CIO ANALYTICS

NORTHERN EUROPE'S LARGEST REPORT FOR IT DECISION-MAKERS

18%
has created substantial value with AI.

76%
do not practice their security plans regularly.

2026

No. 1
challenge for IT decision-makers: resources.

IN-DEPTH INTERVIEWS

16
Statens IT:
Preparedness in a World Without a Script.

22
LTG Group:
Bringing AI Into Rail Transformation.

34
Green Mountain:
When Data Center Growth Drives IT Investment.

Do you have any questions about the report? Get in touch at contact@cioanalytics.com

Page #

Contents

About the report
CIO Analytics is an annual, data-driven survey designed to capture the priorities, challenges, and strategic direction of today's IT decision-makers. First launched in Sweden in 2018, the survey has evolved into one of the most comprehensive studies of IT leadership in Northern Europe.

In 2024, the scope was expanded beyond Sweden to include Norway, Denmark, Finland, Estonia, Latvia, and Lithuania (referred to throughout the report as Northern Europe), providing a broader regional perspective. The survey targets CIOs and IT decision-makers across both the public and the private sectors.

The 2026 edition is based on 1,478 responses, with 59 per cent from the private sector and 41 per cent from the public sector, offering a robust foundation for benchmarking, trend analysis, and strategic insight.

Data and charts in this report are based on the survey responses. For clarity and consistency, some questions and response options have been slightly adapted, while preserving the original intent and meaning.

The report is issued by Atea ASA, the leading supplier of IT infrastructure in the Nordic and Baltic regions.

The New Era of IT Decision-Making

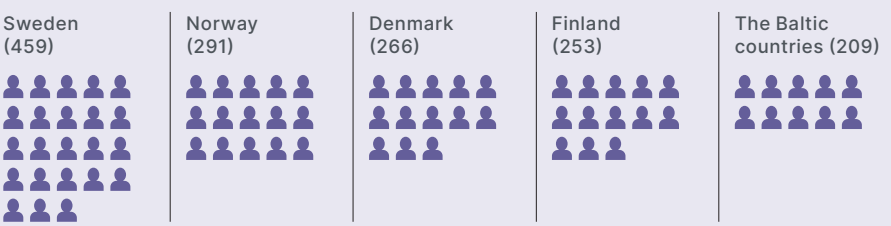
The everyday life of an IT decision-maker is multifaceted, with many difficult tasks, balancing mandatory responsibilities with aspirational goals. The role requires both technical expertise and strategic thinking. Decisions must be made while multiple demands compete for attention under continuous pressure.

This report is based on a comprehensive survey involving nearly 1,500 IT decision-makers across Northern Europe, providing you with in-depth insights into the prevailing priorities, challenges, and strategies. It highlights the most critical issues for IT decision-makers today and outlines the essential conditions for effective modern IT leadership, guiding you on how to succeed in today's dynamic environment. It is an invaluable tool for benchmarking your own IT operations, understanding trends in security and innovation, and making data-driven strategic decisions.

Through the report, you can compare your organization with other similar businesses, understand the data, and see where you stand on issues such as AI, security, and resources.

A noticeable shift towards proactive engagement in organizational strategies is emerging. To sustain this shift, it is crucial to establish strong governance, clearly defined investment priorities, and articulate leadership expectations. IT decision-makers also face challenges in resource allocation, requiring clearer prioritization and explicit trade-offs. As AI evolves, organizations should prioritize aligning AI capabilities with tangible business value and growth rather than just experimenting. This report makes you better at understanding how technology impacts business strategies and provides you with the tools and knowledge that you need for your on-going journey.

→ Response distribution by country, out of a total of 1,478 IT decision-makers in Sweden, Norway, Denmark, Finland, and the Baltic countries.



1 figure = 20 respondents, rounded to nearest 20.

