BS 65000:2014

BSI Standards Publication

Guidance on organizational resilience

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

Published by BSI Standards Limited 2014

ISBN 978 0 580 77949 7

ICS 03.100.01

The following BSI references relate to the work on this document:
Committee reference SSM/1
Draft for comment 14/30258791 DC

Publication history

First published November 2014

Amendments issued since publication

Date	Text affected

Contents

List of figures

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 16, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 November 2014. It was prepared by Technical Committee SSM/1, *Societal security management*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

It has been assumed in the preparation of this British Standard that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Resilience is a strategic objective intended to help an organization to survive and prosper. A highly resilient organization is also more adaptive, competitive, agile and robust than less resilient organizations.

Organizational resilience is the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes.

Resilience is a relative, dynamic concept and, as such, an organization can only be more or less resilient. As a result, resilience is a goal, not a fixed activity or state, and is enhanced by integrating and coordinating the various operational disciplines that the organization might already be applying (see **5.4**). In addition, an organization operates within a potentially complex web of interactions with other organizations, so it is essential to build resilience not only within the organization, but across its networks, and in its interactions with others. The organization therefore needs to provide direction to its efforts and ensure effective governance and risk management, as well as build resilience in partnership with others.

This British Standard gives guidance on achieving enhanced organizational resilience. In particular, it describes organizational resilience, articulates its benefits, and explains how to build resilience. To aid the integration and coordination of the various disciplines that are essential for resilience, the standard references other standards, published and in preparation, relating to these disciplines. Finally, it offers some basic models for assessing the resilience measures of an organization.

1 Scope

This British Standard gives guidance on building organizational resilience by:

a) clarifying the nature and scope of organizational resilience for top management (see note);

b) identifying the principal components of resilience to enable an organization to review its resilience and to implement and measure improvements; and

c) identifying and recommending good practice already defined in existing standards and disciplines.

*NOTE References to "top management" throughout this standard are to be interpreted as including both of the bodies defined in **2.2** and **2.6**.*

This standard also gives guidance on how other standards contribute to the development and management of organizational resilience with a consistent good practice structure, using agreed terminology and practices (see Bibliography) relevant to the development and management of organizational resilience.

2 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

2.1 governance

system by which the organization is directed, controlled and held accountable to achieve its core purpose over the long term

NOTE The term "corporate governance" is typically used for the governance of private and publicly-listed companies or to denote governance of the whole organization.

[BS 13500:2013, modified]

2.2 governing body

individual or group of people ultimately responsible and accountable for the long-term direction and control of the organization

NOTE Governing body can in some jurisdictions be a board of directors.

[BS 13500:2013]

2.3 organizational resilience

ability of an organization to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper

2.4 risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

[ISO Guide 73:2009]

2.5 situational awareness

state of individual and/or collective knowledge relating to past and current events, their implications and potential future development

[BS 11200:2014]

2.6 top management

person or group of people who directs and controls an organization at the highest level

NOTE Top management has the accountability for the execution of the direction provided by the governing body and may delegate its responsibilities whilst remaining accountable to the governing body.

[BS ISO/IEC 27000:2014, modified]

3 Overview of organizational resilience

3.1 Principles

Resilience involves dealing with disruption, uncertainty and change with clear intent, coherence and appropriate resourcing. In particular, it is a combination of maintaining continuity through disruptive challenges, and long-term viability against a backdrop of strategic change and the changing external environment. The first of these is a precondition for, but no guarantee of, the second. Resilience is therefore a strategic concern requiring effective leadership, with direction and enduring commitment from the very top of an organization through its governance and risk management.

Resilience needs to be embedded across the organization, cutting across silos, organizational structures and hierarchies, with operational activities aligned with strategic priorities. In addition, the organization needs to satisfy itself that its relationships with partners, outsourcers, suppliers and other key interested parties are sufficiently resilient (and satisfy them of its own high level of resilience).

