

CAPABILITY TO ACT: THE NEW FOUNDATION OF ORGANISATIONAL RESILIENCE

EXECUTIVE BRIEFING

EXECUTIVE SUMMARY

Leadership is no longer exercised primarily by reducing uncertainty, but by enabling organisations to perform despite it.

When was the last time leaders could confidently assume that next year would look broadly like this year? Many executives would struggle to answer that question. Perhaps some are still waiting for a return to “business as usual”. The challenge is that business as usual may no longer exist in the form many organisations were built for.

AI, cyber threats, geopolitical tensions, demographic shifts and growing dependencies drastically reshape the environment in which organisations operate. A diverse set of developments dynamically interacts with one another rather than appearing as isolated developments. Arguably, uncertainty is becoming less of a temporary disruption and more of a defining characteristic of the operating environment.

In the World Economic Forum’s 2026 Global Risks Perception Survey, 50% of more than 1,300 experts worldwide anticipated a “turbulent” or “stormy” global outlook over the next two years, rising to 57% over the next decade.¹ Uncertainty also affects corporate investment decisions. In the EIB Investment Survey 2025, 83% of EU firms identified uncertainty about the future as an investment barrier, making it the most widely cited obstacle to investment.²

This fundamentally changes the conditions under which organisations make decisions, deliver their mission and create long-term value. It also changes the nature of organisational resilience.

We argue that resilience can no longer be understood primarily as the ability to withstand disruption or recover from crises. In an environment characterised by continuous uncertainty, a “return-to-normal” approach is not viable anymore. A new understanding of resilience is needed, grounded in the concept of “Capability to Act”:

Capability to Act is the organisational capacity to decide, coordinate and execute.

Resilience is what enables that capability to be sustained and adapted when disruption, uncertainty and strategic pressure occur.

Capability to Act is more than a leadership attribute, an operational capability or a resilience programme. It is an executive framework for strengthening organisational resilience. It integrates leadership, governance, technology, dependencies and ecosystem coordination into a comprehensive objective: maintaining an organisation’s freedom to make sound decisions and execute effectively when it matters most.

Based on this conviction, this briefing explores five executive priorities that strengthen the foundations of Capability to Act and thereby ultimately contribute to resilience:

- Artificial intelligence as a mission-critical organisational capability.
- Cyber resilience as the foundation of operational continuity.
- Strategic dependencies and digital sovereignty as the basis for preserving freedom to act.
- Ecosystem strength as a response to increasingly interconnected organisational networks.
- Decision effectiveness as the organisational outcome of integrating these capabilities into consistently better strategic decisions.

These priorities form a framework for organisations seeking to strengthen resilience – not by preparing for any possible disruption, but by continuously preserving their Capability to Act. In the coming decade, this capability may become the defining differentiator between organisations that merely withstand uncertainty and those that continue to lead through it.

¹ World Economic Forum (WEF): Global Risks Report 2026. Available online at: <https://www.weforum.org/publications/global-risks-report-2026/in-full/>

² European Investment Bank (EIB): EIB Investment Survey 2025: European Union Overview. Available online at: <https://www.eib.org/en/publications/20250216-econ-eibis-2025-eu>

WHY CAPABILITY TO ACT MATTERS NOW

FROM MANAGING STABILITY TO LEADING THROUGH UNCERTAINTY

Organisations have traditionally strengthened their competitiveness through efficiency, optimisation and scale. These capabilities remain essential. Yet, they are no longer sufficient on their own. As uncertainty becomes a structural condition, organisations that will succeed are not necessarily those that change the fastest. It is those that continuously adapt while preserving their ability to execute.

Governance, compliance and risk management remain indispensable pillars of organisational performance. Many organisations have become exceptionally good at providing stability, accountability and control. However, these mechanisms were largely designed for an environment in which change was more predictable, disruptions more isolated and planning horizons more stable. Far fewer organisations have deliberately developed the capability to lead through uncertainty.

Today's conditions do not invalidate these mechanisms, but they expose their limits. The challenge is therefore to recognise where governance reaches its natural boundaries and leadership must begin. Rules help organisations manage what is known. Leadership enables organisations to navigate what is not.

As conditions become increasingly novel, interconnected and unpredictable, resilience depends on leaders' ability to make sound decisions, align capabilities and sustain coordinated execution under pressure.

We thus argue that leadership is no longer exercised primarily by reducing uncertainty. Increasingly, it is

demonstrated by enabling organisations to perform despite uncertainty.

The defining organisational capability in an age of continuous uncertainty will not be the ability to predict every disruption or recover from every crisis. It will be the ability to adapt without losing the capacity to execute. This is what we call Capability to Act and what defines, at the core, resilient organisations.

