Whitepaper
Organisational Resilience Management

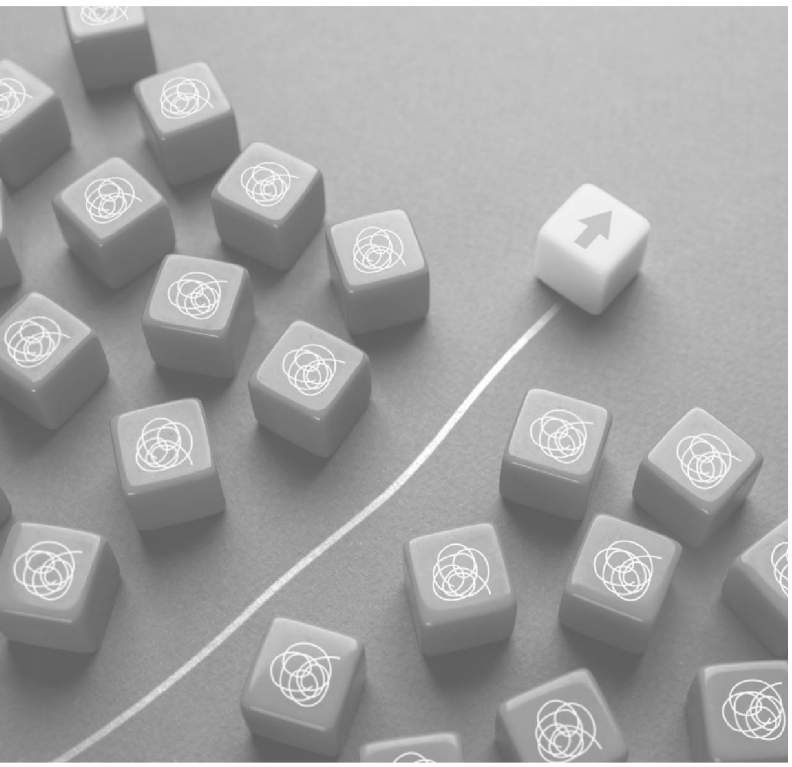
How to embed short-term stability and long-term adaptability in a dynamic overall strategy

controllit
Business Continuity Management

Contents

Introduction

Organisational Resilience Management (ORM) is an essential component of a future-proof corporate strategy. It enables organisations to not only prepare for regulatory requirements such as the Digital Operational Resilience Act (DORA), the Network and Information Security Directive 2 (NIS2) or the Critical Entities Resilience Directive (CER) , but also to effectively overcome unforeseen challenges.



While the aforementioned regulations primarily focus on operational resilience to ensure the resilience of critical functions (technical systems and processes), the decisive step goes beyond this: the development of organisational resilience. This aims to align the entire organisation – from culture to strategy to governance – towards long-term resilience.

Many companies have concepts for operational resilience in place, even if these are often not explicitly named as such. However, the necessary systemic integration of the individual management systems is often lacking in order to actually qualify as operational resilience. Extending this to the organisational level, however, represents a greater effort and requires a systematic approach.

This white paper presents the challenges and highlights the differences between operational and organisational resilience. It also introduces a holistic approach to implementing ORM. The aim is to combine short-term stability and long-term adaptability through a coordinated overall strategy and to treat this as a central task.

Context and initial situation

The current requirements, risks and challenges are complex and dynamic. The key challenges facing companies are outlined below:

- **Regulatory requirements** such as the Digital Operational Resilience Act (DORA), the Network and Information Security Directive 2 (NIS2) and the Critical Entities Resilience Directive require comprehensive measures. These regulations set clear framework conditions that oblige companies to adapt their processes to ensure resilience.
- **Technological risks** include cyber attacks that jeopardise sensitive data and business processes. Equally critical are system failures that can interrupt operations, as well as data-based disruptions such as manipulation or loss of important information.
- **Market dynamics, economic crises, technological disruptions, talent shortages and strategic misjudgements** can put companies in critical situations. These challenges lead to increased competitive pressure and impair organisations' ability to adapt effectively to new conditions.
- **Social and environmental challenges affect supply chain disruptions, resource scarcity and environmental disasters**, testing companies' ability to respond quickly and effectively. Companies must increasingly adapt to dynamic environmental conditions and social requirements.