Resilience is inherently relative, and no organization, person, network or system can be absolutely resilient, as they experience constant change and operate under varying degrees of uncertainty. An organization that is highly resilient to certain risks might be vulnerable and less resilient if exposed to others. Organizational resilience should therefore be informed by effective risk management practices (see BS ISO 31000).

3.2 Benefits of building resilience

The core strategic purpose of resilience is to enable an organization to survive and prosper. However, resilience is also closely aligned with the concerns of most managers, which can be summarized as follows.

a) **Competitiveness.** Being able to continue past, recover and learn from and, where appropriate, capitalize upon the opportunities presented by disruptions can increase value better than competitors who are less resilient. A highly resilient organization is able to identify and adapt to change and uncertainty before the case for change becomes urgent. The behaviours that an organization develops as part of a resilient culture can also help to build innovation and common values and vision, and develop an ability to anticipate and adapt to change and evolve the business model.

b) **Coherence.** A highly resilient organization aligns operational resilience measures with strategic resilience objectives. The former are protective, risk control and response measures, and the latter define the organization and guide its longer-term decision making. The side-to-side and top-to-bottom integration and coherence of these is fundamental to resilience. Resilience both requires and allows organizational silos to become more integrated and interoperable.

c) **Efficiency and effectiveness.** Working within a coherent and integrated framework has time- and cost-saving implications. An organization’s framework for resilience meshes together diverse components, allocating resources to improve overall resilience, efficiency and effectiveness.

d) **Reputation.** The coherent framework built by resilience supports the organization in understanding and acting on the interdependency of brand, trust and reputation, thereby managing and enhancing its reputation.

e) **Societal/community resilience.** Societal and community resilience are enhanced by organizational resilience, particularly when the organization provides vital products and services to the public. Resilience can also give assurance to other interested parties, such as regulators, third parties, government, customers, partners and shareholders.

3.3 Challenges to building resilience

To secure the benefits of building resilience, a number of challenges and dilemmas need to be confronted:

a) understanding when to take action;

b) resolving potential tensions between cost and resilience in building just-in-time processes and just-in-case redundancy (see **5.6**);

c) determining an appropriate trade-off between controlling costs and achieving greater resilience;

d) identifying when to embrace new values rather than persisting with existing behaviours;

e) resolving conflicts between the need to keep information from competitors and the need to share information for resilience when collaborating with others; and

f) identifying legal and regulatory constraints, as well as voluntary codes adopted by different sectors, that can limit desirable resilience actions.

Each organization comes to its own decisions on these issues according to the amount and type of risk it is willing to pursue or retain, and the amount it is willing to invest in resilience.

4 The organizational foundations for resilience

4.1 General

For an organization to build resilience (Clause **5**) it first has to have in place the fundamental attributes set out in **4.2** to **4.4** (see Figure 1). These go beyond what the organization does and what it has. They define the attitudes that shape decisions and actions, and ultimately underpin resilience.

4.2 Governance and accountability

The systems of rules, structures and processes that drive coherent decision making within acceptable parameters of cost, risk and speed contribute to resilience. Effective governance enables the exploitation of opportunity and the mitigation of risk, and ensures that appropriate persons and teams are accountable for decisions, according to the organization's nature and level of maturity. Effective governance also provides an environment in which innovation is encouraged and investment is well managed. Resilience is therefore an outcome of good governance.

The governing body and top management together are ultimately accountable for ensuring that an appropriate level of resilience is achieved by the organization alongside other desirable outcomes such as profitability, service delivery, quality and compliance. Indeed, where necessary, it is their obligation to define the balance to be achieved of such outcomes.

4.3 Leadership and culture

Leaders should consider the impact of all strategies and decisions, both at the time decisions are taken and on an ongoing basis. They should seek to build a culture in which it is normal to consider resilience within decision making. Staff should be appropriately empowered by a culture of trust, openness and innovation such that they are both motivated and able to assume ownership of, and address, risks and issues as they arise. Authority and responsibility should be delegated to the individual(s) best able to make the right decision for the organization, in times of crisis as well as during business-as-usual. Transparency should be encouraged and information should be proactively shared across internal boundaries with interdependent partners.

