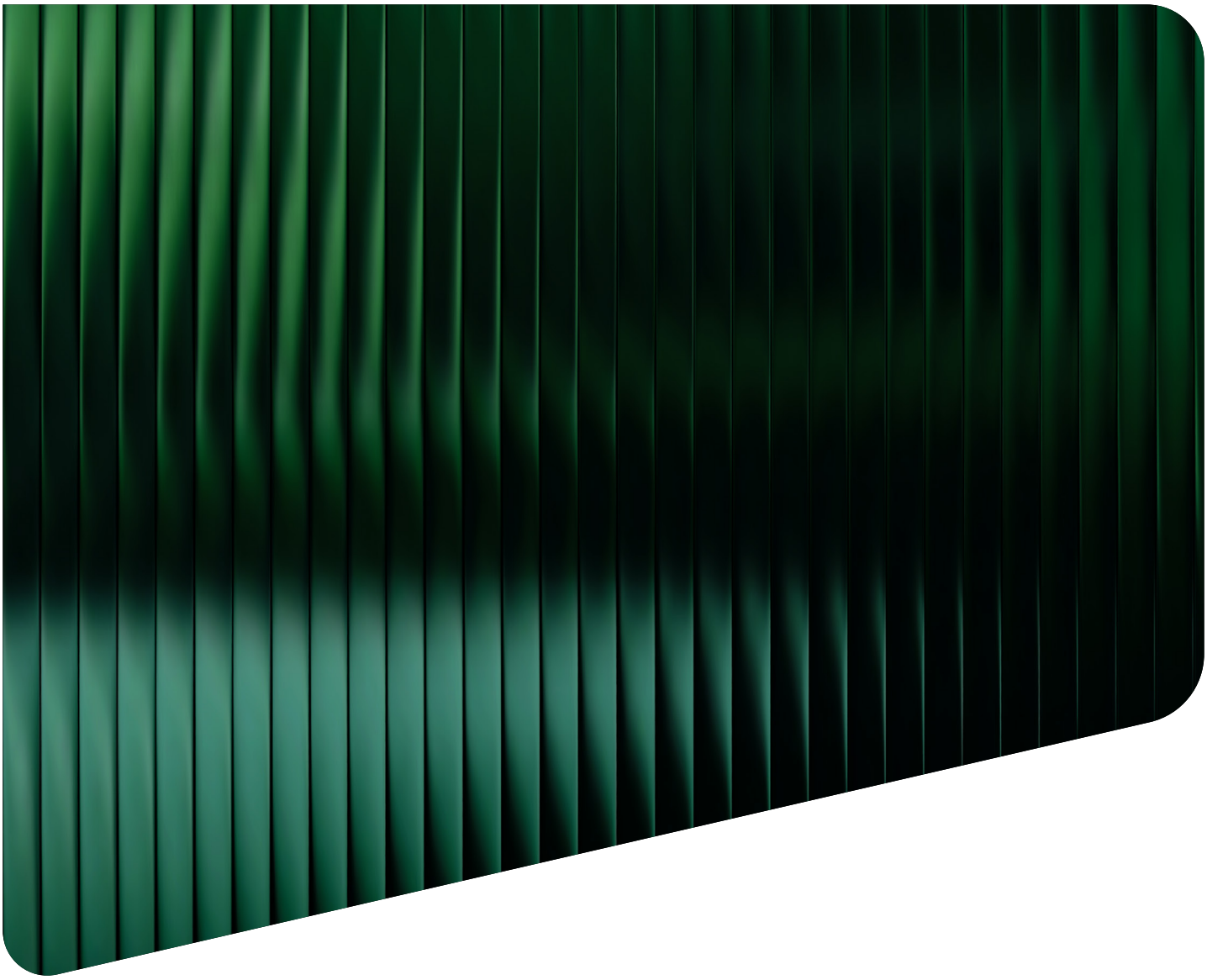


The state of IT resilience in the Nordics

Investment intent is outpacing operational readiness.

Elevated impact.

vivicta

A Vivicta Insight Report

Based on a survey of 320 senior technology and business leaders across Sweden, Norway and Finland.

Research conducted by Kairos Future on behalf of Vivicta.

November 2026

Table of contents

1 Foreword . . . 3
2 Executive summary . . . 4
3 The Nordic IT resilience reality . . . 6
4 IT resilience is about readiness . . . 8
5 People matter more than technology . . . 9
6 Barriers to IT resilience . . . 10
7 The IT resilience ownership gap . . . 11
8 From plans to proven readiness . . . 12
9 The readiness maturity model . . . 13
10 The supplier IT resilience blind spot . . . 14
11 Comparing the Nordic markets . . . 16
12 The next phase of IT resilience . . . 19
13 Conclusions . . . 20
14 The Vivicta perspective . . . 21
15 About the study . . . 23

Foreword

We are operating in an increasingly complex risk landscape. Geopolitical instability, cyber threats, supply chain dependencies, regulatory changes and rapid digital transformation are increasing both the frequency and business impact of disruption. In this context, resilience is no longer a future improvement initiative. It is a business imperative.

IT resilience is more than responding to incidents. It is the ability to maintain critical operations, adapt under pressure and recover quickly. This requires not only resilient technology, but prepared people, clear governance, effective processes and strong collaboration across partners and suppliers.

Digital sovereignty is fundamental for resilience. As organizations become increasingly dependent on digital technologies and ecosystems, they need to maintain control over critical services, data and technology, while retaining the freedom to adapt as circumstances change. The ability to continue operating and recover from disruption is therefore an essential part of maintaining resilience and business continuity in practice.

The findings in this report are encouraging. Nordic organizations recognize the importance of IT resilience and are planning increased investments. Yet a clear gap remains between ambition and execution. Strategies and continuity plans are increasingly in place, but end-to-end testing, supplier validation, accountability and operational readiness remain less consistent.

True resilience is demonstrated when disruption occurs. For leaders, the key question is therefore not whether plans exist, but whether they are actively governed, tested and continuously improved.

I hope this report helps organizations benchmark their preparedness, identify gaps and take practical steps to protect continuity, strengthen their digital sovereignty and build long-term resilience.

Satu Kiiskinen
CEO, Vivicta



EXECUTIVE SUMMARY

Strong ambition, uneven readiness across the Nordics

IT resilience has become a strategic priority across Nordic organizations. Most business and technology leaders recognize its importance and plan to increase investments in the next 12 months. Yet the study reveals a persistent gap between ambition and operational readiness. While many organizations express moderate confidence in their ability to recover critical services, relatively few have the testing, governance and validation practices in place to demonstrate that resilience under real-world scenarios.

The findings suggest that IT resilience is increasingly viewed as an organizational capability rather than a purely technical one. Leaders place the greatest value on workforce readiness, crisis management and clear decision-making structures. At the same time, ownership often remains at the operational rather than executive level, resilience testing rarely extends across organizational and supplier ecosystems and growing IT complexity continues to challenge preparedness.

Nordic organizations are moving in the right direction, but progress is uneven. Finland demonstrates the highest overall maturity, Norway excels in continuity preparedness and rehearsal, while Sweden shows high investment intent but with a larger readiness gap compared to its peers. The overall conclusion is clear: organizations are already investing in IT resilience or planning to do so, but many have yet to translate intent into consistently proven capability.

