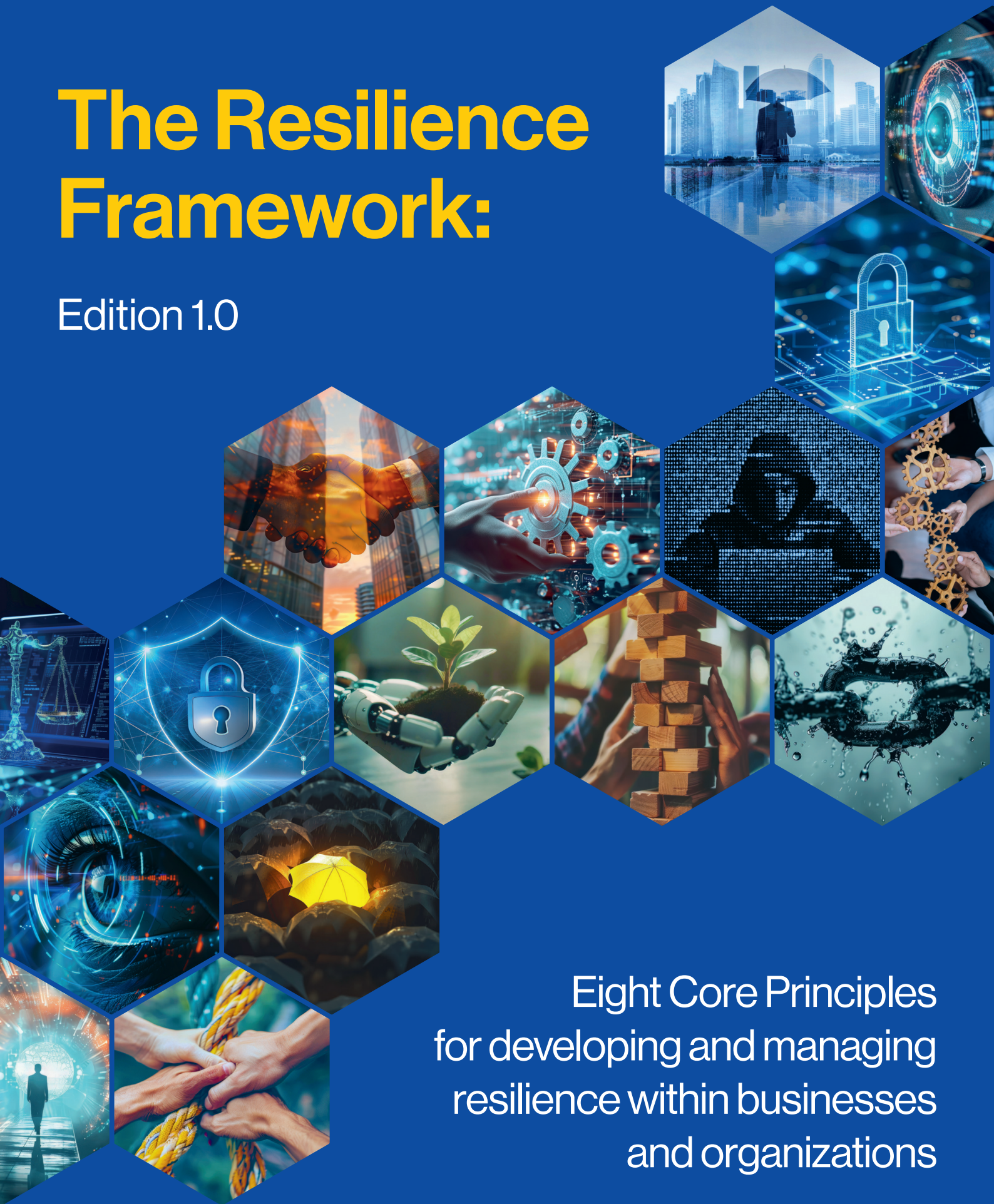


# The Resilience Framework:

Edition 1.0



Eight Core Principles  
for developing and managing  
resilience within businesses  
and organizations

# Contents

- 03 Foreword
- 04 About the BCI
- 05 Executive summary
- 10 Introduction
- 16 Part One: The Core Principles of Resilience Development and Management
- 36 Part Two: Using the Core Principles
- 42 Acknowledgements
- 43 References



## Foreword

The BCI’s remit is to lead the way in resilience and this document aims to continue our commitment to this.

The Resilience Framework is focused on providing strategic guidance and as such is aimed at organizational leaders and top management, enabling the establishment of a resilience management cycle, which will in turn ensure the longevity and competitiveness of the organization.

The Resilience Framework is not directive — it does not detail specific solutions for developing resilience; instead it provides eight Core Principles which will inform resilience excellence. It also combines these into the Resilience Framework Cycle, which provides a structured way to implement the Core Principles.

One of the key aims of the Resilience Framework was to provide guidance which applies to any organization of any size and operating in any industry, profession, or market. I feel that this has been achieved: the Core Principles are universal and the Resilience Framework Cycle is appropriate for every organization.

The Resilience Framework will be a living document that will be reviewed annually to keep it at the forefront of strategic resilience management. To help with this, your feedback would be invaluable. You can find out how to provide your thoughts and input at the end of the document.



**David Thorp**  
Executive Director  
BCI

## About the BCI

The BCI is the global membership association of choice for business continuity and resilience professionals. With 9,000 members in more than 120 countries, we provide education, training and certification, membership, thought leadership, events, and more.

Our mission is to unlock potential through global collaboration, education, foresight and innovation, rooted in world-class knowledge, forging a more resilient future and leaving a sustainable legacy.

Find out more at [www.thebci.org](http://www.thebci.org)

**bci** Leading the way  
to resilience

## Executive summary

Developed by the BCI via a panel of experts, the Resilience Framework offers a robust structure for organizations aiming to develop and enhance resilience in a systematic manner. It starts from the premise that resilience is the key objective of all protective processes carried out by organizations, that there are common foundations that underpin the development of resilience and its management; and that these relate to all organizations and settings.

**The document has two main sections:**

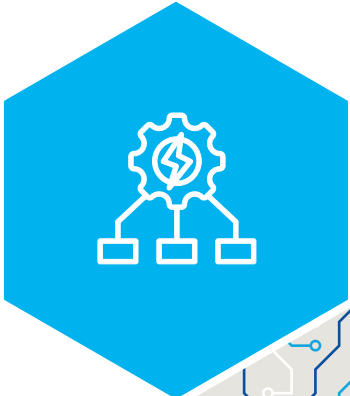
- The Core Principles of Resilience Development and Management.
- Using the Core Principles:  
A framework for developing and managing resilience within a business and organizational setting.

# The Core Principles of Resilience Development and Management

The Core Principles provide a set of eight universal principles that establish a baseline for all resilience development and management activities within an organization. They are:

## Core Principle One: Resilience is Led from the Top

Resilience initiatives must be led by the organization's top leadership, establishing resilience as a strategic priority directly influenced by the highest levels of decision-making. Organizations need to determine from the outset how this requirement will be translated, who amongst the top leadership will take the lead, and how other members of the top leadership will govern, monitor, measure, and challenge the resilience programme. Top leadership is central to the development and management of resilience and is involved throughout the whole cycle.



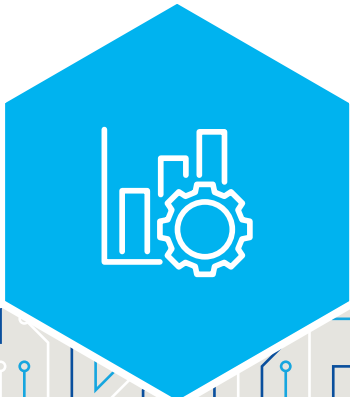
## Core Principle Two: Requires Clear Direction on Purpose, Objectives, and Required Outcomes

The resilience programme requires clear and continued guidance on three key areas: purpose, objectives, and required outcomes; and this is the responsibility of top leadership to establish, direct, and govern.



## Core Principle Three: Requires a Comprehensive Understanding of the Organization's Current State

To develop resilience a complete and clear picture of the business or organization and its wider ecosystem is essential. Understanding the current state of the organization, the external and environmental factors impacting upon it, and its existing levels of resilience provides the starting point for considering what additional activities are required to achieve the desired resilience outcomes. This gives a roadmap of existing good practices and capabilities that can be built upon or expanded; and it also provides clarity on existing silos that need breaking down.



