A guide to BS 65000

Organizational resilience – Code of practice

A BSI executive briefing

Author

Rick Cudworth, Director ResilienC.

By Royal Charter

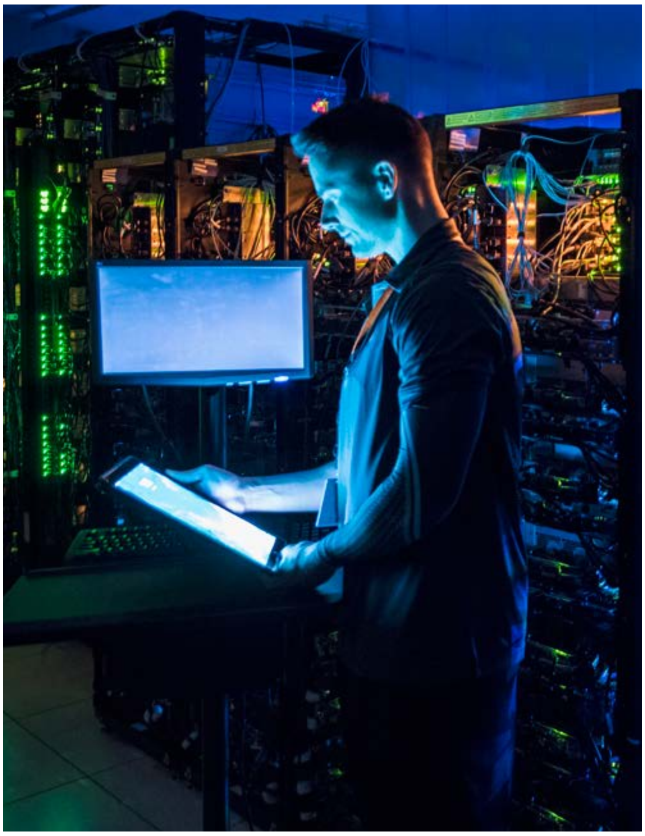
Contents

Overview	**3**
How to implement the standard	6
Challenges and pitfalls in using the standard	9
Wider context	10
Conclusion	12
About the author	**13**
Why BSI	**14**

Overview

Resilience has become a strategic issue for many organizations. It involves developing the ability to anticipate challenges, adapt to them and to anticipate challenges, adapt to them and to absorb shocks. In a time of continuing uncertainty and change, this has rarely been more important.

The new BS 65000 Code of Practice for organizational resilience provides a timely and significant revision of the previous BS 65000 Guidance Standard published in 2014. It recognizes that there has been increased convergence on many of the principles and practices that help build and maintain organizational resilience. It builds on the growing body of evidence from industry and academic research since the earlier Standard was first published.



As a result, the Code of Practice provides clear recommendations of what organizations should do to become more resilient.

Importantly, the Code of Practice extends the scope of organizational resilience to include financial, operational, human, social and environmental considerations and recognizes the importance of resilience across the wider system within which the organization operates.

The Code of Practice also addresses the defensive and progressive dimensions of organizational resilience, supporting continuity and adaptability. It suggests that the organization's strategy, business model and risk management are fundamental to building and maintaining organizational resilience. It places particular emphasis on considering what is truly essential[1], what impacts are tolerable from an 'outside-in' perspective and stress testing for all aspects of organizational resilience.

Together, these updates create a new framework that will help enable organizations improve their approach to organizational resilience.

[1] The Code of Practice defines 'essential outcomes' as being: 'services, products or functions that the organization provides for its customers, end-users or other stakeholders, which if unavailable would likely cause significant harm or detriment which cannot be easily remedied or result in a wider failure within the market, system, or sector or the organization itself.'

Who is the standard written for?

The Code of Practice is intended for all types of organizations, including public and private sector bodies, non-governmental organizations, charities and other not-for-profit organizations and for all sizes, large and small. The core principles and the recommended practices to build and maintain organizational resilience set out in the Code of Practice can be applied to all organizations, though the effort required may vary depending on the specific context of the organization.

The Code of Practice is designed to aid those with accountability and responsibility for resilience within their organizations. This includes non-executive directors, accountable executives, those responsible for the organization’s strategy and operations as well as those who have a specific remit for resilience or risk management within the organization.