CHAPTER

1

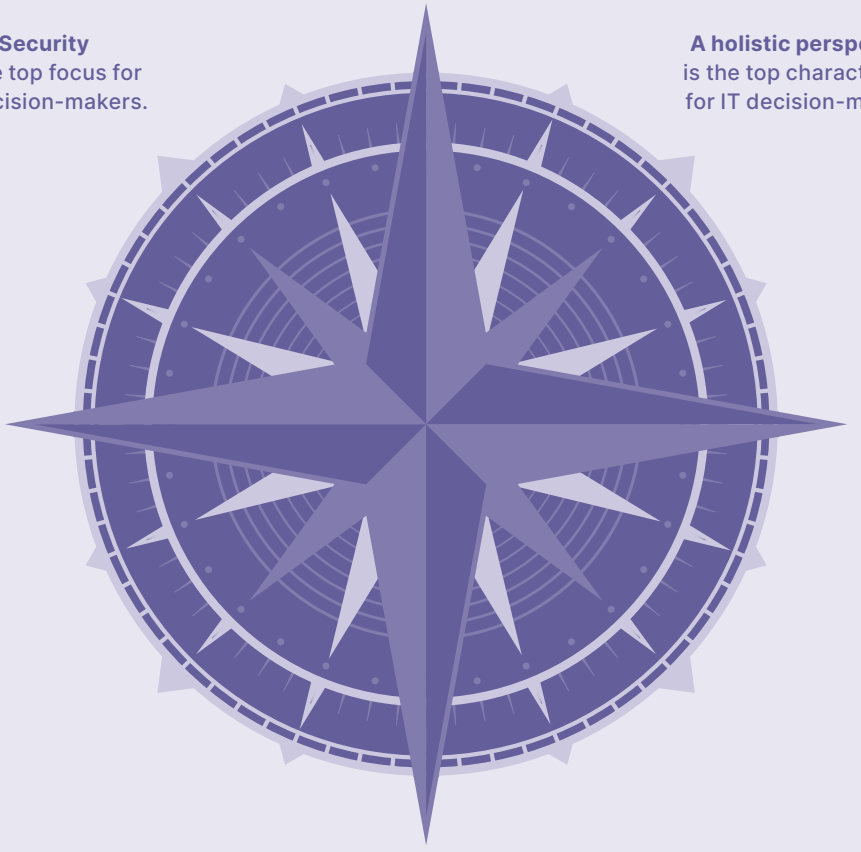
Navigating IT Leadership in a Rapidly Changing World

IT leadership today is defined by constant trade-offs. This chapter explores how IT decision-makers navigate their role, what underpins sound decisions, where attention is currently focused, how ambition is evolving, and which challenges place the greatest strain on day-to-day leadership.

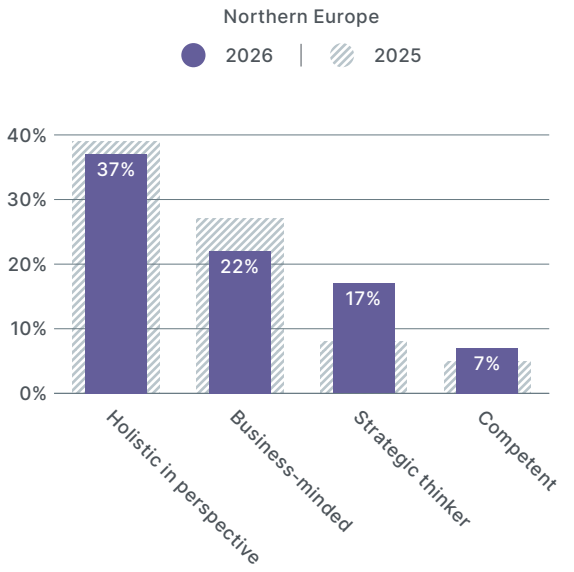
Resources
are the top challenge for
IT decision-makers.

Security
is the top focus for
IT decision-makers.

A holistic perspective
is the top characteristic
for IT decision-makers.



What do you think is the main characteristic of a good IT decision-maker?



