to respond), *capacity* (the amount of capability) and *readiness* (the time and effort needed to achieve effect). Departments should have documented and validated response structures that enable an informed, authoritative, coherent, timely and if necessary sustained response to both specific risks and unforeseen forms of disruption, including concurrent events.
34. **Recover** – departments should have the capability to recover quickly and effectively following disruption or change. Both response and recovery arrangements should be scalable to allow a graduated response from limited and contained incidents through to the most severe levels of disruption.
35. **Renew** – highly resilient organisations are progressive; they learn from success as well as failure. Leaders should approach post-incident recovery with a bounce-forward mindset, rather than assuming that everything will go back to 'business as usual' following periods of disruption and change.

---

[5] Government Finance Function (2021). Risk Appetite Guidance Note Version 2.0
[6] HM Government (2020). The Orange Book: Management of Risk – Principles and Concepts

Cultural Attributes

36. Culture, the shared beliefs, attitudes, and habits of people within a group, can have a profound effect on the resilience of departments. Culture is less tangible and less easy to shape than structures and processes, but the right culture will foster instincts and behaviours that build resilience.

37. The following are indicators of a strong culture of resilience within an organisation:

    a. **Leadership**: the habits and behaviours which promote resilience will become normalised if leaders at all levels visibly demonstrate their commitment, and when they are demonstrably accountable for the resilience of their organisation.

    b. **Common purpose**: leaders at all levels communicate and reinforce the importance of collaboration and a 'beyond silos' mindset in working towards the achievement of the organisation's essential outcomes.

    c. **Communication**: ways of working and expectations support the sharing of information that informs and enables all facets of operational and strategic resilience, both within the organisation and between partners.

    d. **Systems mindset**: the causes of disruption are rarely simple and its consequences are typically complex, so a systemic approach to understanding and managing interdependencies is required[7].

    e. **Engaging with failure**: Engaging with failure: highly resilient departments accept that their capabilities and arrangements are likely to fail to a certain degree at some point. They commit to look for problems, test assumptions, share bad news and challenge ways of working.

    f. **Psychological safety** is a belief that people will not be punished or humiliated for speaking up with ideas, questions, concerns, or about mistakes and it is an essential condition for freely sharing risk information and strong teamwork

    g. **Diversity** is a key enabler of resilience, and departments should recognise the critical contribution of different backgrounds and ways of thinking, seeing and working towards agreed outcomes.

    h. **Empowerment**: highly resilient departments routinely delegate authority to competent people who are close to issues in the interests of timely decisions, guided by a common understanding of strategic priorities.

    i. **Adaptability** is a defining characteristic of highly resilient organisations and individuals which underpins their ability to work flexibly towards essential outcomes as required by circumstances.

    j. **Welfare**: highly resilient departments take care of their people and consider how their choices and actions affect people's physical, mental and emotional wellbeing.

[7] Government Office for Science (2022). Systems thinking for civil servants - guidance.

ENDNOTE

38. This guidance is offered as a set of handrails for departments to use in defining and refining their own approach to organisational resilience. Resilience is neither static nor absolute, and what works well in one context may have less relevance or impact elsewhere. While that caveat is important, the considerations set out above summarise existing good practice and the experience of central government departments, agencies and ALBs in adapting and adopting this, and building specific policies and standards, will be shared across the cross-government business continuity forum and reflected in future versions of this guidance.

ANNEX 1: RELEVANT DEFINITIONS

Business continuity: the capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following disruptive incident (source: ISO22301[8]).

Essential outcomes: services, products or functions that the organisation provides for its customers, end users or other stakeholders, which if unavailable would likely cause significant harm or detriment that cannot be easily remedied, or result in a wider failure within the market, system, sector or organisation (source: BS650000:2022).

National resilience: the UK's ability to anticipate, assess, prevent, mitigate, respond to, and recover from natural hazards, deliberate attacks, geopolitical instability, disease outbreaks, and other disruptive events, civil emergencies or threats to our way of life (source: UK Government Resilience Framework[9]).

Operational resilience: the ability of organisations, infrastructures and sectors to protect and sustain the core products and services that deliver outcomes and prevent, adapt and respond to, recover and learn from operational disruption (source: adapted from Prudential Regulation Authority, Financial Conduct Authority and Bank of England[10]).

Organisational resilience: a strategic capability that enables an organisation to prepare for and respond to disruption, adapt in a timely and appropriate manner and thrive in a changing environment (source: BS650000:2022).

Resilience: the ability to absorb and adapt in a changing environment (source: ISO22316:2017[11])

Risk: the effect of uncertainty on objectives (source: ISO31000[12]).

Security management: effective control of malicious and unlawful threats to the services, processes, systems and assets required to deliver business objectives.

---

[8] ISO 22301:2019 Business continuity management systems — Requirements. International Standards Organization

[9] The UK Government Resilience Framework

[10] Bank of England PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services

[11] ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes. International Standards Organization

[12] ISO 31000: 2018 Risk management – Guidelines. International Standards Organization

ANNEX 2: SUMMARY OF RELEVANT STANDARDS

There is a range of existing authoritative standards and guidance of relevance to business continuity and resilience. This policy and the accompanying standard reflect the expectations and good practice set out in those – principally British and International Standards – that should be considered by government departments and agencies. In summary, those relevant standards are:

a. Used together, **ISO 22301:2019 Business continuity management systems - Requirements** and **ISO 22313:2020 Business continuity management systems - Guidance on the use of ISO 22301** specify the structure and requirements for implementing and maintaining a business continuity management system (BCMS).

b. **BS65000:2022 Organisational Resilience – Code of Practice** sets out guidance on achieving enhanced organisational resilience, in particular it describes organisational resilience, articulates its benefits, and explains how to build resilience.

c. **ISO 31000, Risk management – Guidelines** provides principles, a framework and a process for managing risk.

d. **ISO 22361:2022 Crisis management - Guidelines** was developed to aid in the design and ongoing development of an organisation's crisis management capability. It sets out principles and practices that are applicable to all organisations.

e. **BS16000: 2015 Security management – strategic and operational guidelines** provides guidelines for implementing a security management system to enhance the resilience of an organisation.

f. **ISO 37000: 2021 Governance of organisations – guidance** sets out guidance on the effective governance of organisations, including the effective management of risk.

g. **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – information security management systems** sets out a holistic approach to information security, a critical element of an organisation's risk and resilience capability.

h. **ISO/TS 22318:2021 Business continuity management systems - guidelines for supply chain continuity management** gives guidance on extending the principles of business continuity in ISO 22301 and ISO 22313 to the management of supply chain continuity.

i. **Government Functional Standard 007**[13] The UK Government Security Policy Framework Standard that provides guidelines for emergency planning the security of government information and assets.

j. **National Resilience Standards for LRFs: Business Continuity Management**[14] The UK's National Resilience Standards for Local Resilience Forums (LRFs) provide guidelines for coordinating emergency planning and response activities among local authorities, emergency services and other organisations.

---

13 Government Security Profession: Functional Standard for Security, GovS 007

14 Cabinet Office (2020). National Resilience Standards for LRFs - BCM (Standard #9)