The leadership's approach to key stakeholders, for example customers, communities, suppliers, shareholders, regulators, partners and competition, recognizes the impact of each upon the other. The organization should foster relationships with these groups to further its resilience objectives.

4.4 Common vision and purpose

The purpose of the organization and a common vision of the future, and its consequent requirements for resilience, should be recognized and shared throughout the organization so that challenge, change and opportunity are assessed against the purpose and vision and can be acted upon accordingly.

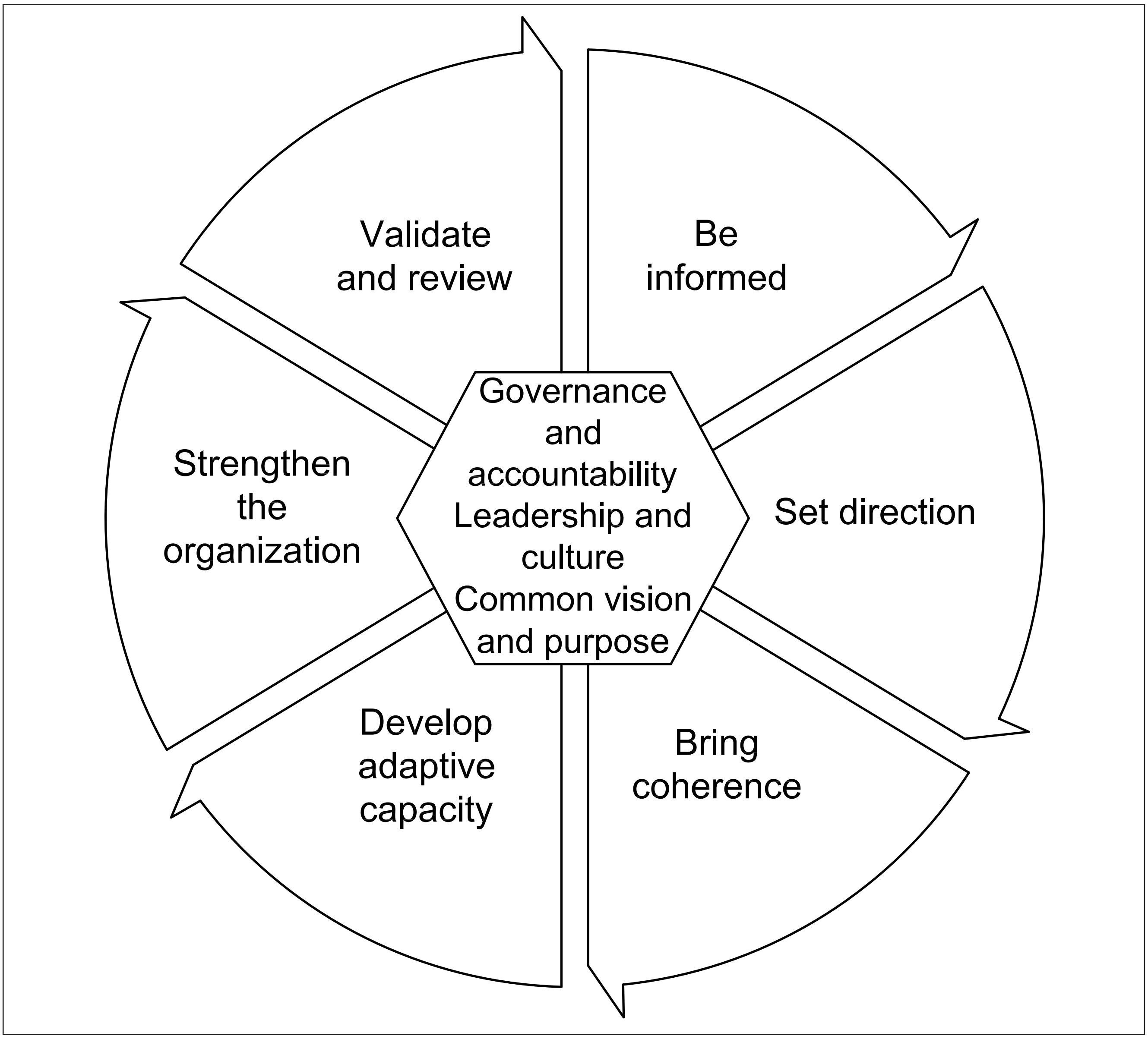
Organizational values should be embedded which contribute to resilience through actively informing decision making and action throughout the organization. These values allow people acting on behalf of the organization to improvise and innovate, knowing that their actions support the core purpose and values of the organization, including resilience.