83%

OF EU FIRMS IDENTIFY UNCERTAINTY ABOUT THE FUTURE AS THE BIGGEST INVESTMENT BARRIER.

The concept of organisational resilience is already evolving in this direction. UK government guidance, for instance, defines it as "the ability to achieve intended outcomes through uncertainty, disruption and change", reflecting this shift from a predominantly preparatory and recovery-oriented model towards risk reduction and adaptation.³ This briefing takes that evolution one step further by asking which specific capabilities enable leaders to preserve their ability to decide, coordinate and execute under such conditions.

³ UK Resilience Academy: Organisational Resilience Guidance for UK Government Departments, Agencies and Arm's-Length Bodies, 2025. Available online at: <https://www.gov.uk/government/publications/organisational-resilience-guidance-for-uk-government-departments-agencies-and-arms-length-bodies>

THE FOUNDATIONS OF CAPABILITY TO ACT

DEFINING CAPABILITY TO ACT

Capability to Act is the organisational capacity to make sound decisions, adapt priorities, coordinate capabilities and execute effectively under changing conditions.

It is not a single function, programme or technology initiative. Nor is it an alternative to governance, resilience or agility. It is the capacity that enables these elements to work together when the strategic environment becomes uncertain, fast-moving and difficult to predict.

In this sense, Capability to Act shifts the focus of resilience. Resilience is not only about resisting disruption or recovering from crises. It is about preserving the ability to decide, adapt and execute while disruption unfolds. The central question is therefore not whether an organisation can return to normal after a shock. It is whether it can continue to act effectively when normal conditions no longer provide sufficient guidance.

Capability to Act also differs from agility. Agility emphasises responsiveness and speed. These remain important, but speed alone does not create resilience. Organisations may react quickly and still move in the wrong direction. Capability to Act is broader. It combines responsiveness with orientation, coordination and execution.

Nor does Capability to Act replace governance. Governance provides structure, accountability and control. Capability to Act ensures that these mechanisms remain effective when situations become novel, interconnected or ambiguous. It enables organisations to complement rules, processes and control frameworks with judgement, adaptability and coordinated action.

We define Capability to Act through five mutually reinforcing dimensions.

First, organisational intelligence.

Organisations need the ability to generate, interpret and apply relevant insights. This includes trusted data, analytical capabilities, human judgement and increasingly AI-supported decision-making. Organisational Intelligence enables leaders to understand changing conditions early enough to respond with purpose.

Second, operational continuity.

Organisations must be able to maintain critical operations and services under stress. This requires more than preventing disruption. It requires the ability to sustain essential functions, recover quickly where necessary and continue delivering the organisation's mission even when systems, processes or external conditions are under pressure.

Third, strategic dependencies.

Organisations increasingly depend on complex ecosystems of technologies, platforms, suppliers, service providers and international partners. These dependencies are neither new nor inherently problematic. In many cases, they are essential to innovation, performance and scale. The central challenge is therefore not to eliminate dependencies, but to understand and manage them consciously. Capability to Act depends on knowing which dependencies affect organisational resilience, how critical they are and what options remain available when circumstances change.

Fourth, ecosystem coordination.

No organisation preserves its Capability to Act alone. Critical capabilities increasingly depend on partners, suppliers, public institutions, private

actors and wider ecosystems. Ecosystem coordination describes the ability to coordinate action across organisational boundaries, build trusted collaboration and mobilise complementary capabilities when they are needed most.

Fifth, decision effectiveness.

Ultimately, Capability to Act is tested in decisions. Decision effectiveness is therefore the integrative dimension of Capability to Act. It determines whether intelligence, continuity, dependency management and ecosystem coordination actually translate into timely decisions and coordinated execution.

These five dimensions describe organisational capabilities, which can be strengthened by executives through specific interventions. Therefore, the following section explores five corresponding executive priorities that help organisations build, strengthen and preserve these capabilities.

Observing these dimensions does neither substitutes for nor guarantees responsibility. Responsibility remains the overarching leadership principle that determines how these capabilities are exercised.

Long-term Capability to Act costs money

It is worth acknowledging that, ultimately, Capability to Act reflects an allocation-of-resources problem. The uncomfortable reality executives face is that strengthening these capabilities requires deliberate investment. Redundancy, continuity mechanisms, alternative sourcing options, trusted partnerships and resilient digital infrastructures often appear less efficient when assessed through a short-term cost lens. Yet, as we argue, they determine an organisation's ability to act when conditions deteriorate. Executive leadership therefore requires balancing short-term efficiency with long-term organisational resilience.