Meeting these requirements, risks and challenges requires a strategic combination of operational and organisational resilience. Operational resilience stabilises critical functions, while organisational resilience ensures long-term adaptability. The combination of both approaches enables companies to respond flexibly and robustly to various challenges.

Differentiation: Operational vs. Organisational Resilience

Operational and Organisational Resilience are two different but complementary approaches that companies can use to strengthen their resilience.

A comparison:

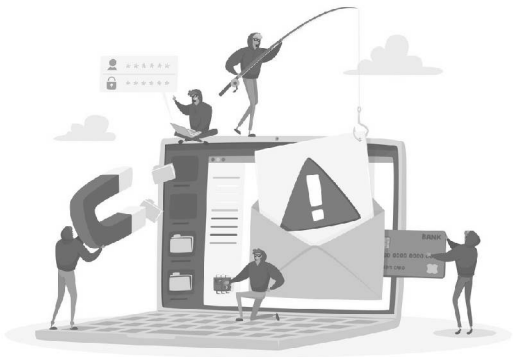
Criterion	Operational Resilience	Organisational Resilience
Time horizon	Short term: Stability and maintenance of critical functions during acute disruptions	Long term: Adaptability and strategic realignment over an extended period of time
Objectives	Minimisation of disruptions, restart, restoration and stabilisation of critical functions	Building long-term resilience, improving competitiveness and innovation
Focus	Processes, systems, technical infrastructure, physical security, personnel security	Corporate culture, governance, strategic leadership, communication
Relevant areas	Business continuity, crisis management, information security, physical security, security management, risk management, etc.	Strategic management, organisational development, innovation promotion, leadership, stakeholder management, etc.
Typical threats	Cyber attacks, natural disasters, technical failures, supply chain disruptions, business interruptions, etc.	Regulatory changes, market changes, social trends, etc.
Risks	Lack of availability of IT systems, staff shortages, physical damage to infrastructure, etc.	Strategic misalignment, lack of adaptability, communication deficits in times of crisis, etc.
Methods and models	Business impact analysis, protection needs assessment, gap analysis, threat analysis, fault tree analysis, etc.	SWOT analysis, PESTEL analysis, stakeholder identification analysis, scenario planning, etc.

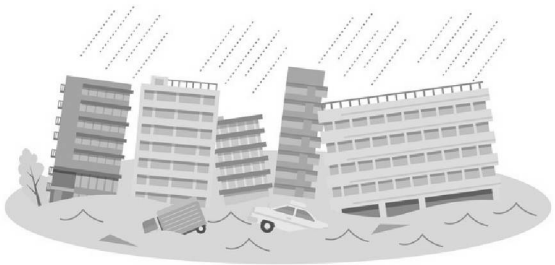
Differentiation: Operational vs. Organisational Resilience

Operational and Organisational Resilience explained using examples:

Supply chain disruption:
Operational Resilience ensures that alternative supply routes are established in the event of supply chain disruptions, while Organisational Resilience enables the development of strategic partnerships and flexible processes to respond to long-term market changes.

Cyber attacks:
Operational Resilience provides technical security measures such as firewalls and real-time monitoring in the event of cyber attacks, while Organisational Resilience includes training and communication strategies to minimise long-term risks.