Key insights

Investment ambition exceeds readiness.

While 64% of organizations expect to increase IT resilience investments within the next 12 months, only 33% report high confidence (6 or 7 on a seven-point scale) in their ability to recover critical services. Only half of the organizations have tested disaster recovery end-to-end and only 44% have undergone independent assessment against regulatory frameworks such as DORA or NIS2.

IT resilience starts with people, leadership and preparedness.

Workforce readiness and crisis management structures emerge as the most important resilience capabilities, cited by 52% of respondents. Both rank ahead of more technology-centric measures such as monitoring and detection (44%) and automated failover capabilities (36%).

Third-party dependencies remain a critical source of risk.

Reliance on suppliers is one of the most cited barriers to resilience, yet only 22% of organizations regularly test continuity capabilities with their key partners and providers. One in five organizations never conducts such testing.

IT resilience ownership often sits below the level it depends on.

Workforce readiness and crisis management are viewed as the most critical resilience capabilities (52% each), yet governance often falls short of that ambition. Four in ten organizations place primary ownership of IT resilience below the executive level, and 11% lack a clear owner altogether, creating a potential gap between responsibility and the authority needed to drive organization-wide preparedness and resilience.

Readiness maturity varies significantly across the Nordics.

Nearly half (46%) of Finnish organizations achieve advanced maturity scores, compared with 27% in Norway and 24% in Sweden. These differences underline that while resilience is a shared priority across the region, the ability to operationalize and validate resilience capabilities differs considerably.

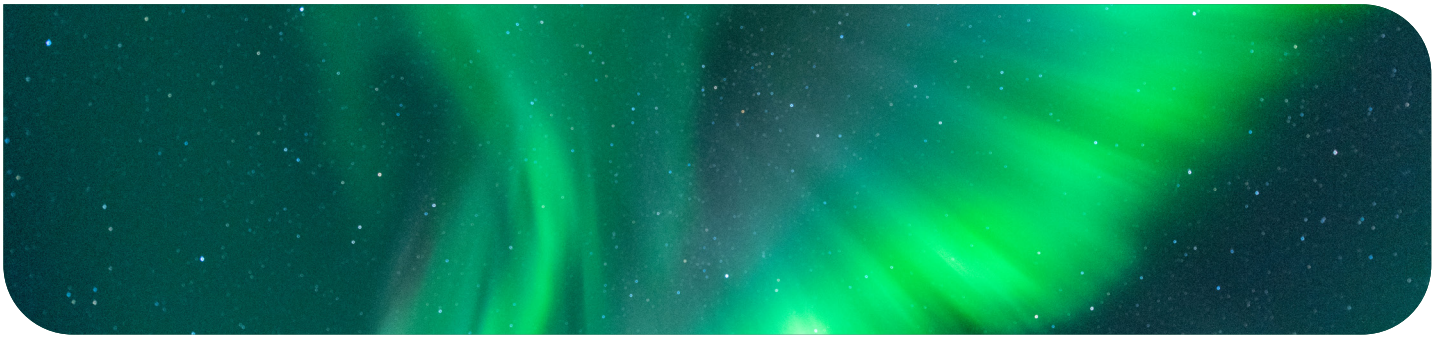


Organizations are ready to invest. Confidence is lagging.

Investment intent is strong among Nordic leaders. However, only one in three is highly confident that they could maintain or recover critical services during a major disruption.

IT resilience has become a standing item on leadership agendas. Almost two-thirds of the organizations surveyed (64%) expect to invest more over the next 12 months, and only 6% expect to invest less. Yet when asked how confident they are that critical services could be maintained or recovered in a major disruption, only one in three respondents (33%) answered with a 6 or 7 on a seven-point scale. The average score is 4.9.

This reflects realism rather than overconfidence. It is a gap between investment intent and operational readiness evidence. The chapters that follow look at where the readiness is thin: definitions, people, barriers, ownership, testing and suppliers.



64% of organizations expect to increase IT resilience spending in the coming 12 months

How do you expect your organization's investment in IT resilience to evolve over the next 12 months? Share of respondents (%).

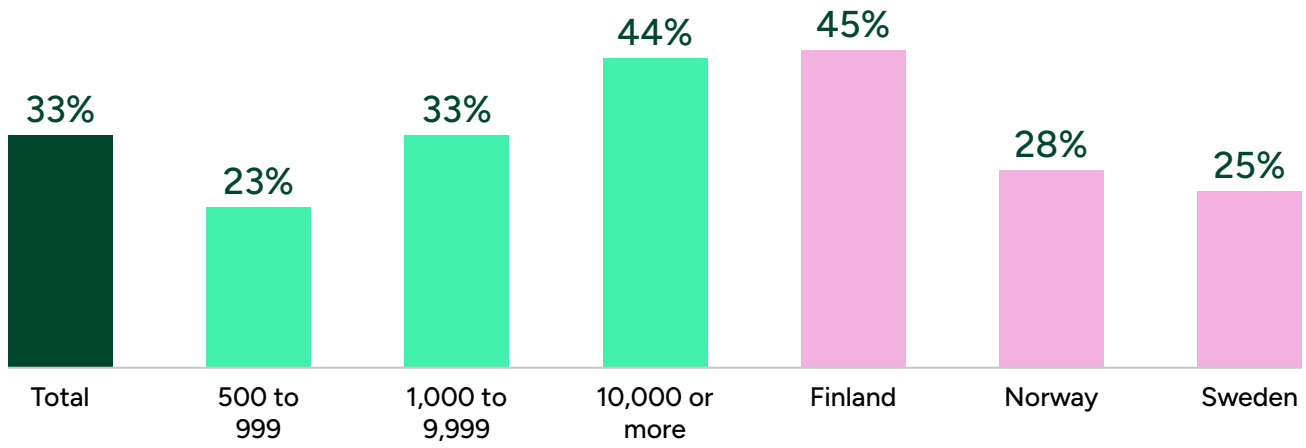


Increase significantly
Increase somewhat
Remain at current level
Decrease (somewhat or significantly)

Percentages are rounded and may not add to 100.
Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

Larger organizations report higher confidence levels, with Finland the most mature in the Nordics

Share of respondents who are highly confident (6 or 7 on a seven-point scale) that critical services can be maintained or recovered during a major disruption (%)



Results are shown for the total sample, organization-size segments (mint) and markets (pink). The smallest and largest organization size segments are based on smaller sample sizes (n=82 and n=61 respectively) and should therefore be interpreted with some caution.

Source: Vivicta Nordic IT Resilience Survey 2026, n=320.



