5.2.4

RESILIENCE: CRISIS PREPAREDNESS, BUSINESS CONTINUITY AND RECOVERY

Why resilience matters

Corporate resilience is the ability of a company to anticipate, prepare for, respond to and recover from significant disruptions while protecting its people, assets, operations, reputation and long-term value. Resilience is not limited to emergency response. It includes crisis preparedness, business continuity, disaster recovery, communication with stakeholders, and the ability to learn and adapt after disruption.

The importance of resilience has increased significantly in recent years due to geopolitical instability, cyber threats, pandemics, supply chain disruption, climate-related events, energy insecurity, regulatory change and social expectations. The G20/OECD Principles of Corporate Governance expressly include a chapter on **Sustainability and resilience**, and emphasise that Boards should consider material sustainability risks and opportunities when reviewing strategy, risk management and internal control systems.

For the Board, resilience is not an operational detail to be left entirely to management. It is part of the Board's responsibility for strategic guidance, effective monitoring of management, risk oversight and accountability to the company and its shareholders.

In the European Union, resilience's importance is increasing as a legal requirement as well as good practice. The NIS2 Directive on cybersecurity, the Digital Operational Resilience Act (DORA) for the financial sector and the Critical Entities Resilience Directive, as transposed in Estonia, Latvia and Lithuania, require many companies to manage their risks, maintain business continuity and report significant incidents, and in several cases place explicit responsibility on the management body. The Board should know which of these regimes apply to the company and how compliance is assured.[17]

What corporate resilience includes

Corporate resilience should be understood as an integrated governance framework and as a legal duty of the companies and their Boards covering four connected

17 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2); Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA); Directive (EU) 2022/2557 on the resilience of critical entities (CER).

areas, supported by crisis communication and by learning from every incident, both of which are addressed below:

Crisis preparedness means the company's readiness to identify, assess and prepare for serious events that may threaten its operations, people, financial position, licence to operate or reputation.

Emergency response means the immediate actions taken when an incident occurs, including protection of life and health, mitigation of damage, activation of crisis teams, internal escalation and communication with relevant authorities and stakeholders.

Business continuity means the ability of the company to continue its most critical activities at an acceptable level during disruption. A business continuity plan identifies critical functions, key dependencies, minimum service levels, alternative processes, responsibilities and recovery priorities.

Disaster recovery usually refers to the restoration of critical systems, infrastructure, data and technology after a disruption. It is particularly relevant for IT, cybersecurity, data protection, operational technology and other infrastructure on which business continuity depends.

These areas should not be managed as separate documents without coordination. A company may have a crisis management plan, business continuity plan, disaster recovery plan, cyber incident response plan, communication plan and other related documents, but they should form one coherent resilience framework. The Board should be able to understand how these documents fit together, who owns them, when they are activated, and how they are tested.

The Board's role in resilience

The Board is not expected to manage an emergency on a day-to-day basis. Operational responsibility normally belongs to the CEO and management. However, the Board should ensure that the company has an appropriate resilience framework, that management is prepared for serious disruptions, and that the company can continue to protect long-term value under stress.

The Board should approve the company's overall approach to resilience, including the risk appetite, governance structure, reporting arrangements and escalation criteria. It should satisfy itself that resilience is embedded in strategy, risk management, internal control, compliance, sustainability and capital allocation.

The Board should also ensure that the company has identified its most material disruption scenarios. These may include cyberattacks, loss of key systems, loss of premises, supply chain failure, energy disruption, industrial accidents, fraud, regulatory intervention, sanctions exposure, pandemics, extreme weather events, product safety incidents, liquidity shocks, reputational crises or loss of key people.

A mature Board should not only ask whether plans exist. It should ask whether they are realistic, tested, understood by the right people, supported by adequate resources, and capable of being executed under pressure.

Responsibilities of management

Management is responsible for designing, implementing and maintaining the company's resilience arrangements. This includes preparing relevant plans, assigning roles, training employees, maintaining emergency contacts, ensuring data back-up and system recovery, engaging with critical suppliers, organising simulations and reporting material weaknesses to the Board.