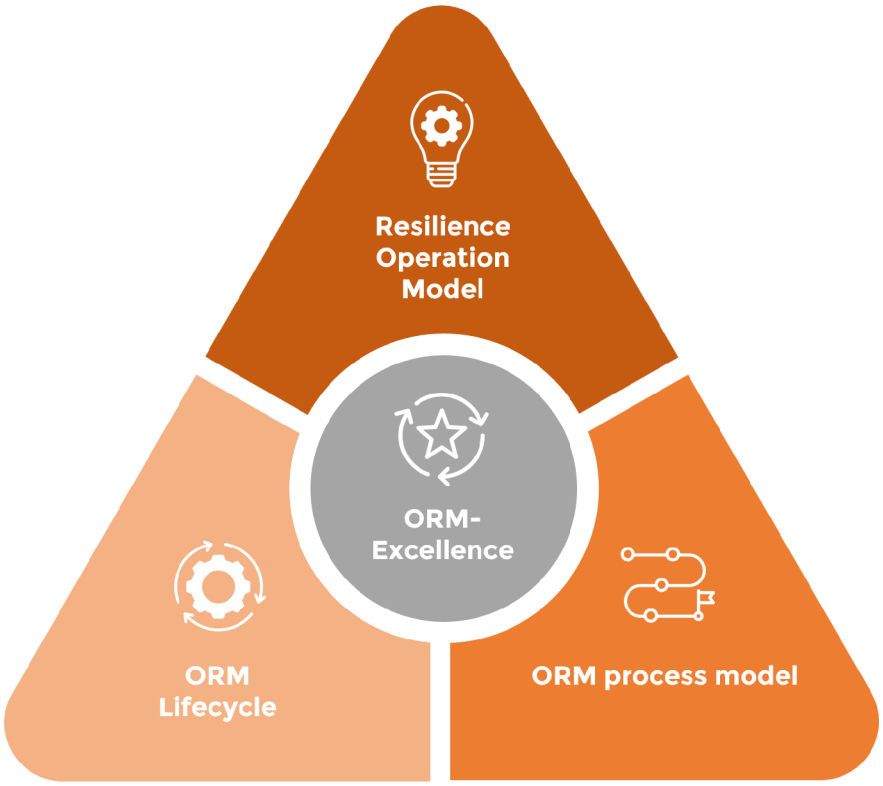


Natural disasters:
Operational Resilience includes protective measures such as evacuation plans and redundant locations in the event of natural disasters. Organisational Resilience focuses on long-term emergency plans and partnerships for resource provision.

Production downtime:
Operational Resilience ensures that redundant manufacturing sites can be activated in the event of production downtime, while Organisational Resilience enables long-term adaptation through strategic planning and investment in alternative markets.

The implementation of Organisational Resilience Management

To implement ORM, we recommend combining the Resilience Operation Model (ROM), the ORM process model and the ORM lifecycle.



The ROM represents the strategic vision and direction and remains the fundamental framework throughout all phases. The ORM process model, in turn, is used as a pragmatic guide for initial implementation to translate the strategies and goals of the ROM into operational reality. The ORM lifecycle begins after initial implementation for regular operations and involves a continuous process of review, adaptation and improvement, using the principles of the ROM as a guide.

The implementation of Organisational Resilience Management

Synergies illustrated by two examples:

	Strategie in action	Continuous improvement	Strategy adjustment
Cyber attacks	A company defines in its ROM that strengthening IT security is a key objective. The ORM process model puts this into practice by introducing an incident management system and training employees.	The measures from the ORM process model are regularly reviewed and further developed throughout the lifecycle to integrate new security standards and/or technological developments.	Findings from the lifecycle, for example on the effectiveness of certain measures, are incorporated into the further development of the strategic orientation of the ROM.
Technical disruption	The ROM provides the strategic basis for responding to technological disruptions such as new business models or competitors. Disruptive technologies require investment in research and the identification of new business areas.	The process model translates strategic guidelines into measures for operational preparation for technological disruptions. These include agile methods, innovation management and processes for the rapid integration of new technologies.	The lifecycle ensures flexibility and continuous adaptation to technological changes. Innovation workshops and market feedback help to identify and exploit new trends at an early stage.

Analyse the initial situation and set the course

Analysing the initial situation helps to systematically identify organisational weaknesses, external threats and strategic potential. These findings form the basis for targeted measures in ORM.