The Modern IT Decision-Maker Sees the Whole Picture

A good IT decision-maker is defined first and foremost by the ability to see the whole picture. Leaders across Northern Europe point to a holistic perspective as the single most important characteristic, reflecting a role that now spans far beyond technology choices. A holistic mindset means understanding how decisions ripple across operations, cost, risk, people, and long-term outcomes. It also means recognizing that IT is no longer a support function, but is rather a structural driver of organizational direction.

Strategic thinking has grown sharply in importance. The role is shifting from operational oversight toward long-term direction-setting, shaped by geopolitical uncertainty, rapid technological change, regulation, and the accelerating impact of AI. Strategic capability allows IT leaders to translate complexity into clarity and to give the organization a sense of direction when conditions are ambiguous.

A strong business mindset completes the profile. Effective IT decision-makers understand how technology enables growth, resilience, and value creation. They align choices with business goals and challenge assumptions when priorities drift.

These are the traits of a good IT decision-maker: holistic understanding, strategic capability, and business orientation form the core of modern IT leadership. Yet the role also demands courage, focus, and decisiveness. IT leaders often act with incomplete information, make tough tradeoffs, and create focus in environments where expectations exceed resources. The business increasingly looks to IT for leadership, not the other way around.

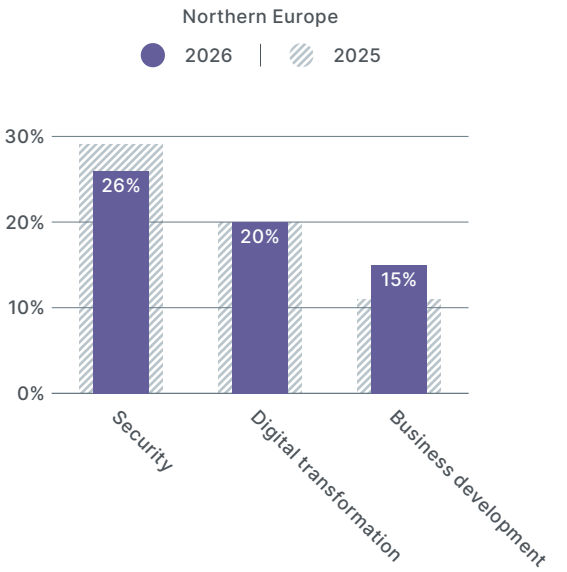
Main Takeaways

→ A holistic perspective is the defining trait because IT decisions shape the entire organization.

→ Strategic thinking is rising fast as IT leaders set long-term direction under conditions of uncertainty.

→ Business-minded leadership turns technology choices into real organizational value.

What is currently your primary focus in your role as an IT decision-maker?



Operational Pressure Keeps Security in First Place

Main Takeaways

→ The focus on security has decreased but still leads by a clear margin.

→ Transformation ambitions stall when operational demands increase.

→ Leadership clarity determines whether IT stays reactive or moves toward value creation.

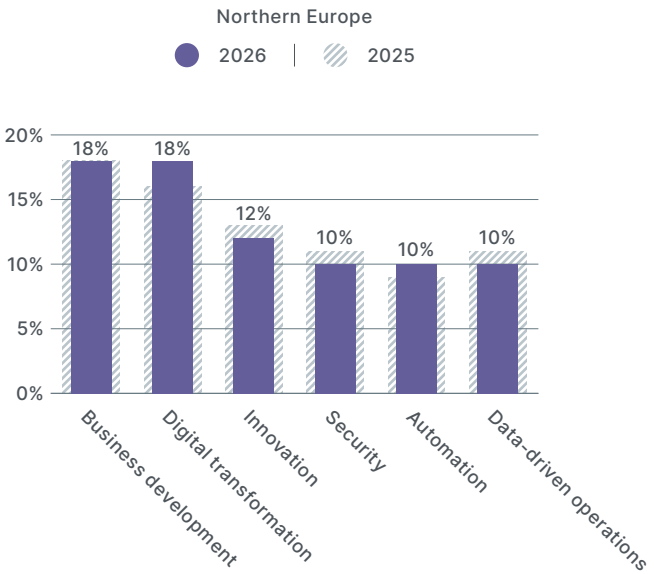
Security remains the primary focus for IT decision-makers in Northern Europe, even though its dominance has weakened slightly. Last year, 29 percent chose security as their top focus, compared with 26 percent this year. The decline signals a small shift, yet security still attracts more attention than any other area. Leaders describe it as mandatory work shaped by regulation, increasing threats, and expectations for operational stability. Security continues to consume substantial time and resources, even though it is not where the most value is believed to be created.