Management should ensure that the company has clear procedures for incident detection, escalation, decision-making and communication. In a crisis, delays, uncertainty and unclear authority may cause as much damage as the incident itself. Therefore, the company should know in advance who has authority to activate the crisis plan, who leads the crisis team, who communicates with employees, regulators, customers, shareholders and media, and when the Board must be informed or convened.

Management should also maintain an up-to-date view of critical dependencies. These include key people, key suppliers, technology systems, outsourced service providers, premises, logistics, licences, funding arrangements, insurance cover and regulatory permissions.

Crisis management and emergency response

A crisis may develop rapidly and under conditions of uncertainty. The purpose of crisis management arrangements is to ensure that the company can make timely, coordinated and well-informed decisions when normal management processes are insufficient.

A crisis management plan should define:

AREA	KEY QUESTION
1. **Activation**	What events trigger the crisis plan?
2. **Escalation**	When must the CEO, Chair, Board or committee be informed?

AREA	KEY QUESTION
3. **Crisis team**	Who is responsible for leading the response?
4. **Decision authority**	Who can make urgent decisions?
5. **Stakeholder communication**	Who communicates with whom, and through which channels?
6. **Regulatory obligations**	Which notifications may be required?
7. **Documentation**	How are decisions and actions recorded?
8. **Recovery**	How does the company return to normal operations?
9. **Learning**	How are lessons identified and implemented?

The Board should agree in advance which events require immediate notification to the Chair, the full Board or a relevant Board committee. For example, the Board should normally be informed promptly of incidents that may have a material impact on people's safety, financial stability, legal compliance, market disclosure, reputation, business continuity, data security or licence to operate.

Business continuity plan

A business continuity plan should identify how the company will continue its essential operations during a disruption. It should be practical, proportionate and tailored to the company's size, sector, complexity and risk profile.

At a minimum, the business continuity plan should address:

AREA	MATTERS TO BE COVERED
1. **Critical functions**	Which activities must continue during disruption
2. **Recovery priorities**	Which services, processes or sites must be restored first
3. **Minimum acceptable level of service**	What level of operation is acceptable during disruption
4. **Roles and responsibilities**	Who activates and manages the plan
5. **Key dependencies**	People, systems, suppliers, premises, data and funding
6. **Alternative arrangements**	Remote work, substitute suppliers, alternative sites, manual processes
7. **Communication**	Employees, customers, regulators, shareholders, suppliers and media

AREA	MATTERS TO BE COVERED
8. **Testing**	Exercises, simulations and lessons learned
9. **Review cycle**	Regular updates and approval process

The business continuity plan should not be a formal document prepared only for compliance purposes. It should be capable of being used in real time. The Board should therefore receive assurance that the plan is up-to-date, tested and known by the relevant people.

Disaster recovery plan

A disaster recovery plan should set out how the company will restore critical systems, data, infrastructure and technology following a major disruption. For many companies, disaster recovery is closely linked to cybersecurity, data protection, digital operations, customer service and financial reporting.

The disaster recovery plan should define recovery time objectives and recovery point objectives (RTO and RPO) for critical systems. In simple terms, the company should know how quickly each critical system must be restored and how much data loss, if any, is acceptable. The plan should also address back-up arrangements, access rights, third-party service providers, cloud infrastructure, alternative communication channels and manual workarounds.

The Board does not need to review every technical detail. However, it should understand whether recovery assumptions are realistic, whether critical systems have been tested, whether there are single points of failure, and whether the company has adequate cyber and technology resilience.

Crisis communication

Communication is a central part of resilience. In a crisis, unclear or inconsistent communication can damage trust, increase legal risk and undermine the company’s reputation. The company should have prepared communication protocols for employees, customers, regulators, shareholders, creditors, suppliers, communities, media and other relevant stakeholders.

The Board should ensure that the company’s communication approach is accurate, timely, responsible and aligned with legal obligations. For listed companies, crisis communication may also involve market disclosure obligations. For regulated companies, communication with supervisory authorities may be critical. For companies providing essential services, communication with customers, municipalities, government bodies and the public may be equally important.

The company should avoid both excessive silence and premature speculation. Good crisis communication should explain what is known, what is being done, what stakeholders should do, and when further information can be expected.