DIMENSION OF CAPABILITY TO ACT

EXECUTIVE PRIORITY

Organisational Intelligence

AI: from productivity tool to mission-critical capability

Operational Continuity

Cyber resilience: from protection to operational continuity

Strategic Dependencies

Strategic dependencies: governing digital sovereignty

Ecosystem Coordination

Ecosystem strength: from partnership to coordinated action

Decision Effectiveness

Decision effectiveness: from insight to execution

BUILDING CAPABILITY TO ACT

Executive priority 1:

AI: FROM PRODUCTIVITY TOOL TO MISSION-CRITICAL CAPABILITY

Core thesis

AI is entering a new phase of organisational relevance. For the first time, organisations are beginning to depend on AI not simply to improve performance, but to perform at all.

As AI becomes embedded across multiple business functions, some organisations are moving towards a level of reliance at which AI availability, quality and governance begin to affect operational continuity. The executive challenge is therefore no longer whether to adopt AI, but how to govern the dependencies, accountability and resilience implications that accompany its growing strategic importance.

Why it matters

AI is emerging as a core component of organisational intelligence. It increasingly shapes how organisations generate insights, interpret information and make decisions across business operations, public services and leadership processes. According to EIB data from 2025, 37% of EU firms use generative AI. Some 55% of European AI users deploy it across more than two business activities.⁴ AI adoption is also associated with a 4% productivity gain, conditional on complementary investment in data, software and skills.⁵

When AI is no longer merely supporting performance but is an integral part of the decision and execution infrastructure of organisations, they become increasingly dependent on AI. This dependency is not inherently problematic. The critical question is whether leaders understand where AI has become mission-critical and how that dependence can be governed responsibly.

At the same time, executives must ensure that AI strengthens rather than gradually replaces human judgement. The resilience challenge is therefore not only technical. Organisations must be able to maintain decision quality, operational continuity and accountability when AI systems fail, become unavailable or produce unexpected outcomes.

Executive implications

AI should no longer be managed solely as an innovation initiative or technology programme. It should be governed as a mission-critical organisational capability.

The executive question is no longer “Where can we use AI?” but “Where can we no longer operate effectively without it?”

Leadership teams should understand where AI has become operationally indispensable, identify emerging dependencies and ensure that accountability evolves alongside technological capability. The objective is not to limit AI adoption. It is to ensure that organisational dependence on AI remains transparent, deliberate and aligned with executive responsibility.

55%

OF EUROPEAN FIRMS USING AI
DEPLOY IT ACROSS MULTIPLE
BUSINESS ACTIVITIES.

Resilient organisations will not be distinguished by the scale of their AI adoption, but by how deliberately they govern AI as a mission-critical capability.

⁴ European Investment Bank (EIB): European Firms Show Resilience, Invest in Green Transition and Match US Companies in Adopting AI Technologies, 2025. Available online at: <https://www.eib.org/en/press/all/2025-383-european-firms-show-resilience-invest-in-green-transition-and-match-us-companies-in-adopting-ai-technologies-new-eib-survey-shows>

⁵ European Investment Bank (EIB): Economics Working Paper 2026/02, 2026. Available online at: <https://www.eib.org/en/publications/20250383-economics-working-paper-2026-02>

Executive priority 2: CYBER RESILIENCE: FROM PROTECTION TO OPERATIONAL CONTINUITY

Core thesis

Cyber resilience is no longer primarily a security issue. It has become a question of operational continuity.

As organisations become increasingly dependent on digital technologies, the executive challenge is no longer to prevent every cyber incident. It is to ensure that critical operations, essential services and decision-making can continue despite disruption.

In this new reality, cyber resilience is measured less by the absence of successful attacks than by an organisation's ability to sustain its mission when disruption inevitably occurs.

Why it matters

Maintaining operational continuity is a defining feature of Capability to Act. As organisations become increasingly dependent on interconnected digital systems, cyber resilience becomes inseparable from the ability to sustain critical operations.

Historically, cybersecurity focused on protecting systems and reducing vulnerabilities. While these objectives remain essential, executive leaders must increasingly assume that disruption will occur despite significant investments in prevention.

At the same time, digital transformation has created new concentrations of dependency. Critical services, core processes and decision-making increasingly rely on a relatively small number of digital systems, data flows and external providers. These dependencies create strategic control points:

Critical assets, capabilities or positions whose control enables one actor to influence, restrict or shape the strategic options available to another.