## Core Principle Four: Take a Risk-based Approach

Resilience in a business and organizational context is risk-based. Organizations need to understand what they need to be resilient against; and that requires an understanding of the risk environment. This will drive the priorities, the strategies, and the resilience decision-making.



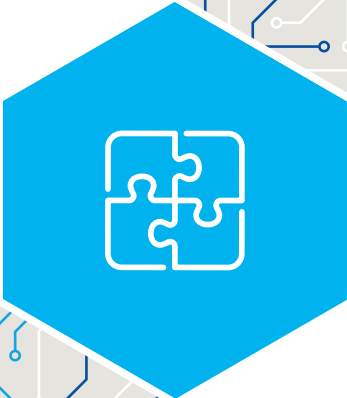
## Core Principle Five: Resilience is Coherent and Collaborative

Resilience strategies need to be coherent and integrated across the whole organization and require collaborative efforts both internally and with external stakeholders. This Core Principle involves breaking down organizational silos and enabling the management and development of resilience to take place in a structured, consistent, and aligned way.



**Core Principle Six:**  
**Incorporates a Defined Set of Strategies and Related Operational Solutions**

Organizations need to have specific, clearly defined resilience strategies and related operational solutions tailored to their unique needs and environments.



**Core Principle Seven:**  
**Being Able to Adapt is a Characteristic of Resilience**

The capability to adapt is an organizational skill and ability, which flows from and is led by top management. It is used on a day-to-day basis to help the organization develop to ensure long-term sustainability and growth; and it is used in response to an incident or event to determine whether and how the organization needs to change or transform in order to be able to continue to deliver on outcomes during and after the challenging situation. Being able to adapt is an intrinsic capability that flows through and informs the whole resilience cycle.



**Core Principle Eight: Is Always Cyclical**

Resilience is not a static project but a continuous cycle of reviewing, assessment, learning, and improvement. There are many ways of achieving this and the appropriate methods will be determined by top management.

**Using the Core Principles**

**A framework for developing and managing resilience within a business and organizational setting**

In the second section of this document, the above eight Core Principles are structured within the Resilience Framework Cycle. This demonstrates how the Core Principles fit together and flow into each other in a continual improvement process. The Resilience Framework Cycle can be used in a structured way by businesses or organizations of any size or type to develop or improve a resilience programme.



# Introduction

Resilience has many expressions throughout businesses and other organizations, but if resilience is a desired state or characteristic that can be developed, improved, and managed, then resilience must have common foundations. The Resilience Framework was born out of a determination by the BCI to explore what these common foundations are and how an organization can introduce and nurture them.

The Resilience Framework was developed by a Technical Advisory Group, a selection of industry experts, who spent many hours exploring, debating, and honing the eight Core Principles of resilience, which are explored in this document. These are the essential elements that help make something 'resilient' within a business and organizational setting and which, if any are missing, mean that the organization isn't as resilient as it could be.

Exploring the Core Principles and implementing them in a structured way through the Resilience Framework Cycle, which is presented in the second part of this document, an organization can determine how resilient it really is and can identify areas where it can improve in a strategic and managed manner.

The Core Principles are universal: they are relevant to any type of organization, however small or large, whatever sector it operates in, and whatever it does. The Core Principles also apply to all dimensions of developing the overall resilience of an organization. Whether an organization wishes to undertake a fully-fledged organizational resilience programme, or a more specific cyber, supply chain, climate, or operational resilience programme, the Core Principles still apply.

## Why resilience?

The Resilience Framework starts from the premise that resilience is the key objective of all protective processes carried out by organizations. In other words, resilience is how an organization responds to uncertainty, disruption, and change: challenges that reduce its ability to achieve its outcomes. Resilience has many organizational disciplines within its auspices, each of which brings value to the wider resilience picture, however, as the global organizational resilience standard ISO 22316:2017<sup>1</sup> makes clear, none of these disciplines are sufficient in their own right for establishing resilience. "There are established management disciplines that contribute towards resilience but, on their own, these disciplines are insufficient to safeguard an organization's resilience," states this global standard.

If an organization seeks to safeguard itself, an aspect of its operations or outputs, or its value to customers, stakeholders, markets, and others then proportionately investing in its resilience will help to achieve these goals. It can choose to focus on other protective disciplines, but it must do this on the understanding that that choice will ultimately limit how resilient it can be.

Resilience is a goal that can never be fully achieved; an organization can have more resilience (or less resilience even) through its choice of actions, processes, and protective measures, but resilience is always a journey rather than a destination that can be fully reached. This is because there is always more that can be done, more that can be achieved, and further lessons that can be learned from events. This is made clear in ISO 22316:2017<sup>2</sup>:

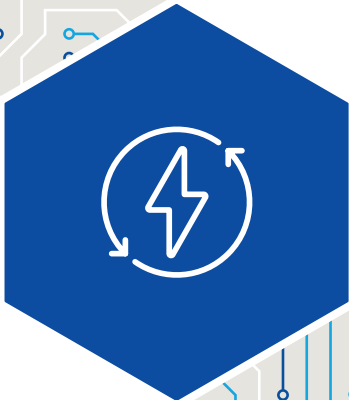
**"An organization's resilience is influenced by a unique interaction and combination of strategic and operational factors. Organizations can only be more or less resilient; there is no absolute measure or definitive goal."**

**Adaptability to change:** resilient organizations are better equipped to adapt to market changes, technological advancements, and evolving customer preferences. This adaptability offers competitive advantage, allowing the resilient organization to seize the new opportunities that arise during challenging times.



**Financial stability:** resilience fosters financial stability, which in-turn allows organizations to invest in new opportunities, even during economic downturns. Access to capital and a strong balance sheet enable companies to take calculated risks and pursue strategic initiatives that less resilient competitors might not be able to take advantage of.

**Regulatory and compliance benefits:** resilient companies are often better at navigating regulatory changes and compliance issues, again through their ability to adapt. As well as protecting against regulatory risks, staying ahead of these changes can provide early-mover advantages and access to – or even the creation of – new markets.



**The ability to continue operating when others can't:** during times of crisis resilient organizations have the ability to respond and recover quickly, whereas competitors may struggle to do so. This not only enables the resilient organization to maintain its revenue, retain its customers, and enhance its reputation, it also provides opportunities to gain new customers from struggling competitors.



**Marketing advantages:** a reputation for reliability and dependability can be a significant differentiator in competitive markets. This is something that can be used in marketing campaigns to help retain existing customers and acquire new ones.

**Risk management:** resilient organizations rely on robust risk management strategies, which not only protect against losses but also can identify potential opportunities within risks. For example, understanding supply chain vulnerabilities might lead to the discovery of more efficient or cost-effective alternative supply chain solutions.



**Protecting shareholder value:** research by PwC and Oxford Metrica<sup>3</sup> showed that, after a crisis, organizations that were perceived to manage the crisis badly saw their shareholder value fall: 250 days after the crisis the shareholder value of such organizations had decreased by 15% on average. Conversely, organizations that had been seen to manage the crisis well had gained an average of 10% in shareholder value after 250 days. The research, which examined 45 major corporate crises since the financial crisis of 2008, provides clear evidence that resilient organizations not only out-perform less resilient competitors after a crisis, they also emerge in a stronger position than pre-crisis when it comes to shareholder value.

## Taking the lead on resilience

Following Part One, which focusses on the Core Principles of resilience, Part Two of this document explores how to use the Core Principles in practice, presenting the Resilience Framework Cycle. This provides a practical basis for developing and managing resilience within a business and organizational setting. Central to this is the premise that resilience is led by an organization's top leadership. The format of what constitutes 'top leadership' may differ depending on organizational size, setting, and culture but, however it is structured, it is the role of those at the apex of the organization to lead the development and management of resilience. Resilience is, at its heart, a strategic discipline; and organizational strategy is led from the top. This is the first of the Core Principles and may be the initial change that an organization needs to consider.