It will also be of interest to those responsible for environmental and sustainability issues, policy makers and regulators. The Code of Practice has specifically drawn on the Supervisory Statements[2] on operational resilience released by the UK’s financial regulatory bodies, the National Infrastructure Commission’s report on resilient infrastructure systems[3] and research conducted by Cranfield University on behalf of the National Preparedness Commission[4].

[2] Supervisory Statement (SS) 1/21: Operational resilience; Impact tolerances for important business services. March 2021. Prudential Regulatory Authority.
Policy Statement (PS) 21/3: Building operational resilience: Feedback to CP19/32 and final rules, March 2021. Financial Conduct Authority.

[3] Anticipate, react, recover. Resilient infrastructure systems. May 2020. National Infrastructure Commission.

[4] Denyer, D and Sutliff, M. Resilience reimagined: A practical guide for organisations. March 2021. National Preparedness Commission, Cranfield University and Deloitte.

The benefits of using the standard

The writers of the Code of Practice have set out to provide practical recommendations that, if adopted, can help organizations to become more resilient and moreover support the resilience of the wider system within which they operate.

As the recommendations in the Code of Practice are based on the convergence of several recent reports and policy statements related to resilience, and on the evidence of practices being used by organizations.

The Code of Practice can help you to:

- **adopt** current leading practices in building and maintaining organizational resilience based on real-world evidence
- **consider** all aspects of organizational resilience, including the financial, operational, human, social and environmental dimensions
- **focus** effort and investment in resilience on what really matters not just to the organization but to its customers, communities and wider society
- **support** the development of adaptive capacity within the organization
- **change** the mindset and culture relating to resilience and embed it within strategy, business model design and risk management

Ultimately, the sustained performance and success of an organization will often depend on its resilience, its ability to continue through adversity and adapt to uncertainty and change. Whilst the subject of organizational resilience will inevitably continue to mature and evolve, this Code of Practice provides tangible principles and practices that any organization can adopt to help make it more resilient.

How to implement the standard

The Code of Practice sets out eight ‘Guiding principles’ for organizational resilience.

The principles are split between cultural – those related to risk behaviours, governance, learning and decision-making within the organization; and design – those related to the physical, financial, human and technological construct of the organization’s business model and processes. The Code of Practice does not set out a preference for any principle over another but recommends adoption of each of the principles.

The principles are broadly set, and those relating to the ‘Culture of resilience’ – foresight, insight, hindsight and oversight – are likely to support improved adaptive capacity.

The principles relating to ‘Design for resilience’ – redundancy, diversity, modularity and adaptability – are likely to be applied to varying degrees to specific aspects of resilience. For example, a more resilient business model may reduce concentration risks or major points of failure by applying the principles of modularity or diversity. A more resilient process may depend on a combination of redundancy (e.g. of stock holding), diversity (e.g. of delivery channel) and adaptability (e.g. flexibility of supply chain). Increased financial resilience may be dependent on redundancy (e.g. cash held in the bank) and adaptability (e.g. the ability to liquidate assets quickly if needed).

In addition to the ‘Guiding principles’, the Code of Practice sets out the ‘Practices of organizational resilience’. These are under the headings of:

- ‘Establishing the context for organizational resilience’
- ‘Developing organizational resilience’
- ‘Stress testing organizational resilience’
- ‘Embedding resilience’
- ‘Organizational learning’
- ‘Organizational structure change’
- ‘Governance for resilience’
- ‘Resilience reporting’

Each heading contains several specific recommended practices. It is possible that organizations may take a graduated approach to adopting these. This recognizes that building and maintaining organizational resilience is an on-going activity and may need to be achieved in stages.

Equally, an organization may want to focus on specific dimensions of its resilience, e.g. strengthening its financial, human or environmental resilience as a first step, or improving its operational resilience for a particular product or service, applying the principles and practices to each dimension in turn.

However, the most efficient approach will be one that starts with the organization's strategic goals and context, assesses the resilience of its overall business model across each of the five dimensions and focuses on areas where improvements in resilience will have the most benefit in the short, medium and the long-term performance and success of the organization. A strategic, 'top-down' approach to organizational resilience is therefore recommended.

In reviewing the practices, there are some that are worth more detailed consideration here as they are similar to the practices being implemented within financial institutions, large and small, to improve their financial and operational resilience. There is therefore real-world application of these and lessons we can learn from them.