The scale of the challenge is visible in incident data. The European Union Agency for Cybersecurity (ENISA) analysed 4,875 cybersecurity incidents affecting the European threat landscape between July 2024 and June 2025, speaking of a "maturing threat environment characterised by rapid exploitation of vulnerabilities and growing complexity in tracking adversaries".⁶ Regulation is also consequently moving beyond prevention: Since January 2025, for instance, DORA has required financial entities to withstand, respond to and recover from ICT disruption, including through resilience testing and the management of critical third-party risk.⁷

The executive challenge is therefore not simply to protect technology, but to understand which control points are critical to mission delivery and how organisational capability can be preserved when they are compromised.



Arguably, cyber resilience is only one dimension of operational continuity. It can, and should, equally extend to physical resilience. Critical infrastructure failures, extreme weather events, supply-chain disruptions and workforce shortages can impair

⁶ European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape 2025, 2025, S. 6.
Available online at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

⁷ European Insurance and Occupational Pensions Authority (EIOPA): Digital Operational Resilience Act (DORA).
Available online at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

operations just as severely as cyber incidents. The executive task is therefore to understand which disruptions, regardless of origin, threaten the organisation's Capability to Act most significantly.

Executive implications

Cyber resilience should be governed as a mission-critical organisational capability rather than a technology programme.

Rather than asking "Can we prevent every incident?" executives today deal with the question of whether they can continue delivering their mission when critical control points are under attack.

Leadership teams should identify the organisational capabilities and services that must remain operational under all circumstances, together with the digital control points on which they depend. Particular attention should be given to dependencies whose disruption would significantly impair decision-making, service delivery or operational execution.

Cyber resilience should therefore be integrated into business continuity planning, crisis management and executive decision-making. Organisations should regularly test whether they can continue to operate, coordinate resources and make effective decisions under degraded conditions.

The objective is not to eliminate cyber risk entirely. It is to ensure that disruption does not compromise the organisation's Capability to Act.

Resilient organisations will be distinguished not by the absence of cyber incidents, but by their

ability to sustain critical operations and fulfil their mission despite them.

Executive priority 3:

STRATEGIC DEPENDENCIES: GOVERNING DIGITAL SOVEREIGNTY

Core thesis

As organisations become increasingly interconnected, strategic dependencies are emerging as a defining factor of organisational resilience. The executive challenge is not to eliminate them, but to understand which of them determine the organisation's freedom to decide and act.

Digital sovereignty and trusted data help organisations preserve meaningful control over critical decisions despite growing technological, operational and geopolitical interdependencies.

Why it matters

Strategic Dependencies are a core component of an organisation's Capability to Act. Cloud platforms, AI models, data ecosystems, software providers and global supply chains have become integral components of modern organisational capability. As a result, dependencies are a structural feature of today's operating environment. With 53% of EU enterprises using paid cloud services in 2025, it matters that AWS, Microsoft Azure and Google Cloud jointly hold about 70% of the European market, compared with around 15% for European providers.^{8, 9, 10} Beyond the often-cited cloud segment, there is also significant ICT concentration risk in the financial sector. Based on voluntary data from financial entities across 30 EEA countries, the three European Supervisory Authorities identified around 15,000 direct ICT third-party

⁸ Eurostat: 53% of EU Enterprises Used Paid Cloud Computing Services in 2025, 2026.

Available online at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1>

⁹ European Parliament: Digital Sovereignty and the European Cloud Market, 2025.

Available online at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA%282025%29780413_EN.pdf

¹⁰ Synergy Research Group: European Cloud Providers' Local Market Share Holds Steady at 15%, 2025.

Available online at: <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

providers and found that most services supporting critical functions, or carrying a high impact if disrupted, could not be substituted.¹¹

Most dependencies can be managed through governance, contracts or contingency planning. However, managing them often requires explicit trade-offs. Alternative suppliers, sovereign options, reserve capacity or additional governance mechanisms can increase cost in the short term while strengthening organisational freedom to act in the long term. The executive challenge is therefore not simply to optimise efficiency, but to determine which dependencies justify deliberate investment in resilience.



This is certainly the case for dependencies which directly influence an organisation's ability to make decisions, deliver critical services or adapt to change. These are strategic dependencies.

In this context, trusted data and digital sovereignty become essential capabilities. Trusted data enables confident decision-making. Digital sovereignty enables organisations to preserve decision-making authority despite unavoidable dependencies.

Executive implications

Leadership teams who, for a while, have asked "What are all our dependencies?" must now change

the question to "Which dependencies determine our freedom to decide and act?"

They should identify the technologies, platforms, suppliers and external relationships on which critical organisational capabilities depend. The objective is not to govern every dependency equally, but to focus attention on those that could materially constrain strategic choice, operational continuity or organisational resilience.