## The Definition of Resilience

The definition of resilience chosen for the Resilience Framework is focussed on organizations, businesses, and their processes. As such it deals with:

### The ability to deliver outcomes...

This is the start of the chosen definition and has two core aspects:

- **Resilience is the ability...** ability is a capacity to perform a certain task, activity, or function. Abilities can be innate, learned, developed, or improved. Abilities are not static and can increase or decrease over time depending on the attention given to that ability.
- **To deliver outcomes...** this means to achieve goals or purposes as a result of actions taken or efforts made, or to have a desired impact or effect. In organizational terms, outcomes are the changes, benefits, or effects that occur because of the completion of objectives or as a result of achieving an organization's ongoing purpose. Any organization, business, or subset of these, is focused on delivering outcomes. Outcomes are the *raison d'être* for organizational existence.

### ...through uncertainty, disruption, and change

- Resilience enables an organization to continue to provide its desired outcomes despite disruption to its normal operating regime, however disruption is not the only situation where resilience is important. It also enables an organization to continue to deliver its outcomes in times of uncertainty and change. Organizational uncertainty occurs when there is a lack of predictability or clarity within an organization regarding various aspects of its operations, environment, or future direction. This is often due to changing external circumstances, for example in the organization's market conditions, regulatory environment, competitive landscape, and geopolitical, economic, or technological environment. Uncertainty can also occur as a result of internal changes, such as corporate ownership changes, mergers, and top leadership changes.

**From the above our full definition is:**  
**Resilience is the ability to deliver outcomes through uncertainty, disruption, and change.**

This is very similar to the definition of organizational resilience decided upon by the UK Government in its recently published organizational resilience guidance<sup>4</sup>. **This defines organizational resilience as the ability of an organisation to achieve intended outcomes through uncertainty, disruption and change.**

## Resilience or resiliency?

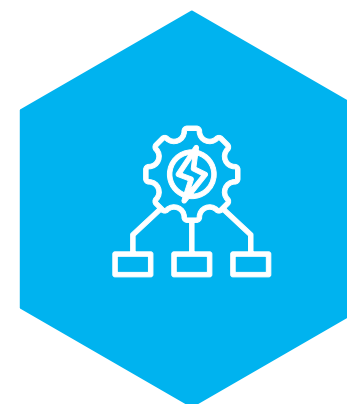
One of the initial considerations of the Technical Advisory Group was whether to use the term 'resilience' or 'resiliency' and whether there are any differences between the two terms. The conclusion was that the group felt that both are two forms of the same word, with resilience being more commonly used in British English and resiliency more frequently used in American English. This thinking is supported by various dictionaries and grammar resources. As an example:

Resilience and resiliency are different forms of the same word. But in today's English, resilience is far more common than resiliency, notably outside of the U.S. and Canada. In North American publications, resilience appears about four times as often as resiliency. Outside North America, resiliency appears only rarely<sup>5</sup>.

In the Resilience Framework resilience will be used throughout the text, but on the understanding that this can be used interchangeably with resiliency.

# Part One: The Core Principles of Resilience Development and Management

Core Principles are fundamental values or aspects that guide decision-making and actions in a specific area: they are the baseline requirements. The following section sets out eight Core Principles for developing and managing resilience within businesses and organizations. As explained in the introduction, above, the Core Principles, in combination, define the essence of what highly resilient organizations do, have, and are able to demonstrate.



## Core Principle One: Resilience is Led from the Top

Resilience development and management needs to be led by the organization's top leadership, whatever this constitutes for the organization in question. This could be the executive, the board in a larger organization, an individual director in a small organization, trustees in a charity, or political leaders in a public organization.

Developed and demonstrable resilience capabilities are an enabler of organizational success, underpin operational agility, assure stakeholders, and help grow the organization's reputation as a responsible organization. Irrespective of an organization's size, sector, or structure, the most senior leader(s) accountable for the success of the organization's mission should recognise resilience as a specific strategic objective and should define associated strategies and policies to develop, establish, and maintain activities and skills which achieve proportionate, pragmatic, and effective resilience capabilities.

Developing and maintaining resilience is a key factor in both an organization's long-term sustainability and its short-term ability to successfully achieve its current aims: as such, it is a strategic objective and therefore needs to be directed, owned, driven, motivated, energised, and resourced by the organization's strategic leaders.

Resilience is led by the top leadership because they establish the direction of the organization and own and set the organization's appetite for risk and resilience, which in turn is the basis for all investment decisions in these areas.

While some organizations will decide to place responsibility for resilience leadership with an individual — whether a dedicated c-level executive, such as a chief resilience officer (CRO), or as part of the role of a specific c-level executive — it is important to recognise that responsibility for resilience sits with the whole of the organization's top leadership. All c-level executives share the common goal of driving the organization's success and ensuring its long-term sustainability, therefore they are all accountable for the organization being resilient. Resilience is also a governance requirement and therefore is a collective responsibility, which includes the board as well as the c-suite.

One key word in this Core Principle is led: resilience is led from the top. Organizations operate at three levels — strategic, tactical, and operational: and the top leadership are responsible for the strategic level decision making. Tactical and operational aspects of resilience development and management are carried out at other levels within the organization and its partners; but top leadership sets the direction for these areas and maintains overall responsibility.



Organizational culture

Top leadership also plays a key role in setting and modelling the organization’s culture.

Organizational culture refers to the shared values, beliefs, attitudes, and standards that shape the way that individuals within an organization interact with each other and with customers, suppliers, and other external stakeholders. The approach and attitude to resilience is a vital part of organizational culture. Where resilience is seen as an important part of organizational culture then members of the organization are more likely to play their part in the tactical and operational development and management of resilience. Values reflect what the organization considers important and can influence priorities and actions. Where the organization clearly values resilience, it will be given the attention it requires by teams and individuals. Top leadership has a crucial role to play in shaping culture and, therefore, the resilience aspects of this. Being an advocate for resilience and a role model for what it means to take resilience seriously are vital parts of top leadership’s role. Top leadership must demonstrate, model, and drive behaviours that contribute to resilience.

Regulatory requirements

As well as being best practice, it is also mandatory in some sectors - particularly those in the financial and banking sectors - for top leadership to take responsibility for and provide direction for resilience. For example, The Board of Governors of the U.S. Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency<sup>6</sup> require the board to work “with senior management to confirm that operational resilience practices are led and staffed by individuals with relevant expertise, approve appropriate budgets and resources, and [to] promote a culture of effective risk management.” These agencies are also clear that, in terms of operational resilience, a regulated firm’s board of directors “oversees the firm’s management of operational risk in its business line operations, its independent operational risk management function, and its independent internal (or external) audit function. Senior management is accountable for ensuring that each of these areas adheres to the firm’s tolerance for disruption,” and “Senior management is accountable for developing, implementing, and managing effective and resilient information systems and controls, as appropriate, to maintain critical operations and core business lines consistent with the firm’s tolerance for disruption.”

The role of top leadership in resilience is echoed by the UK’s financial regulators. The Financial Conduct Authority<sup>7</sup> states in no uncertain terms that when it comes to operational resilience “senior management is accountable for their firm’s operational resilience.”

Additionally, the Basel Committee on Banking Supervision<sup>8</sup> states that when it comes to operational resilience the board has a requirement to “review and approve the bank’s operational resilience approach,” while senior management “should implement the bank’s operational resilience approach...”

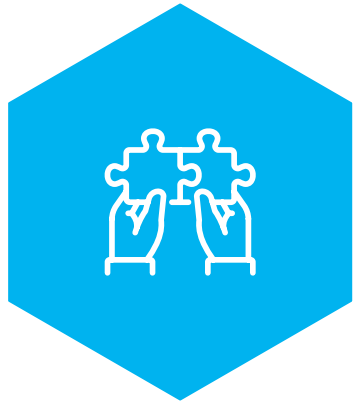
How this Core Principle links to current standards

**ISO 22316:2017<sup>9</sup>**  
ISO 22316 states that to develop organizational resilience the organization should take a coordinated approach that provides a mandate to ensure its leaders and top management are committed to enhance organizational resilience and appropriate governance structures to achieve the effective coordination of organizational resilience activities.

**BS 65000: 2022<sup>10</sup>**  
BS 65000 states that organizations need to build a framework of governance and accountability for organizational resilience. The standard also includes nine areas where top leadership and the board should be involved in the governance of resilience.