These practices are:

- the identification of 'essential outcomes, which are the services, products or functions that an organization provides for its customers, end-users and other stakeholders'
- the setting of 'impact thresholds' which 'should be measurable and anchored within a specific timeframe'
- the identification of 'the components of the system and sector(s) in which the organization operates, their interconnections and their vulnerability to failures'
- undertaking 'stress testing to evaluate whether impact thresholds can be met under various severe but plausible scenarios'
- increasing the resilience of essential outcomes through the application of resilience design principles – redundancy, diversity, modularity and adaptability

Following the financial crisis, the financial sector has demonstrated improved financial resilience through the COVID-19 pandemic. In achieving this, it implicitly and sometimes explicitly applied these practices. Essential outcomes were identified as 'economic functions' (e.g. 'payments, settlement and clearing'), impact thresholds were set for liquidity ratios and capital adequacy and regular stress testing was introduced to ensure that these are not breached under severe but plausible scenarios. Vulnerabilities wereidentified and adaptations made.

A similar approach is now being applied to improve operational resilience across the sector. In this case, the focus has been on identifying those services or products which, if not available, could cause widespread or irreparable harm to customers, communities or other third parties. Understanding the nature of impact (e.g. distinguishing between inconvenience and annoyance, harm that can be easily remedied and irreparable harm), who would be impacted (vulnerable members of society, widespread across the customer base, suppliers or other third parties, or the wider sector in which they participate) and when such impact would materialize has been particularly informative.

This work has enabled a much deeper understanding of the nature of impacts, to who and when, and a clearer distinction between 'inconvenience' (if possible, we'd like to avoid this) and 'irreparable harm' (we must avoid this). Vulnerabilities, such as major points of failure in the way such services or products are provided are being identified and actions taken to reduce or remove such vulnerabilities, e.g. through increased redundancy, diversity, modularity or adaptability, including opportunities for substitution (e.g. through an alternative channel or by another provider).

This, combined with the on-going stress testing of their operational resilience and impact thresholds against severe, but plausible scenarios are providing the basis for a better understanding of the gaps in their resilience and more focused investment decisions to improve resilience. It is also enabling better informed decisions and priorities when responding to incidents or crisis events.

Pre-requisites to the success of this work have been a change in mindset, the accountability of a senior executive and improved governance arrangements over resilience. It is also anticipated that this will lead to technology renewal and more flexible outsource arrangements over time, which will help financial institutions to renew their business models to be more resilient and able to adapt to change more quickly.

These practices are not unique to the financial sector, and similar practices have been cited by the National Infrastructure Commission, National Preparedness Commission and by the OECD.[5]

[5] OECD (2014). Guidelines for Resilience Systems Analysis; How to analyse risk and build a roadmap to resilience. OECD Publishing.

Challenges and pitfalls in using the standard

The Code of Practice does not attempt to be a panacea for organizational resilience, and as noted previously the subject will undoubtedly continue to mature and evolve. There are also likely to be challenges and some pitfalls in implementing the recommendations in this Code of Practice. These include:

- mistaking operational resilience for organizational resilience. The Code of Practice recommends that organizational resilience is considered across five dimensions: financial, built, human, environmental and social. Each of these dimensions needs to be considered and addressed, as they are mutually supportive of each other. If a significant event occurs, the initial impacts are likely to cascade across multiple dimensions, and a successful outcome will be dependent on the resilience across all of these dimensions. These five dimensions clearly extend beyond the normally accepted scope of operational resilience, which typically focuses on the delivery of products or services. In this context, the Code of Practice, in its introduction suggests that 'operational resilience can be considered as a subset of organizational resilience' and goes on to say that organizational resilience is the 'framework in which all resilience activities including operational, financial, environmental, reputational and human resilience can be positioned'
- making organizational resilience primarily a risk management or business continuity issue. Achieving resilience needs to be by design, and through adopting the principles laid out in the Code of Practice within strategy considerations and the design of the business model. A strategy or business model design that is inherently flawed from a resilience perspective cannot be made significantly more resilient through risk management or business continuity plans alone