5 Building resilience

5.1 General

Resilience requires the ability to make good decisions informed by an understanding of what the organization stands for and where it is trying to go, the organization's environment, what matters to the organization and what resources it has at its disposal (see **5.2**). This knowledge should then be used to determine the actions necessary to make the organization more resilient. These are set out in **5.3** to **5.7** (see also Figure 1). Most of the steps are continuous or repeated periodically.

Figure 1 **Developing resilience**


Validate and review
Be informed
Strengthen the organization
Governance and accountability
Leadership and culture
Common vision and purpose
Set direction
Develop adaptive capacity
Bring coherence

5.2 Be informed (situational awareness)

The organization needs to be highly informed about its environment, both internal and external, and risks, events and opportunities that might influence or compromise its resilience, recognizing that some opportunities and latent weaknesses are internal while others are beyond direct control. Specifically, the organization should achieve this situational awareness by:

- identifying what it values and wants to protect, and any single points of failure that could impact what the organization values;
- establishing and resourcing a system to anticipate, identify, monitor and evaluate the trends, potential issues, opportunities and future developments, emerging and approaching over different timescales (also known as "horizon scanning"), that could impact upon the organization;
- drawing upon the existing risk management framework, continuously monitoring the **environment** in which it operates, including the legal and

regulatory context, the geopolitical and competitive environment and the organization's stakeholders' needs and expectations;

NOTE 1 The organization may detect threats informally, e.g. identifying a new competitor or a change in the way the organization is funded, but ought to build this into a capability to consistently identify threats before they pose a risk and to consistently identify opportunity before it has diminished. To do this the organization ought to engage in stakeholder management and collaboration, actively participate in discussion and debate relevant to it and develop a high level of awareness of its organizational environment. Risks ought to be documented and tracked to enable the organization to further understand trends or common sources of risk.

NOTE 2 Monitoring might require the organization to establish and resource systems, processes and controls to make it more responsive to rapidly emerging risks.

- understanding the overall strategy of the organization and its implications for resilience;
- understanding the current level of its resilience, i.e. maturity (see Clause **6**);
- understanding the interdependencies with other organizations (e.g. suppliers, outsourcers and competitors), their resilience and events to which they have responded;
- understanding and validating the explicit and implicit **assumptions** that underpin the resilience of the organization; and
- **identifying** and capturing lessons to be learned and embedded in the future (see **5.5**), drawing on events, including, but not limited to:
  - successes;
  - experience;
  - near misses;
  - failures;
  - exercises (see **5.7**);
  - audits;
  - assessments (see Clause **6**); and
  - learning from others.

5.3 Set direction

Top management should ensure that the organization has a clearly identified purpose, a vision for its future direction and aspirations, and clearly articulated values and priorities, including requirements for resilience, which are shared and understood throughout the organization. Specifically:

- all aspects of **governance** (see BS 13500) should be integrated into a single, coherent, transparent and forward-looking system that is embedded in a culture which empowers staff and encourages the continuous enhancement of organizational resilience;
- the **core purpose** and vision of the organization should be clearly articulated and communicated to all staff, partners and other interested parties;
- the **values** of the organization, which set out the universal expectations for conduct and decision making for all of its people, should underpin and shape the behaviours that strengthen the organization and promote flexibility that enables adaptability;
- the strategic **priorities**, including the level of resilience sought and the

timescales for this, should be clearly set out and act as the "compass" to align and focus effort and resourcing within the organization; and

- clear **roles and responsibilities** should be established for different aspects of organizational resilience planning.