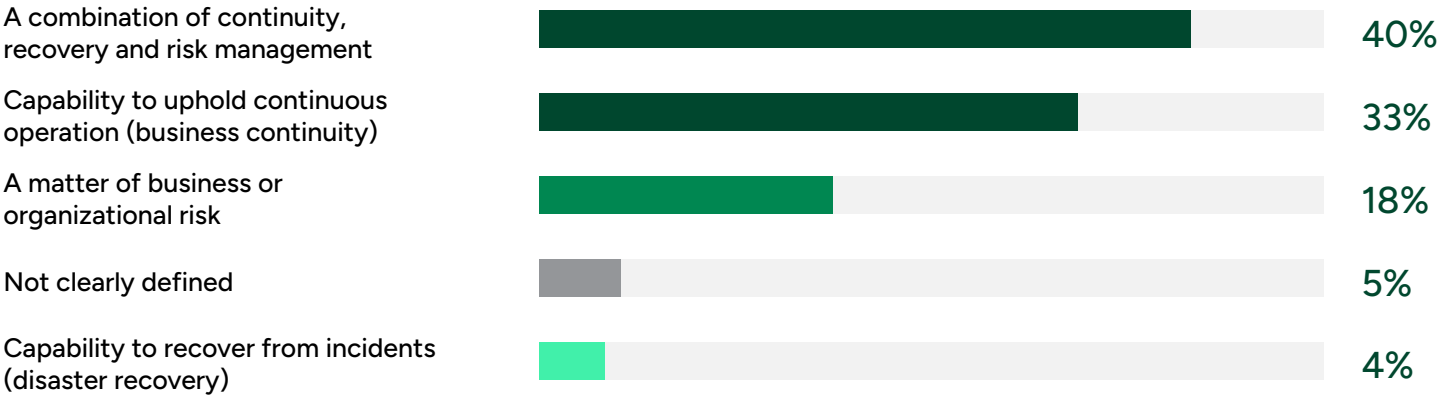
IT resilience is increasingly defined by readiness rather than recovery

From how fast we recover to whether we can keep operating.

For a long time, IT resilience meant disaster recovery: restore the systems, restore the data and get back to normal. Definitions shape budgets, metrics and ownership, so the shift from recovery focus to readiness matters. The findings show that leaders now define IT resilience more broadly than incident recovery alone. This broader definition raises the bar: continuity must be governed, rehearsed and demonstrated across the business ecosystem. Only 4% of leaders define IT resilience primarily as the ability to recover from incidents. The largest group, 40%, sees it as a combination of continuity, recovery and risk management, and a further 33% define it as the capability to keep operating.

IT resilience is understood as continuity first

How is IT resilience primarily understood in your organization? Share of respondents (%).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

PEOPLE MATTER MORE THAN TECHNOLOGY

Human readiness is the foundation of IT resilience

The capabilities leaders value most are workforce readiness and crisis management structures.

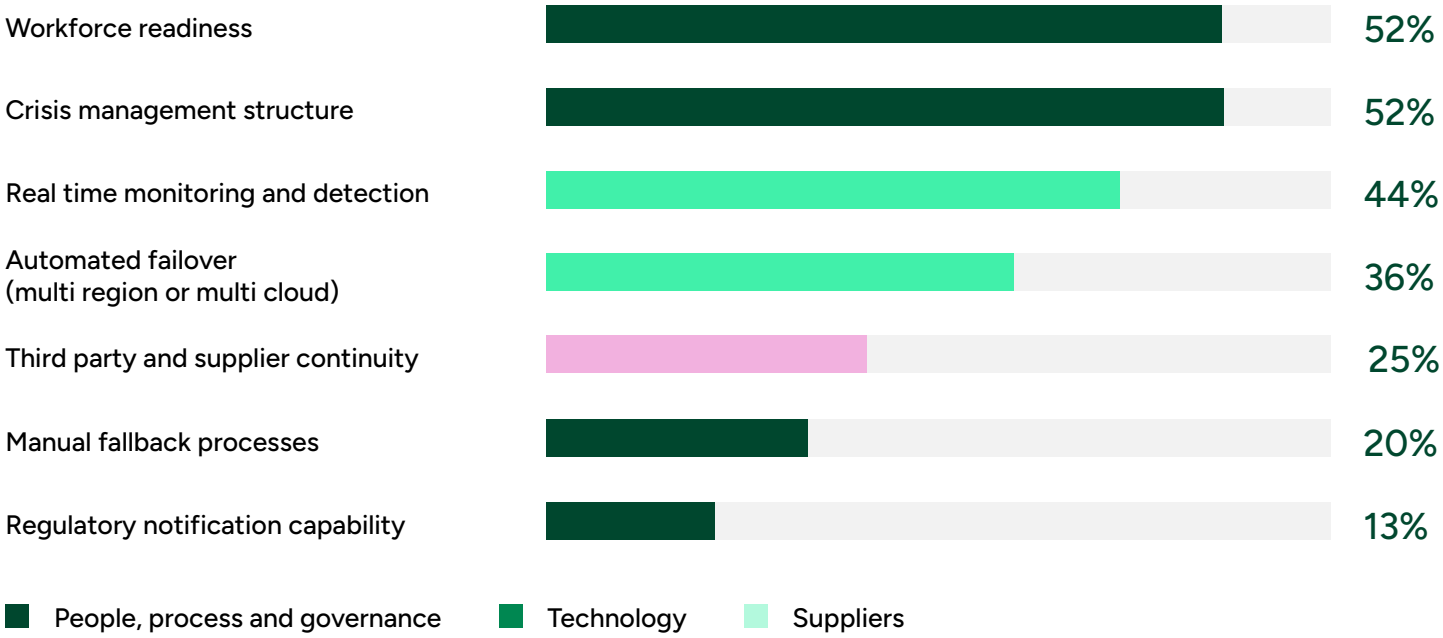
When asked to select the three things most critical to staying resilient, leaders put workforce readiness and crisis management structures first, each chosen by 52% of respondents. Real-time monitoring follows at 44% and automated failover at 36%. Technology is essential, but it is rarely what decides the outcome of an incident.

In practice, IT resilience depends on leadership, communication, coordination and the authority to act.

What those top capabilities have in common is that they cannot simply be bought or installed. They are built through training, rehearsal, clear mandates and trust between functions. Technology alone does not create IT resilience. Even the most robust failover design relies on clear decision rights, defined responsibilities and effective communication when disruption occurs.

People and governance rank as the most critical resilience capabilities.

Most critical to remain IT resilient and maintain operations, share selecting each (up to three options).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