The Board should ensure that the company has a written crisis communication plan that is approved at the appropriate management level and reviewed by the Board or relevant Board committee. The plan should be proportionate to the company's size, sector, ownership structure, regulatory status and risk profile.

Testing and Board assurance

Resilience cannot be assessed only by the existence of written plans. Plans should be tested through exercises, simulations, scenario discussions and post-incident reviews. Testing helps to reveal gaps in decision-making, communication, technology recovery, supplier readiness, employee awareness and Board escalation.

The Board should receive periodic assurance on resilience. This may include management reports, internal audit reviews, external assessments, cyber resilience testing, supplier resilience reviews, insurance reviews and tabletop exercises involving senior management and, where appropriate, Board members.

A useful practice is to conduct at least one annual Board-level resilience discussion. This may focus on a major scenario such as cyberattack, loss of a critical supplier, liquidity stress, geopolitical disruption, energy shortage, product safety incident or reputational crisis. The purpose is not to predict the future precisely, but to test whether the company can think and act under pressure.

Good governance practices

A company with a sound resilience framework will usually have the following features:

GOOD PRACTICE	EXPLANATION
Board-level oversight	The Board periodically reviews resilience risks, plans and test results
Clear management ownership	A senior executive is responsible for resilience coordination
Integrated plans	Crisis management, business continuity and disaster recovery plans are aligned
Defined escalation	The company knows when and how to inform the CEO, Chair and Board
Tested procedures	Plans are tested through realistic exercises

GOOD PRACTICE	EXPLANATION
Critical dependency mapping	Key systems, people, suppliers and sites are identified
Communication protocols	Internal and external communication responsibilities are clear
Supplier resilience	Critical third-party dependencies are reviewed
Cyber resilience	Technology recovery and cyber response are regularly tested
Lessons learned	Incidents and exercises lead to documented improvements
Regular reporting	The Board receives concise, decision-useful information
Proportionality	Arrangements reflect the company's size, sector and complexity

KEY TAKEAWAYS

A. Corporate resilience is the ability to anticipate, prepare for, respond to and recover from serious disruption while protecting people, assets, operations, reputation and long-term value. It is part of the Board's responsibility for strategy, risk oversight and accountability, not an operational detail.

B. Resilience is one integrated framework: crisis preparedness, emergency response, business continuity and disaster recovery, supported by crisis communication and learning from incidents. The Board should know how the plans fit together, who owns them, when they are activated and how they are tested and results assessed.

C. The Board does not manage emergencies, but it approves the overall approach and risk appetite, ensures that the most material disruption scenarios and critical dependencies have been identified, and agrees in advance which events must be escalated to the Chair, the Board or a committee.

D. For many companies' resilience is also a legal duty under EU rules such as NIS2, DORA and the Critical Entities Resilience Directive, with obligations on the management body.

E. Plans are only as good as their testing. The Board should receive periodic assurance on resilience and hold at least one Board-level resilience discussion a year around a major scenario.

F. Good crisis communication is prepared in advance for all key stakeholders, avoids both silence and speculation, and is aligned with disclosure and regulatory obligations.

QUESTIONS FOR THE BOARD

1. *What are the most serious disruption scenarios that could affect the company, and which activities, systems, people and suppliers are critical to continuing operations?*
2. *Do we have approved and tested crisis management, business continuity and disaster recovery plans, and do they form one coherent framework with clear ownership?*
3. *Who has the authority to activate the crisis plan, and when must the Chair, the Board or a Board committee be informed?*
4. *Which resilience-related legal regimes (NIS2, DORA, critical entities) apply to us, and how is compliance assured?*
5. *Have we tested crisis decision-making at senior management and Board level, and what did the last exercise, incident or near miss teach us?*
6. *Are our communication protocols clear for employees, regulators, shareholders, customers and the media, and consistent with our disclosure obligations?*
7. *Do we understand our critical third-party and outsourced dependencies, and is our insurance cover, including D&O, cyber and business interruption, adequate?*
8. *Does internal audit or another assurance provider review our resilience arrangements, and are resilience risks reflected in strategy, capital allocation and risk appetite?*
9. *In a group, are the group resilience policies suitable for each subsidiary, and could we continue critical operations if several disruptions occurred at the same time?*