5.4 Bring coherence

The governing body of the organization sets priorities for the organization to ensure resilience and inform operational activities. Top management should align operational activities with these priorities and achieve coherence across the various management systems, to build resilience. To ensure that organizational silos support resilience, the organization should integrate the risk management activities and operational disciplines, and ensure that knowledge is actively shared across internal organizational boundaries, so that risks and opportunities are addressed coherently by all parts of the organization. Specifically:

- the **management** of all of the risks and resilience capabilities should be **coordinated** so that they directly and collectively contribute to the organization's core purpose and the protection of what it values;
- the organization should **manage change** to enhance organizational resilience by ensuring that, whilst new initiatives and organizational models for improvement are taken up, they have appropriate levels of resilience "built-in", ensuring that unnecessary overlap in activities and processes that waste resources is avoided and that resilience is neither weakened nor made excessive as a consequence of the change activity;
- the **operational disciplines** to be integrated should include, but not be limited to, the following:
  - asset management (BS ISO 55000);
  - risk management (BS ISO 31000 and BS 31100);
  - stakeholder and collaboration management (BS 11000);
  - reputation management;
  - horizon scanning;
  - environmental management (BS EN ISO 14001);
  - health and safety (BS OHSAS 18001);
  - fraud control;
  - business continuity (BS ISO 22301);
  - information, communications and technology (ICT) continuity (BS ISO 27031);
  - cyber security (PAS 555);
  - change management;
  - information security (BS EN/ISO 27001);
  - physical security;
  - facilities management;
  - emergency management;
  - crisis management (BS 11200);
  - supply chain (BS ISO 28000, and PD 25222);
  - human resource planning;
  - financial control; and

  - quality management (BS EN ISO 9001);

- the organization should create the means, incentives and imperatives to **communicate and share information** about risks, incidents, near misses, vulnerabilities and opportunities across the organization and with partners and other interested parties, including competitors where this could realize mutual benefit, in order to ensure that actions are taken to strengthen the organization throughout; and

- the organization should go beyond information sharing to **collaboration** (see BS 11000) and joint actions where this realizes mutual benefit and where interdependencies require this.

5.5 Develop adaptive capacity

The organization should build an ability to adapt to changing conditions as they emerge, switching between pre-planned responses and adaptive actions as necessary and modifying its structures, activities and behaviours to adjust to new conditions, while retaining its core purpose, vision and values. Specifically, the organization should:

- build an ability to identify and respond to change in a **resourceful** manner and to modify assets, arrangements, structures, activities and behaviours to adjust to new conditions;

  NOTE One aspect of this is the ability to redeploy assets to respond to disruption.

- promote **innovation**, e.g. introducing new methods, ideas and/or products that exploit opportunity and control risk, such that everyone proactively applies learning to identify new and better solutions and address the shifting needs of the organization arising from its changing environment;

- enable **flexibility** and **agility** such that everyone is able to improvise and change to address current and future challenges and create and exploit opportunity, whilst maintaining coherence; and

- build **adaptive capacity** through applying the lessons identified (see **5.2**) by:

  - disseminating and implementing good practice identified from within and outside the organization;

  - sharing errors, failures and mistakes openly such that all appropriate parts of the organization learn from and avoid these same issues;

  - proactively seeking lessons from other organizations and other operating contexts; and

  - training and developing people to contribute to innovation and providing an environment that enables flexibility when required.