Analysis of the current situation

The analysis of the current situationis based on the ROM target model and is carried out using supplementary methods. The aim is to identify strengths, weaknesses and areas for action in a structured manner, which are then incorporated into the development plan.

Steps	Explanations
Define the framework and objectives	Definition of objectives, areas of analysis and stakeholders for the strategic orientation of the analysis
Data collection	Conduct interviews, workshops and technical document analysis
Analysis and evaluation	Application of the ROM target model for qualitative maturity assessment, supplemented by SWOT/PESTEL for environmental analysis
Derivation of the resilience strategy concept	Transfer to strategic target categories (protection, preservation and risk reduction) and fields of action
Development of an implementation plan	Prioritisation of fields of action, formulation of initial strategic and operational measures, and approval of investments

ROM Target Model: maturity analysis for Operational and Organisational Resilience

The ROM target model is a central strategic approach within ORM. This model systematically links the strategic guidelines of ROM with clearly defined resilience targets and operational implementation.

Key points of the ROM target model
The ROM target model forms the basis for deriving and managing resilience targets and continuously improving them. The following aspects are taken into account in particular:

- Link between ROM and target model: The ROM provides the strategic framework from which concrete resilience targets are derived and operationalised in the target model.
- Maturity assessment: continuous monitoring of the degree to which the defined goals have been achieved using suitable key performance indicators
- Strategic goal derivation: Derivation of measurable resilience goals that are systematically transferred to resilience controlling
- Control and optimisation: Regular review and adjustment of goals and measures to sustainably increase resilience

From the ROM target model to the resilience strategy concept
The ROM target model creates the basis for developing the resilience strategy concept. This concept translates the strategic targets into actionable measures and defines processes for operational implementation. Clear, measurable guidelines ensure that strategic targets are effectively implemented and continuously improved.

Implementation planning as the next step
Implementation planning specifies the measures of the resilience strategy concept and assigns clear responsibilities and priorities to them. Integration into resilience controlling enables transparent management, regular performance measurement and continuous optimisation based on reliable data and findings.

Conclusion

The effective implementation of ORM is based on the ability to systematically integrate strategic goals, operational measures and continuous adaptation. The ROM target model helps with strategic implementation.

Key Takeaways:

- Companies must address regulatory requirements and dynamic risks in equal measure. An integrated, forward-looking resilience strategy is crucial.
- Operational and Organisational Resilience complement each other. While one ensures short-term stability, the other creates long-term adaptability.
- A well-thought-out concept that ranges from strategic goals to implementation and continuous improvement is essential for a future-proof organisation.
- A structured analysis of the current situation and an implementation plan based on this enable a step-by-step, traceable increase in resilience.
- The ROM target model forms the basis for systematic target derivation, maturity assessment and control through Objectives and Key Results and Key Performance Indicators in resilience controlling.

The combination of strategy, implementation and continuous improvement is essential for making companies more resilient and giving them a sustainable competitive advantage. Resilience is not a static state, but an ongoing process that should be integrated into the DNA of every organisation.

Do you have any questions on this topic? Feel free to contact us!

Controllit AG
Kühnehöfe 20
22761 Hamburg
Germany
www.controll-it.de/en

Status: July 2025

Controllit AG is your partner for business continuity management (BCM). Since our foundation, we have been developing integrative concepts and products for business continuity management, IT service continuity management, information security management and crisis management. We help you to secure your business processes against threats and to provide for emergencies with strategic, organisational and technical concepts.

Photo/graphic credits: Titel: iStock.com/Yossakorn Kaewwannarat; S. 3: iStock.com/bagira22; S. 6: iStock.com/Veysel Celikdemir, iStock.com/lemono, iStock.com/morita kenjiro, iStock.com/SiberianArt; S. 8: iStock.com/z_wei; S. 9: iStock.com/VectorMine; S. 12: iStock.com/metamorworks