What stands between ambition and IT resilience

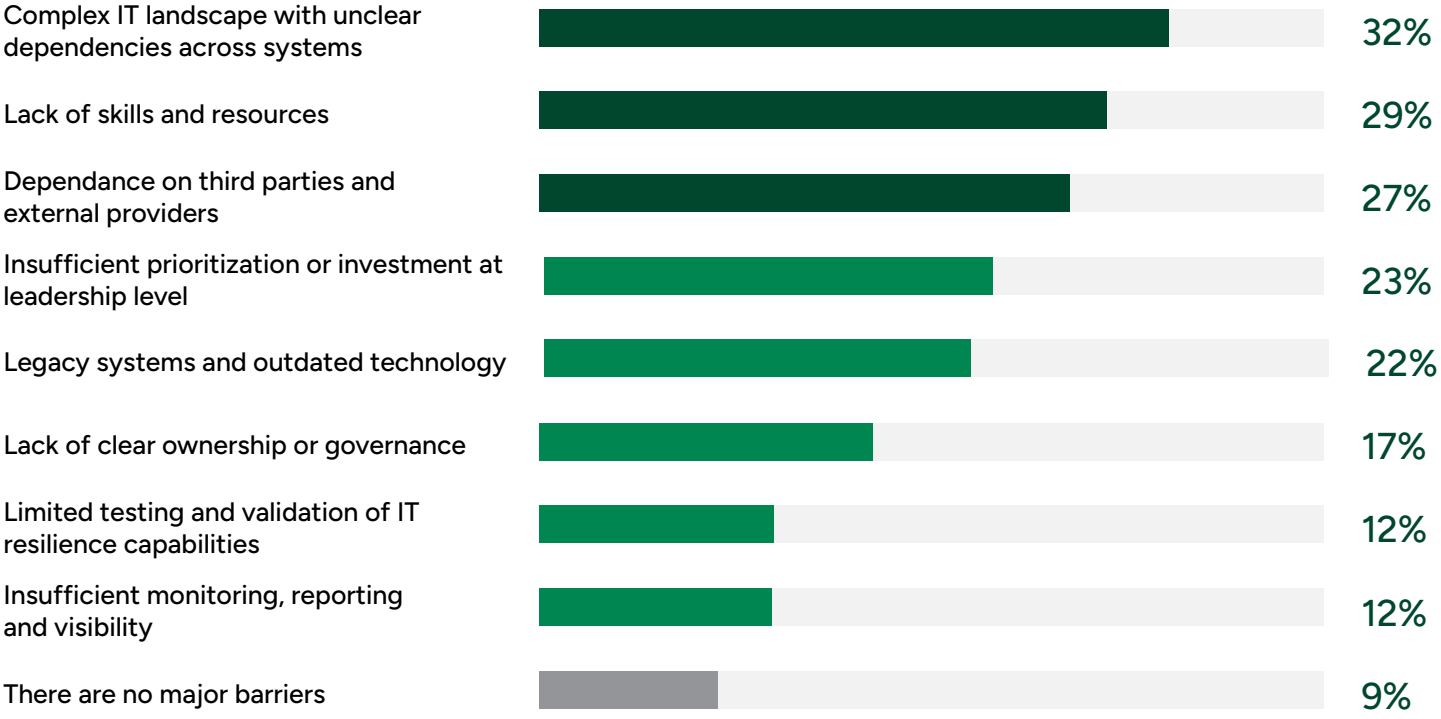
The main barriers are complexity, capacity and priorities.

The most common barrier is a complex IT landscape with unclear dependencies across systems (32%), followed by a lack of skills and resources (29%) and dependence on third parties and external providers (27%). Insufficient prioritization or investment at leadership level (23%) and legacy systems (22%) complete the top five.

Two of the five describe the technology estate. The other three describe people, leadership and dependence on others. Testing appears to be an underestimated barrier: only 12% identify it as a constraint, even though the readiness results show substantial gaps in end-to-end validation.

Complexity, skills and supplier dependence lead the list

Main barriers to full IT resilience, share selecting each (%, up to three options).
The three most common are shown in dark green.



Percentages sum to more than 100 because respondents could select up to three barriers.
Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

IT resilience is often owned below the level it depends on

The most critical IT resilience capabilities require executive authority, yet four in ten organizations place operational ownership below the executive level and 11% report no clear ownership.

Workforce readiness and crisis management are the capabilities leaders most often identify as critical to resilience, each cited by 52% of respondents. Both depend on clear decision rights, executive authority and coordination across functions. Yet primary ownership of IT resilience and continuity most often sits in an IT or infrastructure function below the executive level (40%). The CEO owns it in 16% of organizations and the CIO or CISO in 28%, while 11% report no clear ownership at all.

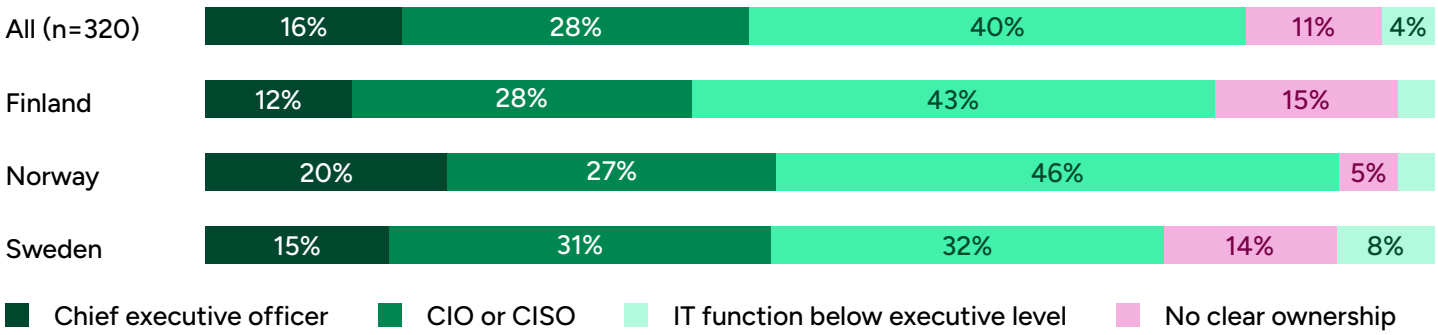
This creates a potential disconnect between the capabilities organizations consider most important and the level of authority required to drive them. While operational ownership can appropriately reside within IT, infrastructure, security or continuity teams, resilience increasingly depends on decisions that span the entire organization. Regulatory frameworks such as NIS2 further reinforce the role of leadership by making boards and executives accountable for overseeing cybersecurity risk management and ensuring that appropriate resilience measures are in place, monitored and continuously improved.

Ownership patterns also differ by market. Norway stands out for having the clearest ownership structure, with only 5% reporting no clear owner. At the same time, responsibility is more frequently assigned below the executive level, suggesting a more operational approach to resilience governance. In Finland and Sweden, ownership is less clearly defined, with 15% and 14% respectively reporting no clear owner.

As IT resilience becomes increasingly tied to operational continuity, customer trust and business performance, organizations need both clear operational ownership and visible executive accountability. Workforce readiness, crisis management and resilience governance cannot succeed without leadership engagement. While operational teams perform much of the day-to-day work, accountability for preparedness, oversight and follow-up ultimately rests with executive leadership and the board.

Where primary ownership of IT resilience sits

Who has the primary ownership of IT resilience and continuity? Share of respondents (%), total and by market.



Executive-level ownership (CEO plus CIO or CISO) is 44% overall.

Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

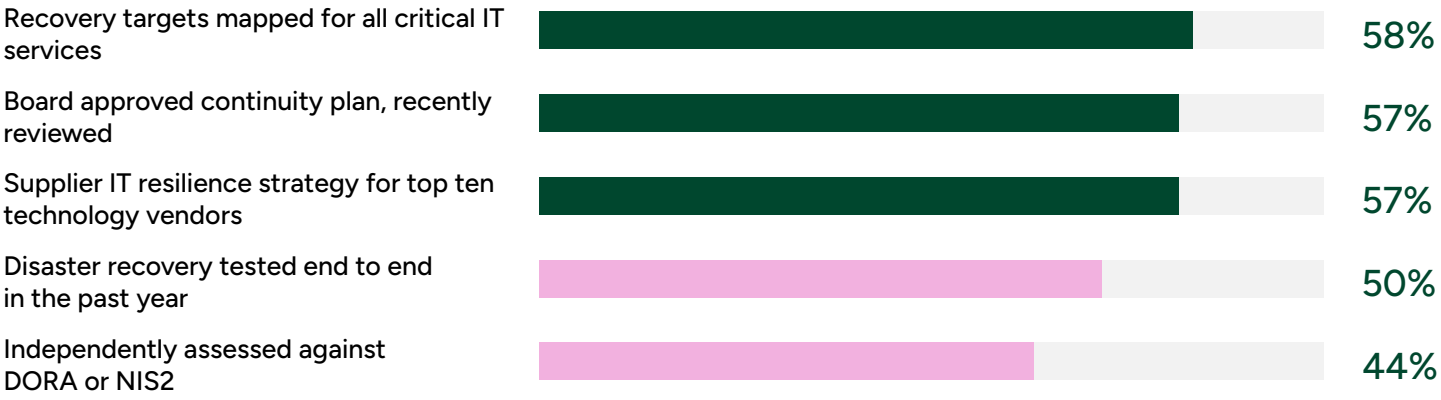
Many organizations have plans. Fewer can demonstrate readiness.

Between 44% and 58% of organizations meet each individual readiness criterion.

The survey assessed five fundamental indicators of operational readiness: a board-approved and recently reviewed continuity plan, an end-to-end disaster recovery test, formally defined recovery time objectives (RTOs) and recovery point objectives (RPOs), a supplier IT resilience strategy and an independent assessment against DORA or NIS2. RTO defines how quickly a service must be restored, while RPO determines the acceptable level of data loss. The results reveal a consistent pattern: controls that can be documented score highest, while measures that require validation through testing, assessment and operational proof score significantly lower.

Documentation outpaces demonstration

Share answering yes to each readiness question (%). The two validation-based checks are shown in pink.



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

Readiness is a spectrum, not a standard

Only three in ten organizations demonstrate high IT resilience across five key readiness dimensions.

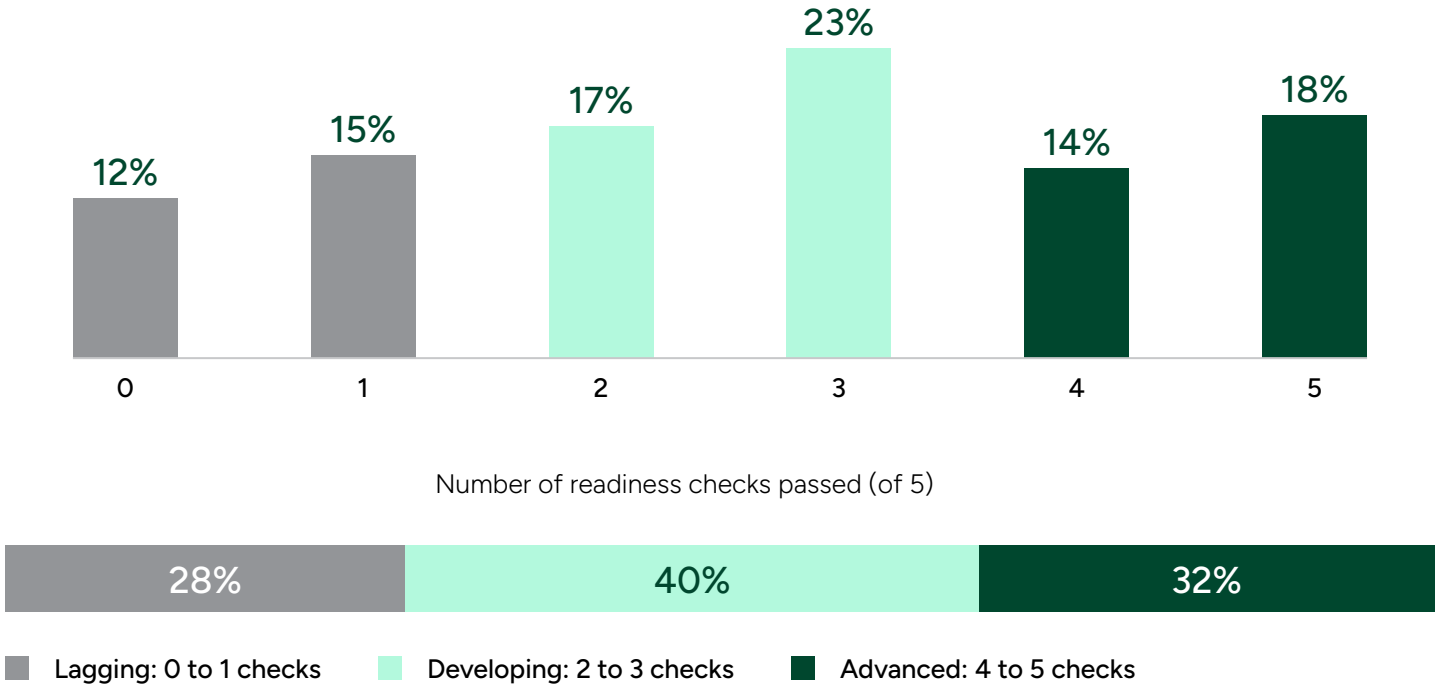
Readiness is rarely all or nothing. While 12% of organizations meet none of the five readiness criteria, only 18% meet all five. The largest group, representing 23%, meets three criteria, indicating that many organizations have laid the foundations for resilience but have yet to fully validate their capabilities.

This places most Nordic organizations in the developing stage of maturity, with relatively few reaching either end of the spectrum.

Finland stands out as the most mature market in the study. Nearly half of Finnish organizations (46%) demonstrate advanced readiness across the five resilience dimensions, while only 16% fall into the lagging category. In Sweden and Norway, around one-third of organizations are classified as lagging. This stronger readiness profile is reflected in the higher confidence reported by Finnish leaders.

How many readiness checks do organizations pass?

Share of organizations by number of yes answers across the five readiness checks listed in the previous chapter (%).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

Organizations test internally more than they test with their suppliers

Continuity increasingly depends on others.

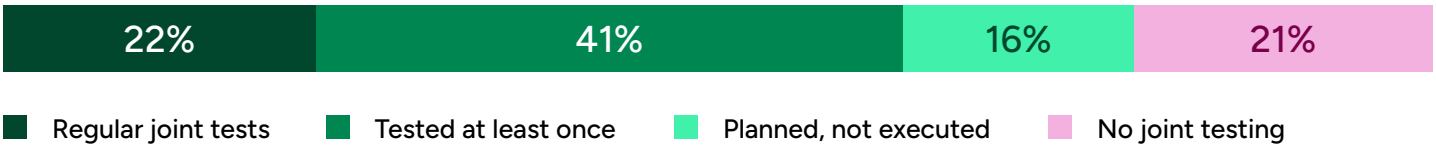
Internal testing has become routine. 68% of organizations test their ability to maintain or recover critical services at least once a year, and 16% do so every quarter. Testing with suppliers is a different story: only 22% run joint continuity tests regularly, 41% have done so once and 21% have never done so.

Internal testing is considerably more established than supplier testing

How often does your organization test its capability to maintain or recover critical services? Share of respondents (%).