Digital transformation remains a strategic priority, but it often competes for space with operational obligations. When new security demands arise, transformation slows. Many see this as a recurring pattern: progress is possible, but rarely continuous.

Business development ranks third as a current focus, yet it is the area where more leaders wish they could spend their time. Capacity limitations and skill shortages make it difficult to shift from reactive tasks to value-creating initiatives. The gap between current and desired focus remains one of the clearest tensions in the IT decision-maker role. Read more on page 7.

Organizational maturity shapes these dynamics. Smaller organizations concentrate on survival and compliance. Larger or more mature organizations have more room to invest in transformation and business development. Clearer leadership direction also plays a crucial part. Where mandates are strong, focus shifts toward long-term value. Where they are unclear, IT remains in reactive mode.

What would you like to focus more on in your role as an IT decision-maker?



Ambition Points Toward Transformation, Not Obligation

IT decision-makers in Northern Europe express a clear desire to shift their focus away from mandatory operational tasks and toward work that creates long-term business value. While security, compliance, and operational stability dominate their current agenda, these areas do not reflect where they want to invest more of their time. The ambition revolves around business development, digital transformation, and innovation. The top two areas that respondents want to focus on the most have both been highlighted by 18 percent.

The gap between current and desired focus is driven by limited capacity and an unclear mandate, rather than a lack of willingness. IT decision-makers say external pressure, resource constraints, and increasing regulatory demands prevent them from contributing more directly to organizational growth and competitiveness.

Many want to move closer to the business and become proactive partners in shaping strategy, rather than solely maintaining operations. They highlight the need to work on initiatives that drive efficiency and measurable impact. Innovation and automation also play a central role in their ambitions. IT decision-makers see these as critical tools to reduce manual workload, address skill shortages, and free up time for more strategic activities.

There is also a strong wish to scale AI initiatives beyond pilots to deliver tangible value. More room for leadership is another recurring theme: to set direction, make tradeoffs, and guide priorities rather than react to short-term challenges. Ultimately, IT decision-makers wish for a shift away from reactively solving acute situations to a more proactive, future-oriented development.

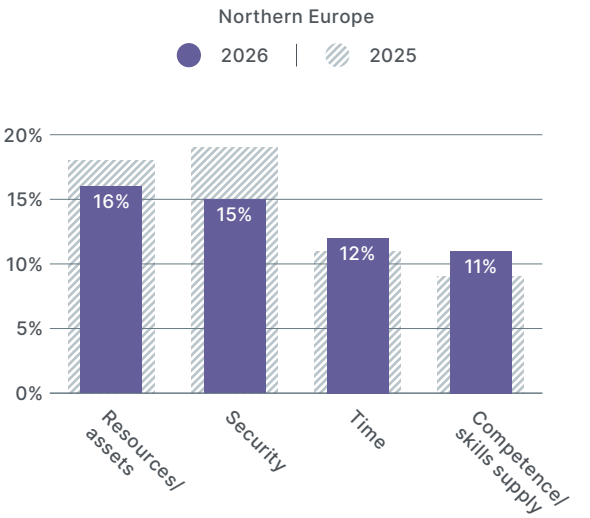
Main Takeaways

→ IT decision-makers want to shift focus from operational obligations toward business development and transformation.

→ Limited capacity, not lack of ambition, blocks progress toward strategic work.

→ IT decision-makers aim to use innovation, automation, and AI to create measurable business value.

What is your IT organization's biggest challenge?



The Growing Strain Behind IT's Daily Work

Main Takeaways

→ Resources and assets limit the IT organization's ability to respond, develop, and prioritize.