Digital sovereignty should be treated as an outcome of sound executive governance rather than a goal of technological independence. The objective is not complete control, but sufficient influence over critical capabilities to adapt, decide and act when circumstances change.

Resilient organisations will not be distinguished by the absence of dependencies. They will be distinguished by their ability to understand, govern and continuously adapt the dependencies that determine their freedom to act.

Executive priority 4: ECOSYSTEM STRENGTH: FROM PARTNERSHIP TO COORDINATED ACTION

Core thesis

No organisation today owns all the capabilities required to fulfil its mission. Increasingly, critical capabilities are created, delivered and sustained across interconnected ecosystems of public institutions, private organisations, suppliers and technology partners.

As a result, resilience has become a collective capability. The executive challenge is no longer limited to strengthening internal capabilities. It increasingly requires leaders to coordinate the broader ecosystem on which their organisation's ability to act depends.

¹¹ European Supervisory Authorities (EBA, EIOPA, ESMA): Report on the Landscape of ICT Third-Party Providers, 2023. Available online at: https://eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1062211/ESA%202023%2022%20-%20ESAs%20report%20on%20the%20landscape%20of%20ICT%20TPPs.pdf

Why it matters

Ecosystem Coordination is a defining dimension of Capability to Act. As digital platforms, critical infrastructure, supply chains and public services become more interconnected, organisations increasingly control only part of the capabilities required to deliver their mission.

With intermediate goods and services accounting for around 60% of global trade, no organisation can secure its operational resilience alone. As the OECD Supply Chain Resilience Review argues, it is essential to focus on trusted partners and effective coordination across organisational and national boundaries.¹²



This changes the nature of resilience. Critical services often depend not only on an organisation's own preparedness, but also on the capabilities and responsiveness of partners. This is particularly visible in areas such as critical infrastructure, trade, healthcare, digital government and public safety, where public and private organisations jointly deliver outcomes that no single actor could sustain alone.

Leadership therefore extends beyond organisational authority. Organisations must be able to align

capabilities, coordinate decisions and enable effective action across institutional boundaries when disruption affects multiple actors simultaneously.

Ecosystem strength is therefore not simply about collaboration. It is the ability to translate interdependence into coordinated action.

Executive implications

The executive question is no longer "Who are our partners?" but "Which critical capabilities depend on coordinated action beyond our organisation?"

Leadership teams should identify where mission-critical capabilities depend on external organisations, strategic partners or public institutions. These relationships should be treated as integral components of organisational capability rather than purely contractual arrangements.

Resilient organisations invest not only in their own preparedness, but also in the strength of the ecosystems on which they depend. This increasingly requires public institutions and private organisations to move beyond transactional relationships towards shared preparedness, joint planning and coordinated response capabilities.

The objective is not simply to collaborate more. It is to ensure that multiple organisations can continue to fulfil a shared mission when disruption exceeds the capacity of any single organisation to respond alone.

Resilient organisations will be distinguished not only by the strength of their internal capabilities, but by their ability to coordinate and mobilise capabilities across the ecosystems through which their mission is delivered.

¹² Organisation for Economic Co-operation and Development (OECD): OECD Supply Chain Resilience Review, 2025. Available online at: https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

Executive priority 5: DECISION EFFECTIVENESS: FROM INSIGHT TO EXECUTION

Core thesis

In an environment characterised by continuous uncertainty, the ability to make and execute better decisions becomes a defining source of organisational resilience.

Decision effectiveness is not primarily the result of individual leaders or technology alone. It emerges from an organisation's ability to combine trusted information, resilient operations, effective governance and coordinated action into consistently better decisions.

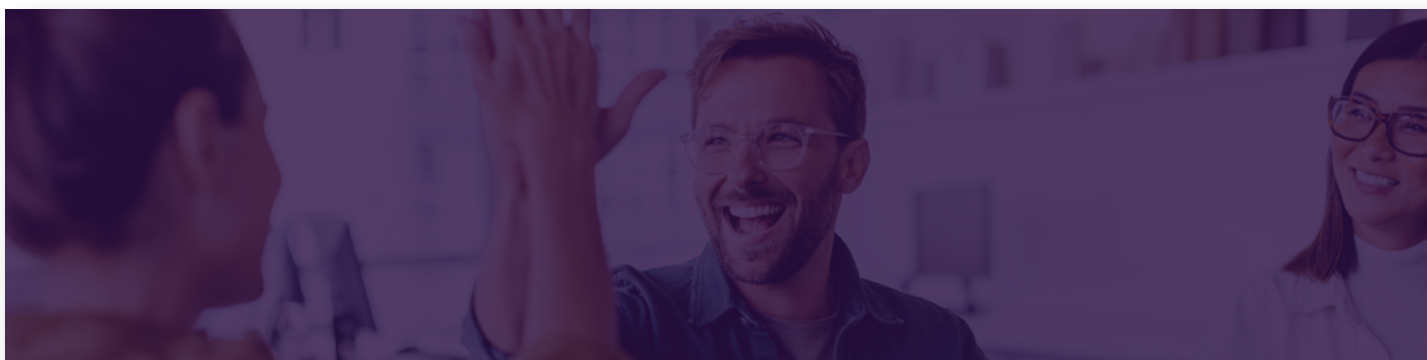
The executive challenge is therefore not simply to improve individual decisions. It is to build an organisation capable of making sound decisions under uncertainty and translating them into effective action.