Has your organization tested end-to-end continuity together with critical suppliers? Share of respondents (%).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

Dependency on suppliers is one of the barriers leaders cite most frequently, as highlighted earlier in this report. Yet one of the most effective ways to reduce that risk remains uncommon: joint resilience testing with suppliers. As organizations increasingly operate within interconnected ecosystems, IT resilience can no longer stop at the organizational boundary. Resilience must also be validated across critical partners and suppliers.

The differences between markets are significant. Finland appears to have made joint testing with suppliers a regular practice, while in Sweden more than one-third of organizations (34%) report never having conducted a joint resilience exercise with key suppliers.

Finland tests with suppliers. Sweden mostly does not.

Joint continuity testing with critical suppliers by market (%).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.



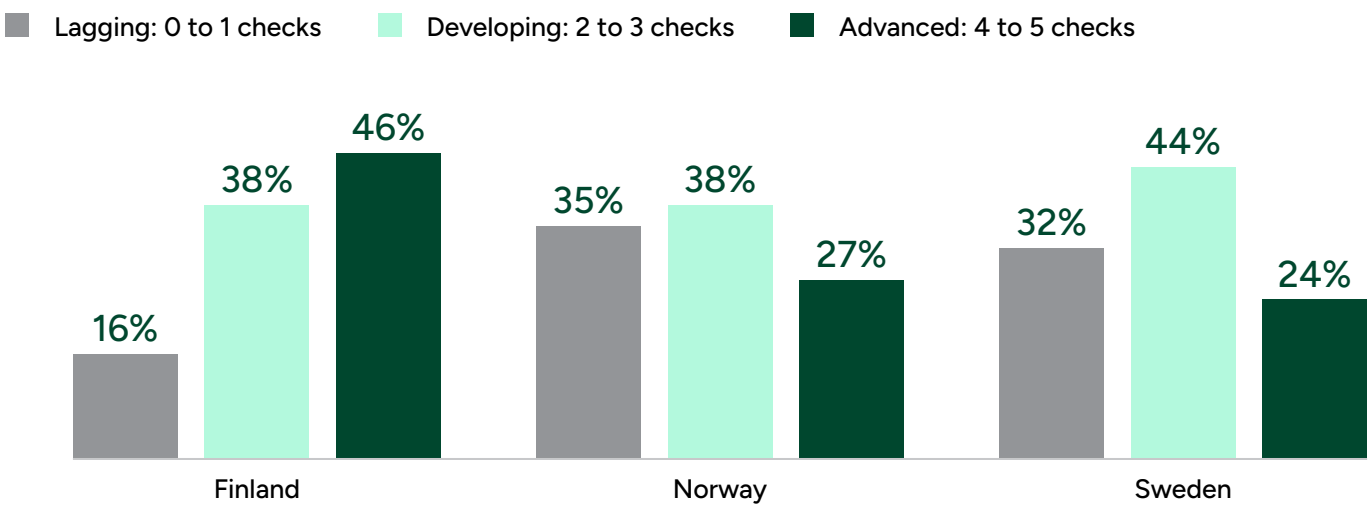
Finland leads the Nordics in IT resilience readiness

What readiness looks like in practice.

The higher confidence reported by Finnish leaders is consistent with the country's stronger resilience maturity profile. The difference is not that Finnish organizations are investing more; the intent to increase investment is similar across the region (66% in Finland, 63% in Norway and 62% in Sweden). The difference lies in what Finnish organizations have done to be more ready to meet and operate under disruption.

Finland has the largest advanced group and the smallest lagging group

Share of organizations by readiness tier and market (%).



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

What Finland demonstrates is a pattern rather than a single practice. Clear recovery targets give continuity plans something concrete to test against. Board approval gives them authority. Independent assessment creates external pressure to keep the plans current. And joint testing extends all of that to the supplier ecosystem. None of these is unusual on its own. The combination is. In general, organizations that perform best combine governance, testing, recovery planning, supplier validation and executive attention into one systematic capability.

The next page compares these practices market by market.

Three markets, three readiness profiles

Finland leads in resilience planning and testing. Norway leads in response and recovery readiness. Sweden has some gaps to close, but its resilience investment ambitions are on par with Nordic peers.

Readiness practices by market

Share of organizations by market (%). The strongest market on each measure is highlighted.

Measure	Finland	Norway	Sweden
Board-approved continuity plan, reviewed in last 12 months	69%	50%	53%
Disaster recovery tested end-to-end in the past year	56%	52%	41%
Recovery time and recovery point objectives mapped	79%	45%	50%
Supplier IT resilience strategy for top ten technology vendors	59%	55%	57%
Independently assessed against DORA or NIS2	56%	34%	44%
Minimum Viable Company defined and tested	19%	24%	10%

Source: Vivicta Nordic IT Resilience Survey 2026, n=320.



Finland

Leads on five of the six measures, with the widest gap on recovery targets and regulatory assessment.



Norway

Leads on one: the share with a tested Minimum Viable Company. Close to Finland on disaster recovery testing.



Sweden

Trails on most measures and has the lowest share with a tested Minimum Viable Company, despite similar investment ambition.

IT resilience takes different paths across the Nordics

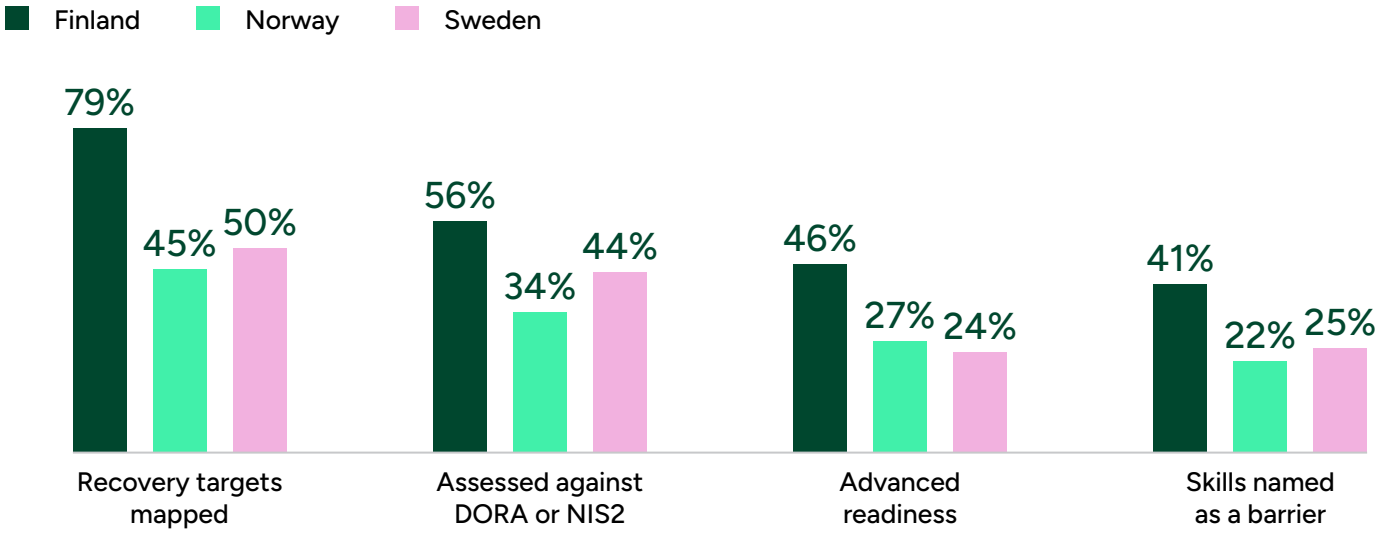
Finland leads in readiness, Norway in operational practice, while Sweden's investment ambitions outpace current readiness maturity.