**ASIS ORM.1-2017<sup>11</sup>**  
The whole of the ASIS International Security and Resilience in Organizations and Their Supply Chains American National Standard is predicated on top management leadership of the development and ongoing maintenance and review of an organizational resilience management system (ORMS).





## Core Principle Two: Clear Direction on Purpose, Objectives, and Required Outcomes

Core Principle Two flows from Core Principle One, since it is the responsibility of the organization's top leadership. Resilience development and management requires clear direction on purpose, objectives, and required outcomes; and this direction needs to be provided by top leadership, who have the overall responsibility for organizational strategy.

In order for resilience to be developed, the purpose, objectives, and required outcomes all need to be established and directed by top leadership. This is because top leadership:

- Sets the overall direction, vision, purpose, and goals for the organization. Top leadership has the overall view of and responsibility for the organization's direction, vision, purpose, and goals therefore it is in the best position to understand and determine where and how resilience fits into the overall organizational picture.
- Sets the budgets and resources. Resilience development and management needs financial, human, and technological resources at appropriate levels to achieve the resilience strategies set by the top leadership. The resourcing level needs to be established by top leadership, as they have the overall responsibility for balancing resourcing across the organization.

- Has appropriate authority and decision-making power. Top leadership has the authority and decision-making power to make significant strategic choices and commitments on behalf of the organization. They can make the appropriate strategic decisions for resilience development and management and delegate or devolve to the people and units that are empowered to make the necessary operational decisions. Top management can also require and ensure that appropriate organizational departments and teams work together to achieve resilience requirements.

As stated above, top leadership needs to give clear guidance on resilience purpose, objectives, and required outcomes. These are as follows:

**Purpose:** purpose addresses the question of "Why are we doing resilience?" But in the context of the wider organizational purpose. The latter is the fundamental reason(s) for an organization's existence. This will be different from organization to organization, but a clear organizational purpose serves as a guiding light, or a North Star, which informs and leads the organization's goals, strategies, decision-making, and culture. Resilience supports the organization's purpose but also the organization's purpose guides the organization's strategic resilience choices, appetite, and investment.



Purpose can change over time so must be regularly assessed; and resilience strategies, processes, solutions, and arrangements need to be adjusted, adapted, and re-worked accordingly and in a timely manner. Purpose can change slowly or rapidly; and resilience must also be capable of responding to dynamic as well as incremental change.

### Objectives

Like any organizational area, resilience requires the setting of clear objectives to give direction to resilience development. Clear objectives help organizations to focus effort, align activities amongst different teams and departments, measure progress, make informed decisions, and set appropriate budget and resource levels. Purpose provides the vision, while objectives provide a roadmap for getting there.

### Required outcomes

Having clear outcomes for a resilience development programme is important and is linked to the objectives that are set. Outcomes are the output of objectives; they are the aims of the resilience development programme and are what will be measured in terms of key performance indicators (KPIs) for resilience development.

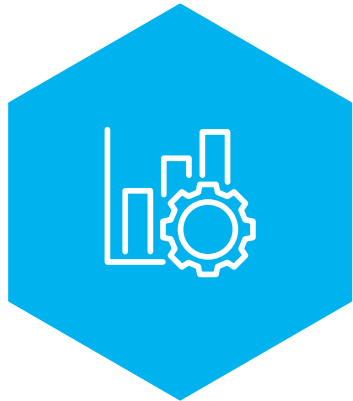
The above three areas are all linked: organizational purpose informs the resilience objectives, which provide the resilience outcomes. Each are established, directed, and governed by top leadership. All three areas need to be periodically assessed, as well as being reviewed whenever a material change is made or happens to the organization.

**How this Core Principle links to current standards**

**ISO 22316:2017<sup>12</sup>**  
ISO 22316 states that: "Organizational resilience is enhanced by a clearly articulated and understood purpose, vision and values to provide clarity to decision making at all levels of the organization."

**BS 65000: 2022<sup>13</sup>**  
BS 65000 states that "top management should demonstrate leadership and commitment with respect to organizational resilience by, amongst other things, establishing and maintaining processes that enable organizational resilience to achieve its intended outcome(s)."

**ASIS ORM.1-2017<sup>14</sup>**  
An organizational resilience management system needs to be 'Outcomes Oriented' according to ORM.1-2017.



**Core Principle Three:**  
**Requires a Comprehensive Understanding**  
**of the Organization's Current State**

Resilience is contextually dependent. To develop resilience you need to understand where you are starting from: what the business or organization does, how it is structured, what its products and services are, who its stakeholders are, and how its supply and value chains are structured. A complete and clear picture of the business or organization is essential.

As well as the details of the fundamental structure of the organization, clarity will be needed on:

**The current and inherent levels of resilience**

Every business or organization will have some inherent or intrinsic capability for resilience. Even in an organization that has never carried out any formal risk management, business continuity, information security, or other protective activities, some resilience will be in place and, however basic this might be, it can often be built upon. Many fundamental business activities play a role in resilience even if this is not recognised as such. For example, environmental management, financial control, health and safety, human resources, quality management, and strategic planning are among the common business areas that ISO 22316 recognises as contributing to organizational resilience<sup>15</sup>.

External requirements: most organizations and businesses have resilience requirements placed upon them, even if the term itself isn't used for these. For example, as highlighted above, health and safety is an area which contributes to organizational resilience and, in most countries, businesses have clear rules and regulations to follow in this area. Some organizations, particularly in the financial sector, will have strong expectations from regulators in terms of what is required in areas such as operational resilience, business continuity, or risk management. The external requirements need to be considered and built into the resilience management programme.

The social and economic environment in which the organization operates: no organization operates in an individual bubble. It is affected by its wider social and economic environment; and this impacts on the organization's resilience. This includes areas such as:

- **Social factors:** the demographics, cultural norms, social trends, and values prevailing in the society / societies where the organization operates.
- **Cultural and ethical factors:** organizations exist within diverse cultural landscapes and may have differing ethical expectations in their operations and interactions with stakeholders.

- **Environmental factors:** sustainability, climate change, and environmental degradation challenges and regulations will have an impact on resilience.
- **Economic factors:** economic conditions such as inflation rates, interest rates, exchange rates, GDP growth, unemployment levels, and overall market stability profoundly affect an organization's financial health and overall resilience.

Understanding the current state of the organization, the external and environmental factors impacting upon it, and its existing levels of resilience, provides the starting point for considering what additional activities are required to achieve the desired resilience outcomes. This gives a roadmap of existing good practices and capabilities that can be built upon or expanded; and it also provides clarity on existing silos that need breaking down.

**How this Core Principle links to current standards**

- ISO 22316:2017<sup>16</sup>**  
Organizational resilience "relies upon an up-to-date understanding of an organization's context," according to ISO 22316. This includes the organization's internal and external environments.
- BS 65000: 2022<sup>17</sup>**  
According to BS 65000 organizational resilience requires a consideration of the organization's role in the wider context in which it operates.
- ASIS ORM.1-2017<sup>18</sup>**  
ORM.1-2017 recognises "that organizations do not operate in isolation but rather as part of a complex and interconnected ecosystem." The ORMS is built taking into account the context of the organization and its supply chain.





## Core Principle Four: Take a Risk-based Approach

Resilience in a business and organizational context is risk-based. Organizations need to understand what they need to be resilient against and that requires an understanding of the risk environment. This will drive the priorities, the strategies, and the resilience decision-making.

Resilience is a holistic capability, with the prevention and mitigation of risks being at least as important as responding to the impacts of events and incidents.

### Risk-based

Risk-based refers to any approach or methodology where decisions, actions, or processes are guided by an assessment of potential risks and their impacts. Instead of applying uniform measures or treatments across all scenarios or impactful possibilities, a risk-based approach prioritises resources, actions, and attention based on the likelihood and severity of identified risks and their anticipated impacts.

Risk-based also means that every aspect of resilience development and management is influenced by an assessment, understanding, and response to risks. These could be systemic risks, which are identified in a formal risk assessment, or they could be situational risks, which are assessed dynamically as an incident or event unfolds.

An organizational or enterprise risk management approach is at the heart of developing and managing resilience.