5.6 Strengthen the organization

5.6.1 The organization should implement specific measures that strengthen its ability to address disruptive events, emergent risks and changes in the operating environment. Specifically, the organization should:

- ensure resilience is routinely considered during decision making and change management;

- take actions to **prevent** or reduce the likelihood of disruptive events or disruption to what it values, including people, physical assets, financial value, reputation and social capital through traditional operational disciplines (see **5.4**);

- accept that some disruptions cannot be prevented and will still occur, and therefore plan, implement, test and review a range of measures to:
  - **prepare** to deal with disruption, possibly arising from unforeseen events; and
  - effectively **adapt** when the established plan does not cover what is being experienced;
- improve **adaptability** through encouraging **innovation** and willingness to embrace change at all levels, so that products, services and business processes are improved to better fit the new conditions brought about by long-term changes to its environment;
- take actions to **protect** its people, physical assets, financial value, reputation and social capital, thereby enabling it to **resist** disruption;
- enhance resilience, by design, by taking appropriate decisions on resourcing and capacity, diversification and replication (**redundancy**) to avoid single points of failure and provide the ability to change or react with relative ease, so that core services are maintained at an acceptable, pre-determined level;
- ensure that it has the ability to take timely and informed actions to intercept and contain adverse events, both foreseen and unforeseen, and mitigate their impact (**respond**), including overwhelming crises that threaten its continued existence;
- ensure that it has the ability to sustain and transition a response through to **recovery** to an agreed state, within agreed timescales and with enhanced resilience capabilities as appropriate; and
- encourage broader participation of business units and proactive collaboration between them to drive continuous improvement of organizational processes and practices.

This requires properly resourced preparations, investing in the development of people (not just the plans) to provide long-term capability, and the building of a crisis management capability (see BS 11200) to permit the organization to continue to operate under a range of challenging conditions.

5.6.2 The organization should promote and create universally shared expectations that strengthen its resilience. Specifically, the organization should:

- develop and promote **cultural norms** that embody its values, including openness in review and evaluation of its resilience, other achievements, goals, mechanisms and processes;
- exhibit and encourage **behaviour** that reflects the cultural norms, which are in turn rooted in the core purpose and values of the organization;
- **trust** its people to exhibit behaviours that strengthen resilience, and encourage its people to trust the organization to protect them when they are working towards resilience;
- enable and prioritize **learning** from the sharing of positive and negative experiences, including risks, incidents, near misses, vulnerabilities and opportunities, with learning involving demonstration of evidence-based actions to strengthen resilience;
- **act** on lessons learned to change and prompt strategic review as appropriate, in order to change structures, activities and behaviours, and to demonstrate that it has taken positive proactive action to improve and seize opportunities; and
- define levels of **accountability** by which individual and collective decisions

and actions are related to the norms, expectations and obligations of the organization, its partners, stakeholders and other interested parties.

The organization should seek to influence its environment in order to enhance its resilience, e.g. influencing the legal and regulatory environment, without prejudice to the needs and interests of other interested parties.

5.7 Validate and review

The organization should undertake, audits, exercises and testing that demonstrate the efficacy or otherwise of its strengthening measures and the capacity of people and teams to learn and adapt when required. The outcome of, and lessons learned from, the activities in **5.3** to **5.6**, together with the organization's assessment of resilience undertaken in accordance with Clause **6**, should inform the organization's understanding of its resilience capability (see **6.2**) and, if necessary, be used to prompt strategic change. As part of this, the organization should verify that it is complying with legal and regulatory obligations (see **5.2**).

6 Assessing the resilience of an organization

6.1 Maturity and measurement

Organizational resilience is inherently relative and no organization can be definitively "resilient". An organization's resilience can be enhanced or degraded as it adapts to changes in its structure, goals and external events. The organization should ensure that the performance and suitability of its current resilience measures are assessed and evaluated at agreed frequencies, agreed with the governing body, according to its risks, needs and aspirations.

The organization should use appropriate measurements to undertake a baseline review to determine existing levels of resilience. This should support an assessment of whether existing levels are acceptable.