Finland leads on readiness, yet skills and resources remain its biggest barrier (41%). Only 7% of Finnish leaders point to limited testing and validation as a concern, indicating that the challenge is less about resilience processes and more about maintaining the capacity and expertise to sustain them.

This may indicate that mature organizations not only have better visibility into the capabilities required to sustain resilience, but also leadership teams that recognize BCP as a strategic priority and consistently allocate the budget and resources needed to maintain readiness over time.

Finland leads on readiness and reports the largest skills gap

Share of organizations by market (%). Skills is the share naming a lack of skills and resources as a main barrier.



Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

Key insights: Norway

Norway's relative strength lies in selected forms of rehearsal, particularly Minimum Viable Company testing. It shows what continuity looks like when it is practiced rather than just documented. Its opportunity is the reverse of Finland's: to write down recovery targets and seek independent validation of what they already do.

Key insights: Sweden

Swedish respondents report some of the clearest readiness gaps. 11% say they have never tested disaster recovery, against 2% in Finland, and 28% see IT resilience mainly as a business risk, more than in any other market. This may indicate a disconnect between risk framing and operational rehearsal, although the survey does not establish causality.

What IT resilience leaders do differently

Five shifts will separate the leaders from the rest.

The survey points to five shifts that separate organizations moving ahead from those standing still. All five require leadership attention, and each can be initiated immediately.

Five shifts from recovery to readiness

Directional shifts drawn from the survey findings.

From	To	What it looks like in practice
Reactive recovery	Proactive preparedness	Scenarios are rehearsed before they happen, not reconstructed afterwards.
Technology protection	Business continuity	The true measure of IT resilience is the business service, not the individual system.
Internal IT resilience	Ecosystem IT resilience	Suppliers and partners are tested, not just contracted.
Plans on paper	Continuous validation	Testing and exercises become a recurring operating rhythm.
Operational ownership	Executive accountability	A named executive owns the outcome and holds the mandate.

Combined, the shifts describe a different relationship with disruption. Instead of treating an incident as an exception to recover from, leaders treat it as a scenario to be rehearsed. Instead of asking whether a system is protected, they ask whether a service is available to the customer, even when a supplier, a platform or a team is not.

Regulation will keep pushing in the same direction. 18% of respondents expect major impact from the EU Critical Entities Resilience Directive (CER), and independent assessment against DORA or NIS2 is already a benchmark. Organizations that treat these frameworks as a baseline and build their own testing rhythm above it will be better placed than those who prepare for each audit separately.

Source: Vivicta Nordic IT Resilience Survey 2026, n=320.

CONCLUSIONS

Five takeaways for Nordic leaders

Five priorities for leaders who want to strengthen their organization's readiness.

1. Prioritize evidence and readiness over confidence

Confidence is a feeling. Readiness is a record. Ask for concrete evidence: when did we last test, what did we learn and what changed as a result?

2. Build IT resilience around people and leadership

Invest in workforce readiness, crisis structures and decision rights alongside tooling. Rehearse the human parts of the response.

3. Make suppliers part of your IT resilience strategy

Identify the suppliers your critical services depend on, and plan joint exercises with them. Start with the suppliers that support your most critical services.

4. Validate continuously through testing

Move from isolated annual exercises to a risk-based testing rhythm combining targeted tests with periodic end-to-end exercises.

5. Establish executive accountability

Name an executive owner with a cross-functional mandate. Ensure the board sees readiness evidence, not only plans.

QUESTIONS FOR YOUR NEXT LEADERSHIP MEETING

- In general, how confident are you that you can maintain or recover critical services during a major disruption?
- Which of our critical services have never been tested end-to-end?
- Who can approve a business trade-off in the first hour of a major incident?
- When did we last run a joint exercise with the supplier we could least afford to lose?

THE VIVICTA PERSPECTIVE

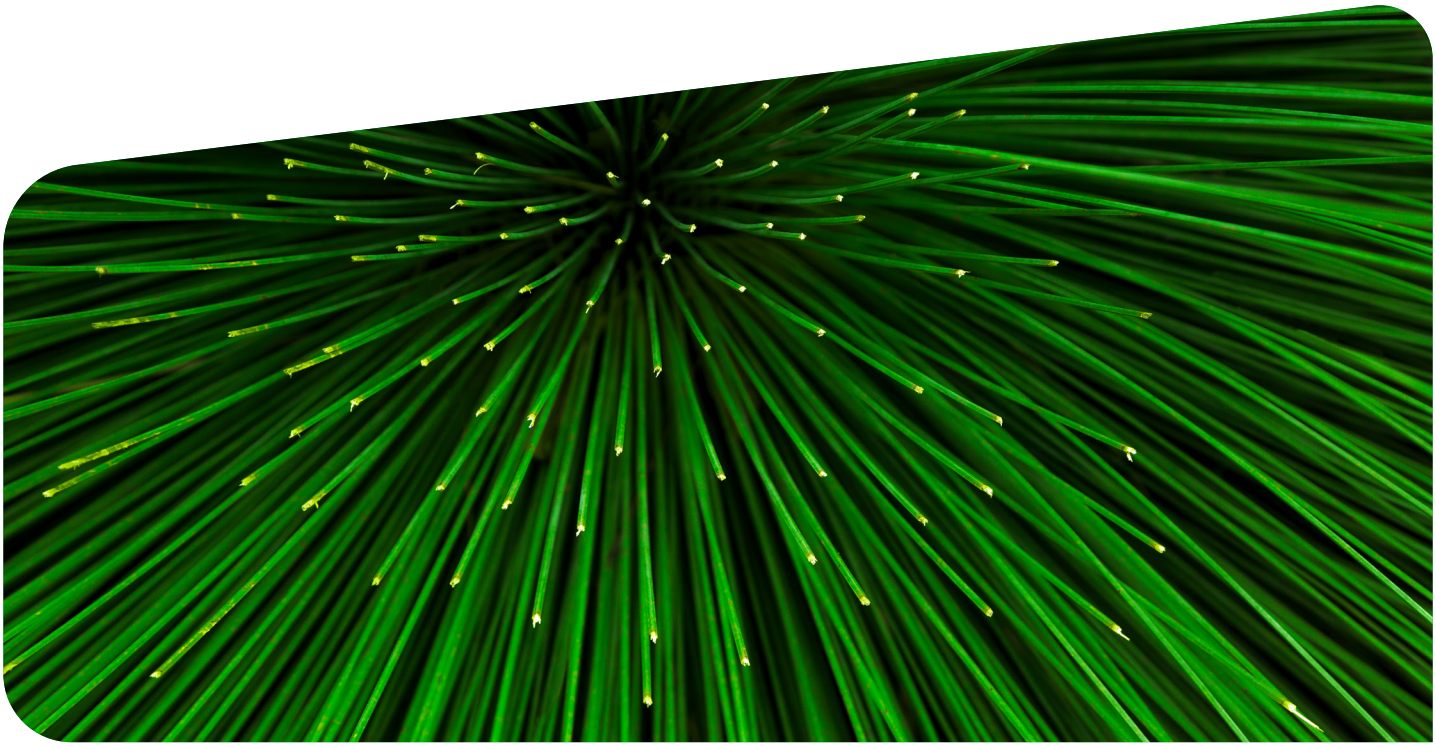
Readiness is a leadership discipline built through practice

Nordic leaders have ambition. The next step is turning that ambition into evidence.