**According to the ISO 31000 standard<sup>19</sup> the risk management approach should be:**

- Integrated into all organizational activities.
- Structured and comprehensive.
- Customized and proportionate to the organization's external and internal context and related to its objectives.
- Inclusive: it includes appropriate and timely involvement of stakeholders.
- Dynamic: it anticipates, detects, acknowledges and responds to changes and events in an appropriate and timely manner.
- Based on the best available information.
- Influenced by human and cultural factors.
- Continually improved through learning and experience.

It includes a structured risk assessment approach that includes a three stage process of Risk Identification, Risk Analysis, and Risk Evaluation. This is followed by Risk Treatment<sup>20</sup>.

Risk management is also a forward looking discipline, ensuring that the organization conducts horizon scanning to understand how risks are developing and changing; and to identify new and emerging risks that need to be monitored.

In terms of the dynamic risks that emerge during incidents and crises, ISO 22361 explains that these should be managed via situational and risk awareness, actively monitoring the internal and external environments and assessing potential vulnerabilities and opportunities<sup>21</sup>.

As can be seen from the above, risk awareness and management are both fundamental aspects of resilience in an organizational and business context. Having a clear understanding of the internal and external sources of risk - and how risk is captured, managed, and communicated - are critical factors in determining and developing resilience capabilities. Risk management processes assist in controlling the development of proportionate and necessary activities to achieve resilience.

Understanding risks leads to one of three decisions: either to remove them, by a change in direction or strategy; mitigate them, in other words to implement measures that result in a reduction of the risk; or to accept them and allow the organization to 'live with them'. The first two decisions involve resilience activities and show how intrinsically and inextricably linked risk and resilience are.

### Beyond risk management

While risk management is an important aspect of resilience, it does not provide a complete picture for resilience management. Risk management can't drive everything: there are unknown issues that can't be planned for but, for which, resilience measures can help an organization respond. Here is where impact-based planning and crisis management come into their own. If an organization understands what happens if a particular process stops or reduces in activity, then it doesn't actually matter what causes that disruption.

Whether the disruption is caused by a known risk or an unknown risk, the impact will be the same in terms of the outcomes of, or outputs from, that process. Resilience management looks to understand the impacts of disruption, for example through the use of the business impact analysis technique, which is central to business continuity management, as well as the causes of disruption through risk management. The former ensures that the organization is 'ready for anything' and can respond effectively when the unexpected and unanticipated happens; while the latter ensures that the organization is strategically protected against the knowable threat landscape.

### Risk and resilience appetite

Risk appetite is a key aspect of risk management and refers to the level of risk or uncertainty that an organization is willing to accept or tolerate. It is about the risks to the organization that can be accepted, the risks that can be taken, and the general cultural approach to risk within the organization.

Risk appetite is a crucial concept for decision-making and strategic planning. It helps organizations determine the types and levels of risks that they are willing to undertake in order to achieve their objectives, while also considering factors such as financial stability, regulatory compliance, and stakeholder expectations.

Organizations with a high risk appetite will be willing to take on greater risks in pursuit of high outcomes, returns, or growth opportunities, while others may have a lower, more conservative, risk appetite, preferring to minimise risk even if it means potentially lower outcomes.

Establishing and understanding risk appetite is essential for effective risk management, as it helps organizations align their risk-taking activities with their overall strategic objectives and ensure that risks are managed within acceptable limits.

While risk appetite is at the heart of risk management activities, so the concept of resilience appetite needs to be central to overall resilience development and management.

Similarly to risk appetite, resilience appetite involves an analysis of how important resilience is to the organization in question. The resilience appetite will drive the time, effort, and resources given to resilience; and will determine the strategies and tactics that are chosen. It will also drive cultural change programmes.

Conversely to risk appetite, organizations with a high resilience appetite will make greater investments in resilience than those with low resilience appetites.

Resilience appetite is about an organization knowing what levels of resilience it wants to aim for, based on its overall vision, goals, culture, and purpose. Being clear about resilience appetite also protects the organization from over-spending on resilience. Protecting a system more than is necessary, or more than is economically prudent, should not happen when an organization has clarity on the levels of resilience that are appropriate; and resilience appetite is an important aspect of that equation. Being over-resilient is a risk in its own right as it can effectively suffocate the organization in terms of its fundamental purpose. It can also make the organization less commercially agile.

Resilience appetite needs to be clarified and set by top leadership, determining, as part of the process, which areas of the organization and its processes are priorities for resilience arrangements and strategies.

Culture has an important role to play in resilience appetite, both helping to inform resilience appetite and, in turn, being influenced by it. An organizational culture can be more or less resilient, depending on how focussed the organization's workforce is on resilience, how attitudes in the wider cultural setting of the organization affect the organization's own culture, and how recruiting practices include attributes that are pro-resilience.

Tolerance

Risk and resilience appetite both feed into the concept of tolerance.

In its risk management context, tolerance refers to the degree or extent of risk that an organization is willing to accept or bear before action is deemed necessary to reduce it. It represents a threshold of acceptable risk, beyond which risk response measures must be enacted to bring the risk level back within acceptable limits.

In terms of organizational impacts, impact tolerance refers to the maximum level of disruption or damage a system, organization, or process can accept without suffering unacceptable consequences.

Tolerance in both the above contexts is dependent in part on an understanding of risk and resilience appetite. Put simply, an organization with a high resilience appetite will have a low impact tolerance and will need to invest more in resilience than an organization with a low resilience appetite and therefore high impact tolerance.

Justification from formal standards for this Core Principle

**ISO 22316:2017<sup>22</sup>**  
ISO 22216 is very clear about the reliance of resilience on risk management. In the Principles section it states that: "An organization's resilience... relies upon effectively managing risk."

**BS 65000: 2022<sup>23</sup>**  
Section 5.7 'Governance for resilience' sets out the view of BS 65000 when it comes to risk management: "Organizational resilience should be a core component of an organization's strategy and business model and embedded in its risk management approach," states the standard.

**ASIS ORM.1-2017<sup>24</sup>**  
The ASIS ORM.1-2017 standard places 'proactive risk management' as central to building a resilience capacity.





## Core Principle Five: Resilience is Coherent and Collaborative

Resilience needs to be developed and managed in a coherent and collaborative way. These two things are closely linked, with collaboration being key to coherence.

### Coherent

In an organizational context, 'coherent' is the quality of being structured, logical, consistent, and aligned across the whole organization. Goals, strategies, policies, and actions related to resilience will be coordinated holistically.

Coherence involves breaking down organizational silos and enabling collaborative working. This will allow consistent and joined-up working across functional, organizational, and geographical boundaries. It will also ensure that duplication is avoided and that resources for resilience are governed, managed, prioritised, coordinated, controlled, and resourced efficiently.

### Collaborative

Collaboration is a process by which individuals across an organization work together towards a common goal or project: in this case, resilience. Collaboration in an organizational context includes:

- **Shared goals and objectives:** collaboration starts with a clear understanding of what the team is trying to achieve. These goals should be aligned with the organization's overall objectives and communicated effectively to everyone involved.

- **Diversity of skills and perspectives:** effective collaboration usually brings diverse skills, experiences, and perspectives together, which can lead to more innovative solutions and a more comprehensive approach to problem-solving.
- **Open, transparent, and effective communication:** good communication is crucial for collaboration. This includes not just verbal and written communication but also listening skills.
- **Trust and respect: trust is foundational for collaboration.** People need to feel confident in each other's skills, abilities, and commitment. Mutual respect ensures that all voices are heard and valued, even when there are disagreements.
- **Clear roles and responsibilities:** clearly defined roles and responsibilities help streamline the collaborative process.
- **Leadership:** effective leadership is crucial for fostering a collaborative environment. Leaders should encourage team participation, facilitate communication, provide the necessary resources, and recognise and celebrate achievements.
- **Conflict resolution:** conflicts are inevitable in any collaborative effort. Effective conflict resolution strategies that focus on finding common ground and addressing the root causes of disagreements are essential.

- **Feedback loops and continuous improvement:** collaboration needs a commitment to continuous improvement. Teams should regularly reflect on their processes and outcomes to identify areas for enhancement.

### Collaboration with an organization's value chain

Collaboration also extends outside the organization itself. No organization is an island: resilience is systemic and an individual organization's resilience strategies and arrangements need to consider the wider ecosystem within which the organization exists. This systems approach will include entities and stakeholders that the organization is dependent on and that are dependent on it. The organization should make a conscious and meaningful contribution to the resilience of its wider network, as this will improve its own resilience.