The organization should identify:

- what needs to be monitored and measured;
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- how to provide a continuous assessment of resilience;
- the thresholds at which the output from measurements will be considered acceptable;
- how measurement and monitoring arrangements will work alongside, support or integrate into existing monitoring processes; and
- how the results from monitoring and measurement shall be analysed and evaluated.

The organization should seek to understand what evidence it requires to support its assessment of resilience and ensure there is an evaluation process is developed to support this.

A basic maturity model, such as the example in Figure 2, can assist in determining to what extent an organization is addressing good practice.

Figure 2 **Maturity model for organizational resilience**

Level of maturity	Notes
Level 0: Immature	Few measures implemented to strengthen the organization. No coherent framework and no management direction. No encouragement of innovation or flexibility.
Level 1: Basic	Organization strengthened through specific disciplines. No formal communication on organizational resilience across the organization.
Level 2: Managed	Activities are controlled and maintained with results specified. Limited coordination between related activities. Improvements made in isolation.
Level 3: Established	Management has set direction and understands the internal and external environment and how it is changing. Steps and programmes undertaken to bring coherence to organizational resilience and to strengthen the operations. Programme to strengthen the organization in operation.
Level 4: Predictable	Organizational resilience being executed consistently over several years, aligned with corporate strategy. Coherent approach working. Strengthening measures implemented and agreed, continual improvement ongoing.
Level 5: Optimizing	Activities are repeated, measured, evaluated and continuously improved to meet current and projected business goals. Divisions are proactively cooperating for improvement. Collaboration with other organizations, as appropriate. Demonstrated application of innovation and flexibility throughout the organization.

6.2 Questions to ask of the organization

The questions that may be asked to determine how an organization’s resilience measures up against the good practice principles are set out in Figure 3. The answers need to be supported by evidence.

Figure 3 **Questions to determine consistency of resilience measures with BS 65000**

No.	Question	Key issues raised	Clause
Be informed			
1	Do we have effective mechanisms to identify and understand current and future risks on the horizon in sufficient detail to develop a strategy and plans to meet the issues that face us?	Linkage of risk, strategy and action	**5.2**
2	Do we know what is important to us and is the resilience implemented consistent with the amount and type of risk we are willing to pursue or retain?	Understanding	**5.2, 5.4**
Set direction			
3	From the Executive and Board level, do we understand what resilience means to us as an organization, and does this align with our core values and strategic aims?	Resilience strategy and approach Culture, behaviours, structure, ownership	**3.1, 4, 5.2, 5.6.2**
4	As leaders, do we have a clear vision of where we as an organization should go, and what we should avoid? Is this vision clearly communicated throughout the organization?	Vision, strategic direction, risk and horizon scanning linkages, strategic threats	**4.4, 5.2**
5	Does resilience form a part of our Board agenda for regular consideration?	Top management buy-in Value and understanding	**4.3, 5.2**
6	Have we defined and established where the responsibilities lie for us to become more resilient?	Linkage of systems, disciplines and strategy	**4.4, 5.1, 5.2, 5.3, 5.4**
Bring coherence			
7	Are we aware of the critical interdependencies, both internal and external, and do we actively consider these when making decisions?	Understanding	**3.2, 4.3, 5.2, 5.4**
8	Have we established which strategic and operational responsibilities support us to become more resilient?	Understanding and coherence	**4.4, 5.2, 5.4**
9	Do we take timely and informed actions to intercept adverse events, mitigate their impact and sustain the transition to recovery and beyond?	Recover	**5.6.1**
10	Do projects always account for resilience to ensure that these enhance and do not weaken capability?	Attitude to change Change management	**3.1, 4.4, 5.2, 5.4, 5.5, 5.6, 5.7**
11	Is our culture sufficiently open and transparent: a) to allow critical risks that are recognized at a low level to be escalated appropriately; and b) that top management pass relevant information down to the appropriate level(s)?	Transparency	**4.1, 4.3, 5.2**
Develop adaptive capacity			
12	Are we flexible enough to respond rapidly to major emerging business risks?	Understanding, coherence, coordination, communication	**5.2, 5.3, 5.4, 5.5**
13	Do we have plans to deal with disruption, the capability to respond to unforeseen events and the ability to successfully adapt when the established plan does not fit what is being experienced?	Prepare	**5.6.1**