The findings in this report point in one direction. What separates the leaders is how systematically they prepare: how clearly they define what must keep running, how often they test it, how far their testing reaches into the supplier ecosystem and how directly executives are accountable for the result.

We believe that IT resilience should be approached as an ongoing business capability rather than a project with an end date. That means starting from the services customers depend on, making ownership explicit, building the skills and crisis structures that decide the first hours of an incident and extending testing beyond the organizational boundary. It also means using regulation as a baseline to build from rather than a deadline to meet.

The Nordic markets can learn a great deal from one another. Finland shows what systematic governance looks like. Norway shows the value of rehearsal. Sweden shows how candid self-assessment can be the first step toward change. Together, these point to a Nordic standard of readiness that is within reach.



THE VIVICTA PERSPECTIVE

Strengthening continuity, control and resilience

Organizations today face a growing range of disruptions, from cyberattacks and technology failures to supplier dependencies, regulatory demands, geopolitical uncertainty and increasing digital dependence. Business continuity is therefore no longer only an operational concern, but a leadership responsibility. The challenge is not only to withstand disruption, but to ensure that critical business services can continue and recover when incidents occur.

This is also central to Vivicta's approach to digital sovereignty. For Vivicta, sovereignty means maintaining control over critical services, data and technology, strengthening resilience, and retaining the freedom to adapt, recover or change providers as circumstances evolve. IT resilience and business continuity provide the operational foundation that turns digital sovereignty from principle into practice.

The Vivicta IT Resilience & Business Continuity Framework helps organizations move from plans and policies to measurable operational readiness across five interconnected areas, addressing key gaps identified in the report:



IT Operational Continuity helps organizations define, test and validate recovery targets and continuity capabilities.



Cyber Resilience strengthens preparedness for cyber incidents and other disruption scenarios that threaten business operations.



Compliance & Governance establishes clear ownership, accountability and structured assessments to support regulatory requirements.



Organizational Resilience develops crisis management capabilities, decision-making structures and workforce readiness.



Ecosystem Resilience improves visibility into critical supplier dependencies and strengthens third-party continuity preparedness through assessment and testing.

Through advisory, implementation, testing and managed services, Vivicta helps organizations identify critical dependencies, strengthen readiness and validate resilience. As part of our digital sovereignty approach, we help customers strengthen control, recover faster and preserve freedom of action as technology, suppliers and circumstances change.

How does your organization compare? Vivicta can help you assess readiness, identify critical gaps and turn continuity plans into tested operational capability.

ABOUT THE STUDY

Who we asked, and how

The Nordic IT Resilience Survey was conducted by Kairos Future for Vivicta in June and July 2026. The results are shown as shares of all respondents (n=320), and market and organization size differences are shown only where they help explain the picture.

Geography:

Finland (n=108), Norway (n=107) and Sweden (n=105).

Organization size:

500 or more employees. The sample includes 82 organizations with 500-999 employees, 177 with 1,000-9,999 employees and 61 with 10,000 or more.

Role in IT decisions:

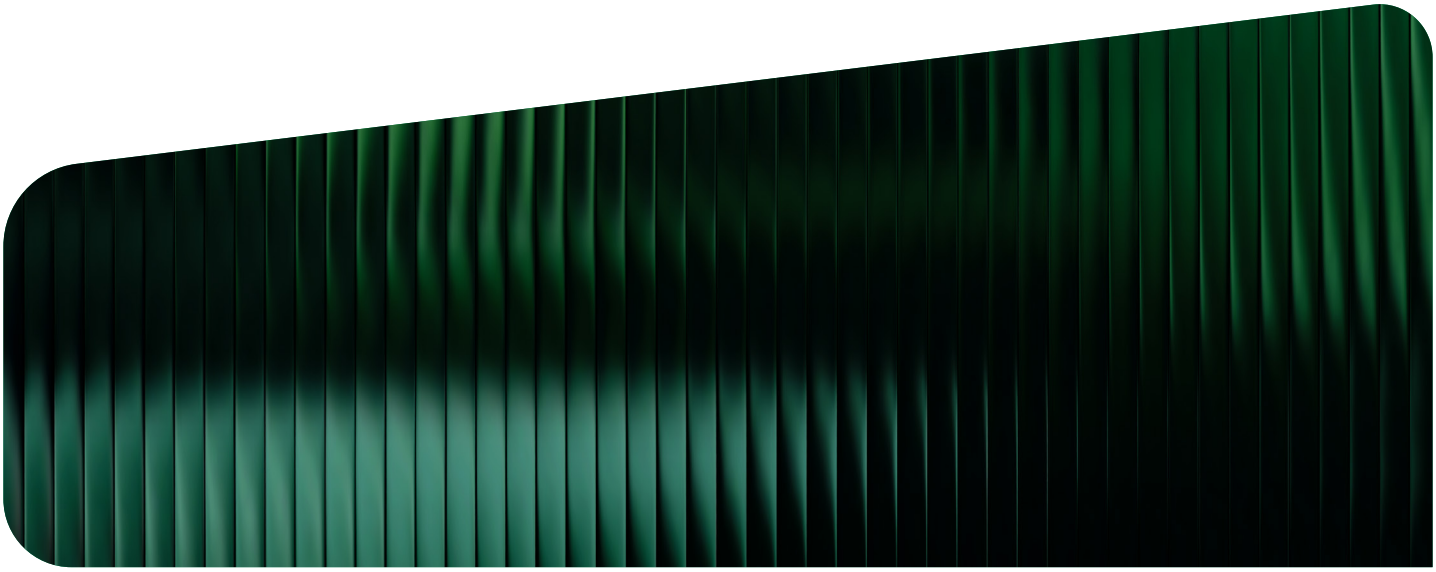
17% had final decision-making authority and 83% acted as key influencers or advisers on IT, AI, data governance or sovereignty decisions.

How to read the results

Unless otherwise noted, figures reflect the full sample of 320 respondents. Several questions allowed up to three selections, so totals within a question do not sum to 100%. Confidence figures combine ratings of six and seven on a seven-point scale. Smaller subgroups should be interpreted with care. Market characterizations in this paper reflect patterns across multiple survey questions rather than a single measured figure.

Sample composition

65% of respondents (n=207) work in organizations classified as critical sectors. The remaining 35% (n=113) work in non-critical sectors. Critical sectors were classified with reference to Finland's National Emergency Supply Agency framework and adapted to the industry categories represented in the survey.



About Vivicta

Vivicta is a trusted Nordic transformation partner making everyday easier through technology. With more than 7,000 experts globally, Vivicta works across Data, Automation & AI, Cloud & Infrastructure, ERP & Applications and Digital Security to help customers unlock new digital opportunities and accelerate transformation.
www.vivicta.com