A stakeholder is anything / anyone that has a stake in or a relationship with the organization: including employees, customers, regulators, markets, the general public, direct suppliers, and the wider supply and value chain.

### How this Core Principle links to current standards

#### ISO 22316:2017<sup>25</sup>

Coherence and collaboration are included in ISO 22316's General Principles: "An organization's resilience... is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise," states the standard.

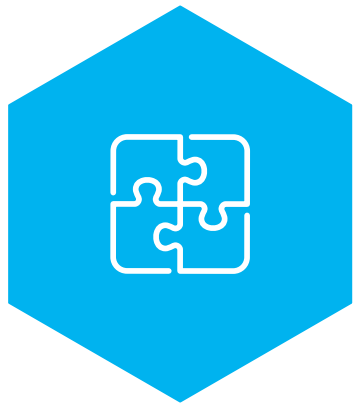
#### BS 65000: 2022<sup>26</sup>

BS 65000 also confirms the importance of coherence and collaboration, stating that: "Organizational resilience requires an enterprise-wide approach, including assets, processes, functions, units and geographies, and involves third parties and other stakeholders..."

This standard also explains the importance of looking beyond the organization itself, with resilience requiring a systems approach, highlighting that even collaboration with competitors may be necessary.

#### ASIS ORM.1-2017<sup>27</sup>

ANSI/ASIS ORM.1-2017 "provides a single integrated management system to eliminate 'siloing'." Coherence and collaboration are at the heart of this standard, with organizational resilience requiring "the convergence of risk disciplines as well as the elimination of and/or collaboration among organizational siloes..." Taking a systems approach is also essential for resilience: "The Standard recognizes that organizations do not operate in isolation but rather as part of a complex and interconnected ecosystem. It is not sufficient to manage just internal organizational risks, but it is essential for organizations to take a systems approach and understand the risk characteristics and interactions with individuals, organizations, the community and society."



**Core Principle Six:**  
**Incorporates a Defined Set of Strategies and Related Operational Solutions**

A resilience strategy outlines how an organization will achieve its long-term goals and objectives in a particular area. It serves as a roadmap, guiding the direction, allocation of resources, and decision-making processes, leading to the development of operational tactics to achieve the goals set out in the strategy. An organization needs an overall strategy for the governance of resilience, but each functional area of the organization, as well as its various processes and different important business services, will also require specific resilience strategies.

**Key components of a resilience strategy include:**

- **Anchored:** the strategy is anchored in the organization’s vision (a statement of what the organization aspires to become and achieve) and mission (a statement of the organization’s current purpose and primary objectives). These elements provide a clear direction and a sense of purpose.
- **Goals and objectives:** the strategy outlines specific, measurable goals and objectives that the organization aims to achieve within a defined timeframe. These goals are aligned with the mission and vision and serve as benchmarks for success.
- **Strategic initiatives:** these are the actions or projects that will be undertaken to achieve the set goals and objectives.
- **Resource allocation:** this involves determining how resources will be allocated to support the strategic initiatives. This includes budgeting and resource planning to ensure that initiatives are feasible and aligned with priorities.

- **Environmental analysis:** the resilience strategy needs to consider both the external environment (for example the regulatory landscape) and the internal environment (organizational culture, operational capabilities, and workforce skills) to ensure that the strategy is realistic and adaptable to change.
- **Performance metrics:** KPIs and other metrics need to be established to monitor progress towards achieving the strategic goals. Regular assessment and adjustment of the resilience strategy based on performance data are crucial for staying on track.

**Resilience strategies will include a set of planned operational and tactical solutions: these will enable the achievement of that strategy and its strategic initiatives. They will include:**

- **Defence and prevention:** stopping threats that might impact upon resilience from being realised. The ability to defend appropriately is necessary to protect the organization, to absorb and block threats, to defend against threats, to prevent things happening, to harden things to stop them breaking, and to provide the ability to failover.

- **Absorbing:** building a capability to be able to accept a certain amount of disruption. This involves the ability to endure adverse events by internally managing the impacts without significant external assistance or alteration in operations.
- **Response:** tactics that help the organization respond to crises, incidents, and events. Response is the active phase of incident management which takes place to enable business continuity through the incident and to minimise the impacts of the incident.
- **Recovery:** tactics that help the organization recover from crises, incidents, and events. Recovery takes place after the response phase to enable the organization to make a planned and managed return to a state of business as usual (BAU) if it deems this is appropriate. As pointed out in the next Core Principle, sometimes adapting to a new situation is more appropriate than returning to the previous BAU environment.

The available solutions for resilience development and management will be shaped via the capabilities, limitations, and tolerances determined by the disciplines contributing to the resilience programme. Some of the solutions will be additions made to existing operational processes, while others may be incorporated during a process, or infrastructure, design phase. The latter is often termed ‘resilience by design’.



Organizational solutions are often delivered as projects, which themselves may be grouped into programmes. Programmes enable a group of related projects to be managed in a coordinated manner. Programmes are by nature cyclical and use organizational learning methods to evolve, grow, and change.

There are no specific resilience strategies or solutions that are prescribed: they need to be developed by each individual organization, matching its resilience aims, policy, risk appetite, resilience appetite, threat landscape, resourcing, and ecosystem.

**How this Core Principle links to current standards**

**ISO 22316:2017<sup>28</sup>**  
In section 4.2 ISO 22316 says that “the organization should develop a coordinated approach that provides: [amongst other things] systems that support the effective implementation of organizational resilience activities; and arrangements to evaluate and enhance resilience in support of organizational requirements.”

**BS 65000: 2022<sup>29</sup>**  
BS 65000 says that organizations should: “develop an organizational resilience strategy that addresses four dimensions: readiness, responsiveness, recovery and renewal.”

**ASIS ORM.1-2017<sup>30</sup>**  
ASIS ORM.1-2017 is written around the ‘Plan Do Check Act’ cycle (PDCA): a four-step management method used for the control and continuous improvement of processes and products. In the Do aspect the standard says that various tactical solutions are needed for resilience.



## Core Principle Seven: Being Able to Adapt is a Characteristic of Resilience

The ability to adapt is a key element of resilience. In an organizational setting, during an incident or event, adaption involves situational awareness and the ability to assess, comprehend, and anticipate what is expected to happen next; adapting and developing organizational and resilience strategies and tactics accordingly. After an incident or event adaption includes understanding what happened, why it happened, what didn't happen that should have happened; and learning, reassessing, and changing as a result of this understanding.

Resilience is not necessarily about recovering to where an organization was before an incident or event, but it may be about strategically adapting during and post-incident to allow the organization to continue to provide the outcomes set by its top leadership. Organizations sometimes need to think about 'new normals', rather than returning to business-as-usual: this may even involve completely redeveloping and renewing the organization.

Resilience includes the capability to adapt, flex, or evolve in changing circumstances. This requires agility: being responsive to a set of circumstances that may change constantly. It means being able to change in a timely and appropriate way in response to challenges in the organizational environment and the impacts that arise from these challenges.

The capability to adapt is not a strategy or solution, instead it is an organizational skill and ability, which flows from and is led by top management.

Adaption is not always an appropriate response to an incident and event: some organizational areas are immutable; and others are desirable to retain. The decision to adapt rather than return to business as usual is a decision for top management to make.

### Justification from formal standards for this Core Principle

#### ISO 22316:2017<sup>31</sup>

ISO 22316 has the ability to adapt as central to organizational resilience.

#### BS 65000: 2022<sup>32</sup>

Similarly to ISO 22316, BS 65000 has the ability to adapt as central to resilience. In the introduction the remit of the standard is set out as considering both defensive and progressive dimensions, for continuity and adaptability.

#### ASIS ORM.1-2017<sup>33</sup>

ASIS ORM.1-2017 states that resilience is: "The absorptive and adaptive capacity of an organization in a complex and changing environment."