- failing to adopt an ‘outside-in’ perspective of the organization – its role in society and within communities and the nature of its services or products – and therefore failing to invest in resilience where it matters most. For example, which services or products are truly essential from a customer, community or societal perspective? How much liquidity and strength of balance sheet is appropriate for financial resilience and is this accepted and supported by its investors?
- failing to recognize that an organization is only resilient if the wider system within which it operates is also resilient. For example, an organization must work with its suppliers, with those who deliver its goods and services to end customers and even with competitors (financial services is an example of this where the resilience of the ‘financial system’ is vital to the resilience of the individual organizations within it)
- not being sufficiently open to challenging (‘severe but plausible’) scenarios when stress testing, and therefore failing to understand at what point the organizations resilience may ‘break’. For example, if impact thresholds are breached too easily, the organizations resilience may not be enough, but if they are only breached in ‘extreme’ circumstances then this could be deemed satisfactory
- not achieving the necessary leadership commitment, senior accountability and appropriate governance to ensure organizational resilience is a strategic objective with the appropriate resources to achieve the intended outcomes

Wider context

The Code of Practice has been developed based on a review of several recent reports and industry practice, most notably, but not exclusively within the financial sector. As noted earlier, the regulators of the financial sector have taken significant steps to improve both the financial and the operational resilience of the sector, and this has provided the opportunity to consider these practices, learn lessons from them, and codify what appears to be working.

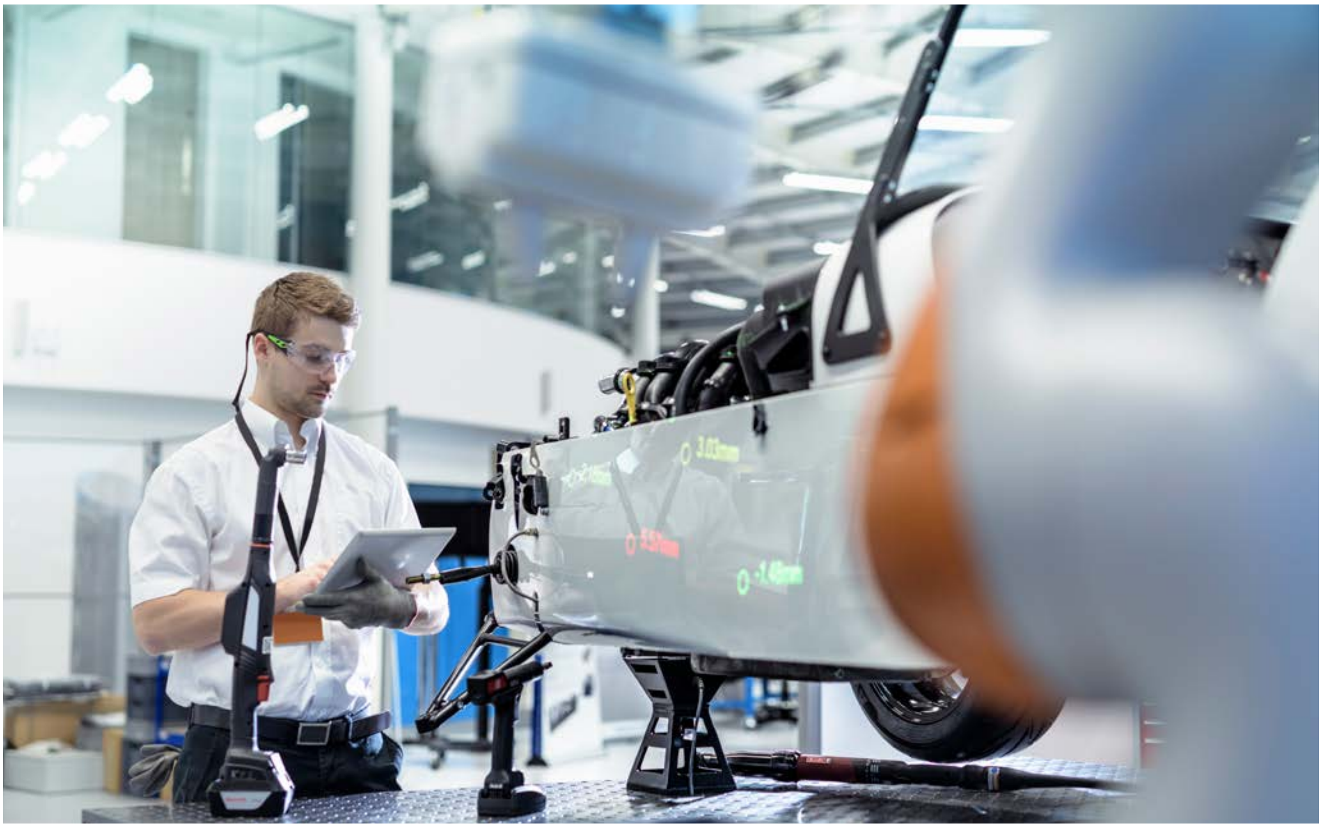
Reports from the National Infrastructure Commission, National Preparedness Commission and the OECD were also considered, as well as related British and International Standards. The list of these can be found in the Further reading section at the end of this brief.