Why it matters

Decision Effectiveness is the outcome dimension of Capability to Act. It is where the other four capabilities prove that they enable consistently better decisions under conditions of uncertainty.

In that regard, it is important to consider the human dimension of decision-making. Organisations operating in prolonged periods of uncertainty may experience decision fatigue, risk aversion and reduced willingness to act. Decision effectiveness therefore depends not only on information and governance, but also on a culture that enables people to exercise judgement, challenge assumptions and take responsibility under uncertainty.

Research shows that organisations can communicate uncertainty transparently without necessarily undermining trust. Cambridge experiments found that presenting statistical uncertainty as a numerical range had no effect on the perceived trustworthiness of the source, whereas merely stating that uncertainty existed without quantifying it could reduce trust.¹³ Other research highlights that complex choices can exceed the time and cognitive resources of individual decision makers, and that communication mechanisms can support collective decision-making.¹⁴ This makes it essential that people can raise concerns, challenge assumptions and discuss mistakes. However, psychological safety alone does not guarantee performance; it must be combined with accountability and mechanisms that translate learning into coordinated action.¹⁵



¹³ Kerr, John, et al.: Communicating Statistical Uncertainty and Public Trust, 2023.

Available online at: <https://www.repository.cam.ac.uk/items/60837e23-a599-4c35-ad2c-b1526b559e49>

¹⁴ Bossaerts, Peter: Communication Mechanisms and Collective Decision-Making, 2026.

Available online at: <https://www.econ.cam.ac.uk/publications/cwpe/2611>

¹⁵ Higgins, Monica: Psychological Safety, Accountability and Organisational Performance, 2020.

Available online at: <https://dash.harvard.edu/server/api/core/bitstreams/d3793d11-bc1e-40c7-ac72-1aefd6ec2c22/content>

Operational Continuity preserves performance during disruption. Strategic Dependencies help protect freedom of action. Ecosystem Coordination enables collective execution across organisational boundaries.

Together, these capabilities create the conditions for Decision Effectiveness: people's ability to make and execute better decisions despite uncertainty.

Executive Implications

Having enough information is a good precondition. Executives must today take it one step further and ask: "Does our organisation consistently turn information into effective action?"

Teams leading organisations should view decision-making as an organisational capability rather than solely an individual responsibility. This requires deliberate attention to the structures, processes, data, technologies and governance mechanisms that shape how decisions are made and executed.

It also requires an organisational environment in which leaders and teams feel able to exercise judgement under uncertainty. Psychological safety and trust help ensure that decision-making capacity is preserved when pressure and ambiguity increase.

The objective is not simply faster decisions. It is better decisions, made under pressure, adapted as circumstances change and translated into coordinated action.

Organisations will not be distinguished by the sophistication of their technologies, the volume of their data or the maturity of their governance alone. They will be distinguished by their ability to integrate these capabilities into effective execution under conditions of continuous uncertainty. Technology can accelerate decisions. Only people can assume responsibility for them.

EXECUTIVE REFLECTION

Resilience has traditionally been associated with protection, recovery and the ability to withstand disruption. These capabilities remain essential. Yet in an environment characterised by continuous uncertainty, they are no longer sufficient on their own.

Today, organisations operate in conditions where technological transformation, cyber threats, geopolitical developments, strategic dependencies and interconnected ecosystems continuously reshape the context for decision-making and execution. In such an environment, resilience can no longer be defined primarily by the ability to return to a previous state. Increasingly, it depends on preserving an organisation's ability to decide, adapt and act while conditions continue to change.

This is the central argument of this briefing. The five priorities presented are not independent technology or management initiatives. Together, they form an executive framework for strengthening the organisational capabilities that preserve Capability to Act: Organisational Intelligence, Operational Continuity, Strategic Dependencies, Ecosystem Coordination and Decision Effectiveness.