## Core Principle Eight: Is Always Cyclical

Resilience development and management is a learning cycle. Some methods to inform this cycle include:

- Testing and exercising to ascertain that the resilience strategies and solutions work as intended and then using the results and lessons identified to change, adapt, and improve the strategies and solutions.
- Debriefing, reviewing, and identifying lessons from incidents and events that occur and then changing, adapting, and improving the resilience strategies and solutions accordingly.
- Reviewing all aspects of the resilience development and management process across the whole organization and the baseline assumptions that sit behind this on a regular, planned, and consistent basis; and when a substantial organizational change takes place.
- Responding to changes in the risks faced by the organization or changes in the organization's environment.

The organizational learning cycle should be directed by top leadership, who will need to approve changes to the resilience strategies and solutions that arise from the process.

### Testing and exercising

The difference between testing and exercising, particularly in the context of resilience, lies in their scope, objectives, and methodologies. Both are essential to improving resilience capabilities.

Testing is more technical and specific in nature, aiming to evaluate the functionality, performance, and reliability of systems, processes, and procedures under challenging conditions. It is often quantitative, providing measurable results that indicate whether systems can meet predefined criteria for performance and resilience objectives.

#### Key characteristics of testing include:

- **Focus:** primarily on systems, technology, and specific processes.
- **Objectives:** to ensure that individual components, such as hardware, software, databases, and other technical resources, operate as expected under stress or failure conditions.
- **Methods:** include disaster recovery testing, penetration testing, load testing, stress testing, scenario testing, and other types of technical assessments.
- **Outcome:** identification of technical vulnerabilities; confirmation that impact tolerances can be achieved.

Exercising is broader and more holistic. It involves simulating scenarios and role-playing to assess the overall resilience of the organization, or specific business units. Exercising includes communication, coordination, and decision-making processes. Exercises are qualitative, focusing on training, awareness, and the effectiveness of strategies, solutions, plans, and teams rather than on technical specifications.



Key characteristics of exercising include:

- **Focus:** on people, strategies, solutions, plans, and procedures.
- **Objectives:** to validate the effectiveness of the resilience strategies.
- **Methods:** range from tabletop exercises, which are discussion-based, to full-scale exercises that simulate real-life emergencies as closely as possible.
- **Outcome:** identifies gaps in strategies, solutions, plans, and procedures; improves team coordination; and enables personnel to practice their resilience roles.

Debriefing, reviewing, and learning lessons from incidents and events

After action reviews (AAR) are a common approach in resilience. These are structured debriefs which take place after an incident or event and are used to analyse what happened, why it happened, and how things can be done better next time. They may result in fundamental changes to the resilience strategies and solutions if these did not perform as anticipated.

Key components of an after action review include:

- **What was supposed to happen:** the review begins with a clear statement of the objectives and what was expected to occur. This sets the stage for understanding the context and intentions behind the actions taken.
- **What actually happened:** participants discuss the actual outcomes, focusing on factual observations and data. This comparison between expected and actual results is crucial for identifying discrepancies and areas for improvement.
- **Why there was a difference:** the review group analyses the reasons behind the differences between expected outcomes and actual results. This involves identifying what went well, what didn't, and what contributed to these results.
- **What can be learned:** the most important part of the AAR is identifying the lessons that can be learned from the experience. This includes discussing what worked well and should be continued, what didn't work and needs to be changed, and how similar situations can be handled better in the future.
- **What should be done differently next time:** based on the lessons identified, the review concludes with specific recommendations for future actions. This may involve changes to processes, strategies, behaviours, or any other aspects that can improve future performance and outcomes.

Reviewing

There are many methods for conducting a review of organizational processes but a common one in the resilience area is the gap analysis.

Gap analysis is a strategic planning tool used to identify the difference between an organization's current state and its desired future state. It's essentially about understanding where an organization is now, where it wants to be, and what needs to be done to bridge the gap between these two states. This analysis helps in pinpointing specific areas that need improvement and in developing action plans to address these gaps.

The process of gap analysis typically involves:

- **Assessing the current state.**
- **Defining the desired future state.**
- **Analysing the gap:** with a clear understanding of both the current and desired states, the organization can identify the gaps between these two. This involves analysing the differences in performance levels, capabilities, processes, and resources. The gap analysis can highlight areas of underperformance, inefficiencies, and other obstacles that are preventing the organization from achieving its resilience objectives.
- **Developing action plans** based on the findings from the gap analysis.
- **Implementing and monitoring the action plans:** organizations should establish KPIs and metrics to measure progress and make adjustments as necessary to ensure that the actions taken are effective in closing the gaps.

How this Core Principle links to current standards

ISO 22316:2017<sup>34</sup>

ISO 22316 includes clear direction on how top management should carry out a periodic review "to ensure the organization's resilience continues to meet expectations."

BS 65000: 2022<sup>35</sup>

BS 65000 includes a sub-section on 'Organizational learning'. This states that organizations should use hindsight to learn from experience and includes nine methods of doing so. The standard also contains a full section on 'Management review', which says that top management should review the organization's resilience, at planned intervals.

ASIS ORM.1-2017<sup>36</sup>

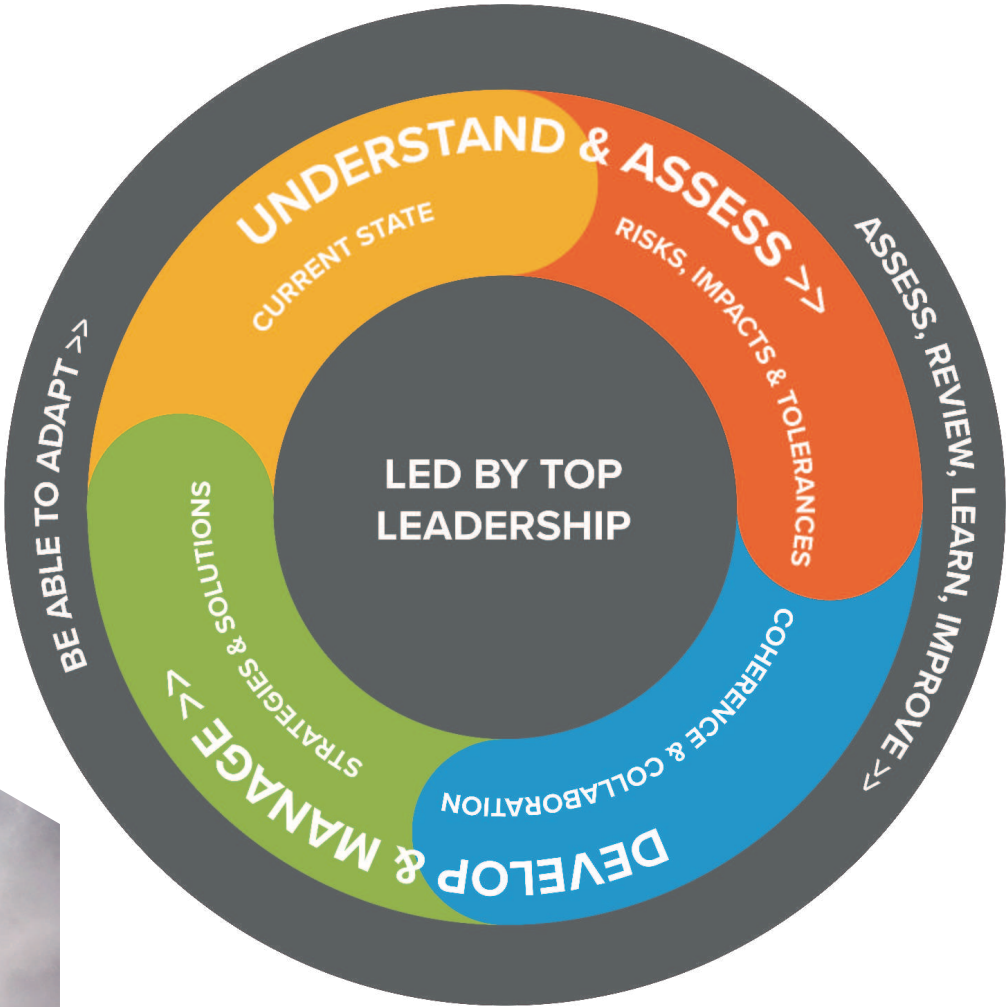
ASIS ORM.1-2017 covers review and improvement processes in some detail in various sections.