Figure 3 **Questions to determine consistency of resilience measures with BS 65000**

No.	Question	Key issues raised	Clause
14	Are we confident that our approach to resilience will stand up to external scrutiny?	Actionable strategy, performance-driven, valued activity	**4.3**, **4.4**
Strengthen the organization			
15	Are we satisfied that our approach to resilience is coherent and is embedded within the organizational vision?	Leadership	**4.3**, **4.4**, **5.4**
16	Are those responsible for delivering greater organizational resilience empowered to work across boundaries and able to speak to top management easily?	Leadership, empowerment, value of resilience, understanding	**4.3**, **4.4**, **5.2**, **5.6**
17	Have we taken steps to protect what we value, including people, physical assets, financial value, reputation and social capital?	Protect	**5.6.1**
18	Do we have the ability to ensure continuity of services in the event of failure?	Adaptive capacity	**5.5**
19	Do we have a programme to build organization’s capability for resilience by developing appropriate competencies among key employees?	Competences	**5.5**, **5.6**
20	Do we learn by identifying the lessons of events, and acting on them in order to change structures, activities and behaviours?	Learn	**5.2**, **5.5**, **5.6**, **5.7**, **6**
21	Do we adapt products, services and processes to better fit the new conditions brought about by long-term changes to our environment?	Adaptive capacity	**4**, **5.5**, **5.6**
Validate and review			
22	Do we test/flex our resilience against a range of operational and strategic scenarios?	Future planning and top management buy-in	**5.2**, **5.7**, **6**
23	Do we audit, exercise and test our resilience capabilities?	Validate and review	**5.6**, **5.7**
24	Does our top management team know exactly the procedures to follow in a crisis and what else happens across the organization? Do we rehearse this?	Top management buy-in, value, preparedness, governance	**4.2**, **5.7**

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 11000, *Collaborative business relationships*

BS 11200:2014, *Crisis management – Guidance and good practice*

BS 13500:2013, *Code of practice for delivering effective governance of organizations*

BS 31100, *Risk management – Code of practice and guidance for the implementation of BS ISO 31000*

BS EN ISO 9001, *Quality management systems – Requirements*

BS EN ISO 14001, *Environmental management systems – Requirements with guidance for use*

BS EN/ISO 27001, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO 22301, *Societal security – Business continuity management systems – Requirements*

BS ISO 27031, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

BS ISO 28000, *Specification for security management systems for the supply chain*

BS ISO 31000, *Risk management – Principles and guidelines*

BS ISO 55000, *Asset management – Overview, principles and terminology*

BS ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

BS OHSAS 18001, *Occupational health and safety management systems – Requirements*

ISO Guide 73:2009, *Risk management – Vocabulary*

PAS 555, *Cyber security risk – Governance and management – Specification*

PD 25222, *Business continuity management – Guidance on supply chain continuity*

Further reading

ANSI/ASIS PAP.1-2012, *Security Management Standard: Physical Asset Protection*

BS EN ISO 14004, *Environmental management systems – General guidelines on principles, systems and support techniques*

BS ISO 22398, *Societal security – Guidelines for exercises*

BS ISO/IEC 20000, *Information technology – Service management*

BS ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*

BS ISO/IEC 27013, *Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

ISO 19600, *Compliance management systems – Guidelines* (in preparation)

ISO 37001, *Anti-bribery management systems* (in preparation)

ISO/IEC TR 90006, *Information technology – Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011*

PAS 99, *Specification of common management system requirements as a framework for integration*

PAS 7000, *Supply chain risk management – Supplier prequalification*

PD 25666, *Business continuity management – Guidance on exercising and testing for continuity and contingency programmes*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™