Organisations that succeed will not necessarily be those that predict every disruption or control every risk. They will be those that continuously strengthen their ability to make sound decisions, coordinate action and execute effectively under changing conditions.

The central question for executive leadership is therefore no longer only how resilient the organisation is, but whether it remains capable of acting when the conditions for action deteriorate.

BOARDROOM DISCUSSION QUESTIONS

Take this conversation to your board meetings. The following questions are not intended as a checklist or a set of independent discussion topics. They are designed as a leadership conversation sequence that progresses from mission and critical capabilities to strategic dependencies, decision-making, ecosystem coordination and future readiness. Together, they help executive teams assess not only how resilient their organisations are today, but whether they are systematically strengthening their Capability to Act.

Mission & Capability to Act

1. Which organisational capabilities are truly mission-critical, and for how long could we continue to deliver each of them at an acceptable level under sustained disruption?
2. Where would a loss of decision-making, coordination or execution capability have a greater impact than the loss of technology or infrastructure itself?

Strategic dependencies & control points

3. Which dependencies most directly determine our freedom to decide and act, and do we actively govern them as strategic risks?
4. Do we understand the critical control points that most significantly determine our Capability to Act, or are important dependencies still largely invisible to executive leadership?

Leadership & decision effectiveness

5. Is our organisation designed to make sound decisions under uncertainty, or primarily to optimise performance under stable conditions?
6. Where are we relying on governance, processes or technology when stronger judgement, adaptability and leadership are actually required?

Ecosystem coordination

7. Which critical capabilities depend on partners, suppliers, public institutions or wider ecosystems, and do we treat these relationships as strategic capabilities rather than external services?
8. If disruption affected an entire ecosystem rather than a single organisation, how effectively could we coordinate decisions and action across institutional boundaries?

Future readiness

9. If a major disruption occurred tomorrow, which capability would we most regret not having strengthened today?
10. What level of redundancy, optionality or reserve capability are we willing to fund today in order to preserve our freedom to act tomorrow?

REFERENCES

Bossaerts, Peter: Communication Mechanisms and Collective Decision-Making, 2026. Available online at: <https://www.econ.cam.ac.uk/publications/cwpe/2611>

ENISA (European Union Agency for Cybersecurity): ENISA Threat Landscape 2025, 2025. Available online at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

European Insurance and Occupational Pensions Authority (EIOPA): Digital Operational Resilience Act (DORA). Available online at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

European Investment Bank (EIB): EIB Investment Survey 2025: European Union Overview, 2025. Available online at: <https://www.eib.org/en/publications/20250216-econ-eibis-2025-eu>

European Investment Bank (EIB): European Firms Show Resilience, Invest in Green Transition and Match US Companies in Adopting AI Technologies, 2025. Available online at: <https://www.eib.org/en/press/all/2025-38-3-european-firms-show-resilience-invest-in-green-transition-and-match-us-companies-in-adopting-ai-technologies-new-eib-survey-shows>

European Investment Bank (EIB): Economics Working Paper 2026/02, 2026. Available online at: <https://www.eib.org/en/publications/20250383-economics-working-paper-2026-02>

European Parliament: Digital Sovereignty and the European Cloud Market, 2025. Available online at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA%282025%29780413_EN.pdf

European Supervisory Authorities (EBA, EIOPA, ESMA): Report on the Landscape of ICT Third-Party Providers, 2023. Available online at: https://eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1062211/ESA%202023%2022%20-%20ESAs%20report%20on%20the%20landscape%20of%20ICT%20TPPs.pdf

Eurostat: 53% of EU Enterprises Used Paid Cloud Computing Services in 2025, 2026. Available online at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1>

Higgins, Monica: Psychological Safety, Accountability and Organisational Performance, 2020. Available online at: <https://dash.harvard.edu/server/api/core/bitstreams/d3793d11-bc1e-40c7-ac72-1aefd6ec2c22/content>

Kerr, John, et al.: Communicating Statistical Uncertainty and Public Trust, 2023. Available online at: <https://www.repository.cam.ac.uk/items/60837e23-a599-4c35-ad2c-b1526b559e49>

OECD: OECD Supply Chain Resilience Review, 2025. Available online at: https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

Synergy Research Group: European Cloud Providers' Local Market Share Holds Steady at 15%, 2025. Available online at: <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

UK Resilience Academy: Organisational Resilience Guidance for UK Government Departments, Agencies and Arm's-Length Bodies, 2025. Available online at: <https://www.gov.uk/government/publications/organisational-resilience-guidance-for-uk-government-departments-agencies-and-arms-length-bodies>