# Part Two: Using the Core Principles

A framework for developing and managing resilience within a business and organizational setting

The following Resilience Framework Cycle shows one method in which organizations and businesses can use the above Core Principles in a structured way to develop or improve a resilience programme.

## The Resilience Framework Cycle



## The Resilience Framework Cycle is structured in the following way:

### Centred on 'Led by Top Leadership'

The centrality of the role that top leadership plays in the resilience development and management cycle is emphasised by its place in the centre of the Resilience Framework Cycle. Whatever the size, structure, or type of organization, resilience development and management is led by the organization's top leadership. Organizations need to determine from the outset how this requirement will be translated, who amongst the top leadership group will take the lead, and how other members will govern, monitor, measure, and challenge the resilience programme. Top leadership is central to the development and management of resilience and is involved throughout the whole framework cycle.

The resilience programme requires clear guidance on purpose, objectives, and required outcomes and this is the responsibility of top leadership to establish, direct, and govern. This is a continual and pivotal process hence the position of this principle in the middle of the Resilience Framework Cycle. All three areas also need to be periodically assessed; as well as being reviewed whenever a material change to the organization occurs.

### Understand and Assess: Current State

The first phase of the Resilience Framework Cycle is to assess and understand the current state of the organization: the mission, structure, products and services, stakeholders, and the supply and value chains. A comprehensive and clear picture of the business or organization is developed and, from here, a complete understanding can be built of the current levels of resilience and the existing resilience solutions that are in place. This provides a starting point for further development and can then lead to a roadmap of what can be built upon or expanded; and clarity on the silos that need addressing.

### Understand and Assess: Risks, Impacts & Tolerances

Once a clear picture of the current state of the organization has been developed it is then possible to fully assess the risks that the organization faces, the impact that these would have on the organization if realised or if processes experience downtime or disruption due to unanticipated causes, and the tolerance that the organization has for disruption. Various methodologies are available for use in analysing risk, impact, and tolerances and the choice of methods will be determined by top leadership.

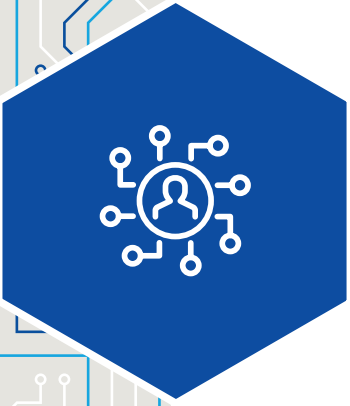
**Develop & Manage: Coherence & Collaboration**

After the Understand and Assess phase the Resilience Framework Cycle moves into the Develop & Manage phase. This commences with an organizational structuring or restructuring stage where coherence is developed and improved. This involves breaking down organizational silos and enabling the management and development of resilience to take place in a structured, consistent, and aligned way. This will enable effective collaboration on resilience to take place across the organization.



**Develop & Manage: Strategies & Solutions**

In order to improve resilience the organization will need to implement a set of strategies and solutions to achieve this. These will be specific to the individual organization and business and the choice will be informed by the information gained in the Understand and Assess phase of the Resilience Framework Cycle.



**Be able to adapt**

The capability to adapt is not a strategy or solution, instead it is an organizational skill and ability, which flows from and is led by top management. It is used on a day-to-day basis to help the organization change and develop to ensure long-term sustainability and growth; and it is used in response to an incident or event to determine whether and how the organization needs to change or transform in order to be able to continue to deliver on outcomes during and after the challenging situation.

It is shown in the Resilience Framework Cycle as an intrinsic capability which encompasses and informs the whole resilience cycle.



**Assess, review, learn, improve**

Another intrinsic capability alongside that of developing the capability to adapt is that of being able to continually improve the organization's resilience through assessing, reviewing, and learning. There are many ways of achieving this and the appropriate methods will be determined by top management. Resilience is a cycle: assessing, reviewing, and learning create a feedback loop for resilience development and management, with a continual process of improvement taking place.

## Acknowledgements

The BCI would like to thank the Technical Advisory Group that developed the Core Principles of resilience and the associated definition of resilience. Participants included:

- **Paul Barker**,  
Business Continuity & Resilience Manager, Railpen
- **Rachael Elliott**,  
Knowledge Strategist, the BCI
- **Daren Evans CEng FIMechE**,  
ChPP RPP FAPM, MBCI, Operational Framework - Programme Manager, BAE Systems
- **Dr Robert MacFarlane OBE**,  
Deputy Director, Risk & Resilience, DWP and Head of UK Government BC Specialism
- **Dianne Stephens FBCI**,  
CBCP, Sr, Manager Enterprise Resilience, Globe Life

## Feedback

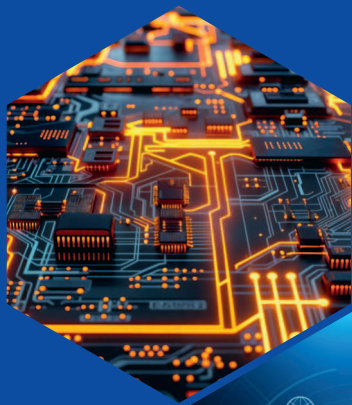
To provide feedback on anything within this document please contact the BCI Thought Leadership Team via the contact form at [thebci.org/about-bci/contact-us.html](https://thebci.org/about-bci/contact-us.html)

## Copyright

The Resilience Framework, the Core Principles, and the Resilience Framework Cycle are copyright © 2024, the BCI. All rights reserved.

## References

1. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, Introduction, p V
2. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, Introduction, p V
3. PwC and Oxford Metrica, Corporate Reputation in Crisis: The Impact on Shareholder Value, February 2020, accessed 7th August 2024, <https://www.oxfordmetrica.com/public/CMS/Files/1769/OxfordMetricaPwCReputation.pdf>
4. Cabinet Office, Organisational Resilience Guidance for UK Government Departments, Agencies and Arm's Length Bodies, August 2024, accessed 9th August 2024, <https://www.gov.uk/government/publications/organisational-resilience-guidance-for-uk-government-departments-agencies-and-arms-length-bodies>
5. Grammarist.com accessed 20th February 2024.
6. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (2020), SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience, p3
7. Financial Conduct Authority (2021), Building operational resilience: Feedback to CP19/32 and final rules, Policy Statement PS21/3, p30
8. Basel Committee on Banking Supervision (2021), Principles for Operational Resilience, p4
9. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, sections 4.2 and 5.2
10. BSI Standards Limited (2022), BS 65000: 2022 Organizational resilience - Code of practice, sections 4 a) 4, 5.1.2, 5.4, 5.5, 5.7
11. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, sections 4.2, 4.10, 6.1, 6.2
12. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, section 5.2
13. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, section 5.1.2
14. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, section 4.4
15. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, Annex A
16. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, sections 4.1 and 5.3
17. BSI Standards Limited (2022), BS 65000: 2022 Organizational resilience - Code of practice, introduction
18. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, introduction and section 5.2
19. ISO (2018), ISO 31000, Risk management - Guidelines, section 4
20. ISO (2018), ISO 31000, Risk management - Guidelines, introduction
21. ISO (2022), ISO 22361 Security and resilience - Crisis management — Guidelines, section 4.5.4
22. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, introduction and section 4.1 g
23. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, section 5.7
24. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, introduction.
25. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, sections 5.3, 5.8 and Annex A
26. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, introduction and section 5.1.1
27. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, introduction and section 0.1 General
28. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, section 4.2
29. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, sections 5.1.2 and 5.2.1
30. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, figure 1
31. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, introduction and sections 4.1 c, 5.7, 5.8 c, and 5.10
32. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, introduction
33. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, introduction
34. ISO (2017), ISO 22316 Security and resilience - Organizational resilience - Principles and attributes, section 6.3.2
35. BSI Standards Limited (2022), BS 65000 Organizational resilience - Code of practice, sections 5.5 and 7
36. ASIS International (2017), Security and Resilience in Organizations and Their Supply Chains - Requirements with Guidance, ASIS ORM.1-2017, an American National Standard, sections 4.11, 6.2, 10.4, 10.6.1, and 11.1



**BCI** 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK  
[bci@thebci.org](mailto:bci@thebci.org) / [www.thebci.org](http://www.thebci.org)



**bci** Leading the way  
to resilience

Find out more [www.thebci.org](http://www.thebci.org)