It is likely that the International Standard on Organizational Resilience will also be revised in the next few years, and this Code of Practice may provide an important and relevant input to it.

Suggested next steps

If you are looking to improve the resilience of your organization, suggested next steps are:

- buy a copy of the new Code of Practice from the British Standards Institution
- start by considering the 'Guiding principles' and the extent to which these are being applied in your organization and where and how changes or improvements in their application could be made
- review and implement the recommended practices and apply these, together with the 'Guiding principles' across the five dimensions of finance, operations, human, social and environment
- be strategic in your approach considering the context of your organization and wider system within which it operates and focusing on 'essential outcomes' you identify
- consider how you wish to measure, monitor and report on your organization's resilience, and to who – some guidance on this is provided in the Code of Practice, together with a simple maturity model in the Annex A.
- ensure the governance and operating model to support, build and maintain organizational resilience is in place



Conclusion

In this time of uncertainty, volatility and change, building and maintaining organizational resilience has become a strategic issue in many boardrooms. They have recognized that resilience provides the ability to navigate such challenges – helping to anticipate and be able to absorb and adapt to them.

Resilience is also vital to the long-term performance and success of an organization – if you ask an athlete, they will likely tell you that it is something that they consciously develop and nurture as a strength, essential to their performance and success!

This Code of Practice will provide you with the principles and practices that can help you build and maintain your organization's resilience, and thereby creating a more resilient future for us all.

Further reading

Denyer, D. and Sutliff, M. **Resilience reimagined: A practical guide for organisations**. National Preparedness Commission, Cranfield University and Deloitte, 2021.

Financial Conduct Authority. **Policy Statement (PS) 21/3: Building operational resilience: Feedback to CP19/32 and final rules**.

Prudential Regulatory Authority. **Supervisory Statement (SS) 1/21: Operational resilience: Impact tolerances for important business services**.

National Infrastructure Commission. **Anticipate, react, ecover. Resilient infrastructure systems**. May 2020.

OECD (2014). **Guidelines for Resilience Systems Analysis; How to analyse risk and build a roadmap to resilience**. OECD Publishing.

BS EN ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

BS ISO 22301:2014, Societal security — Business continuity management systems — Requirements

PD ISO/TS 22317:2015, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

PD ISO/TS 22318:2021, Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management

BS 31100:2021, Risk management — Code of practice and guidance for the implementation of BS ISO 31000:2018

About the author

Rick Cudworth
Director, ResilienC.

Rick Cudworth is a recognized leader in Organizational Resilience, Operational Readiness and Strategic Risk Mitigation. He is Chair of the British Standards Institution Technical Committee for Continuity and Resilience and a member of the Cabinet Office Behavioural Science Expert Group as part of the National Security Risk Assessment process for the UK. He edited and contributed to the National Preparedness Commission's Report: 'Resilience reimagined: A practical guide for Organisations', published in March 2021 in collaboration with Cranfield University.

Following a successful career with as a Partner at KPMG and Deloitte for over 20 years, he has established a new consultancy firm, ResilienC.

Technical reviewer

David Austin, Director, Operational Resilience Ltd

Why choose BSI?

As the financial, environmental, and social climates of our planet continuously shift, BSI's founding purpose to benefit society is more relevant now than ever before.

By shaping, sharing, embedding, assessing, and supporting industry best practice, for 120 years BSI has equipped organizations with the tools and techniques they need to turn today's challenges into tomorrow's opportunities.

Working globally across a range of sectors – with specialist expertise in the sustainability and ESG, built environment, food and retail, and healthcare – BSI offers a range of services and solutions to make organizations worldwide more trusted and resilient. We adopt innovative technology and processes to offer our services in an efficient and effective manner, partnering with our clients to embed sustainable behaviours for the long-term benefit of their people, their customers, and our planet.

bsi.

Read more about standards at:
knowledge.bsigroup.com