World Economic Forum (WEF): Global Risks Report 2026, 2026. Available online at: <https://www.weforum.org/publications/global-risks-report-2026/in-full/>

CONTACT PERSON



RON DE JONGE

Head of Public Sector, Defense & Security
E. ronald.de.jonge@soprasteria.com



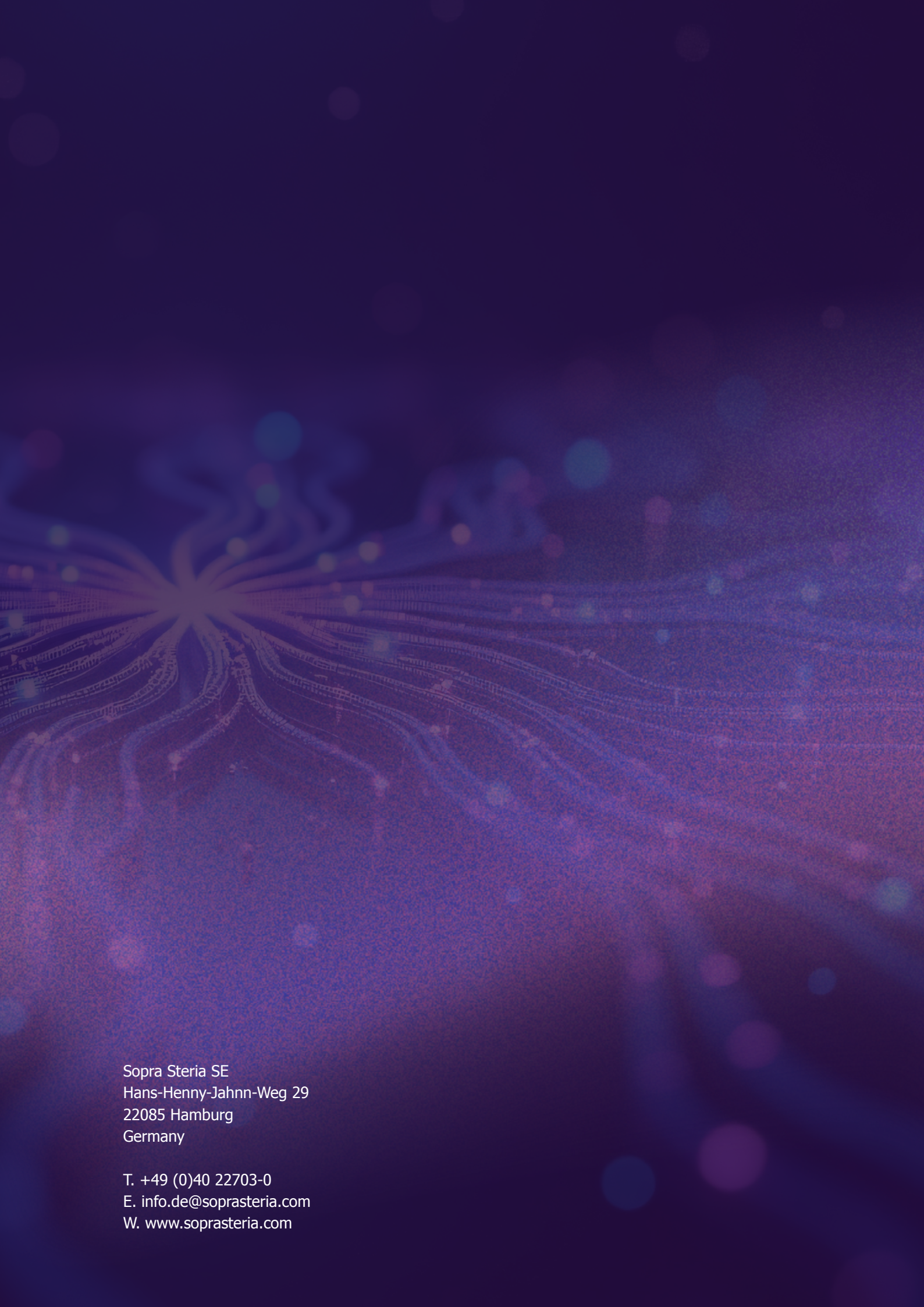
ULF GLÖCKNER

Group Practice Lead Public Sector
E. ulf.gloeckner@soprasteria.com



VIKTORIA RAHN

Senior Manager Public Sector, Defence & Security
E. viktoria.rahn@soprasteria.com



Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Germany

T. +49 (0)40 22703-0
E. info.de@soprasteria.com
W. www.soprasteria.com