→ Security continues to shape daily work and preparations for deeper structural challenges.

→ Time pressure, competence gaps, and rising costs reinforce a cycle that slows strategic progress.

Resources and assets stand out as the most critical challenge facing IT organizations in Northern Europe. IT decision-makers describe an environment where capacity is stretched thin, and foundational elements of IT delivery require more attention than the organization can supply. This lack of available resources slows development and forces difficult prioritization long before strategic work begins.

Security follows closely and remains a defining pressure point. Even though its prominence is declining over time, it continues to shape budgets, governance, and the operational rhythm. Read more about IT spending on page 30. Regulatory demands, compliance work, and persistent cyber threats absorb substantial focus. This sets the stage for the next chapter, where security maturity and structural weaknesses become central to understanding IT's reality.

Time constraints amplify the pressure. Mandatory work leaves little room for long-term planning or proactive development. IT decision-makers report a constant struggle to carve out time for transformation amid operational demands.

Competence shortages contribute to the challenge, especially in advanced roles, yet they are secondary to the broader lack of capacity and time.

Rising costs deepen the uncertainty. Hardware, cloud services, and AI-related infrastructure costs continue to grow more unpredictable, making planning difficult and reducing flexibility in investment decisions.

Bridging Art and Technology Inspires the CIO of the European Capital of Culture 2026, Oulu

Tapio Matinmikko, Chief Information Officer of the City of Oulu, is a passionate innovator who would like to spend more time on rapid experimentation. The Capital of Culture year, and visual art in particular, have brought new perspectives to the role of technology.

In the public sector, Information and Communication Technology (ICT) solutions must work for everyone. Even amidst the reforms, it is essential to ensure that daily operations run smoothly: the functionality of ICT services, data security and the adequacy of resources must be guaranteed. The challenge for the CIO is that information technology is expected to be both a facilitator of operational development and a source of savings.

"Even if the future is uncertain, it is important to get started and be ready to change direction, when necessary."

Tapio Matinmikko, Chief Information Officer, City of Oulu.

"Even if the future is uncertain, it is important to get started and be ready to change direction, when necessary. You can't wait for perfect information; you have to move agilely," says Tapio Matinmikko.

Matinmikko is responsible for the city's ICT services, the promotion of digitalization and key areas of information management, such as cybersecurity and the ICT budget, and cooperates with companies and research institutions.

"This job requires experience, but also humble listening to others. One must be able to move forward, but at the same time accept that the original plan may not work. Then, we just have to change direction."

According to Matinmikko, the most important quality of a good CIO is the capability to renew the city's service production and the efficiency of internal processes together with the city's management. It requires interaction and the ability to understand the big picture. The City of Oulu focuses on bringing new technologies into the everyday life of the city's residents and employees in a controlled manner.

"The key is to support administration branches in promoting digitalization and utilizing new technologies. AI is one typical example of this."

Development is Matinmikko's personal passion. He would like to spend more time experimenting.

"When something concrete and visible is created, you can see that the work makes a difference. By piloting, one learns about the utilization of technology and its impact on operations as well as the risks. It quickly becomes clear which matters should be taken forward."

The City of Oulu's eventful Capital of Culture year has opened up new perspectives for the CIO on the use of technology.

"It's fascinating how technology has become part of art. We have several exhibitions where some of the works have been implemented using immersive technology. The number of events in the City of Oulu has increased in general and we have made high-quality AV implementations in them."

Matinmikko believes that the role of CIOs will become even more important in the future as the importance of technology increases and new solutions are constantly introduced to the market.

"Even though technology develops, people are always people. We experience things in the same way as before, and we are all different. It must be taken into account in everything we do."

CHAPTER

2

Adapting to the Present While Preparing for Tomorrow

Security maturity is revealed in day-to-day practice, not policy. This chapter examines how organizations manage security in reality, capturing current maturity, daily challenges, real incidents, and adaptation to an evolving threat landscape, while exposing how prepared IT organizations truly are for disruption and the unexpected.

No. 1

biggest security challenge: a fragmented IT landscape.

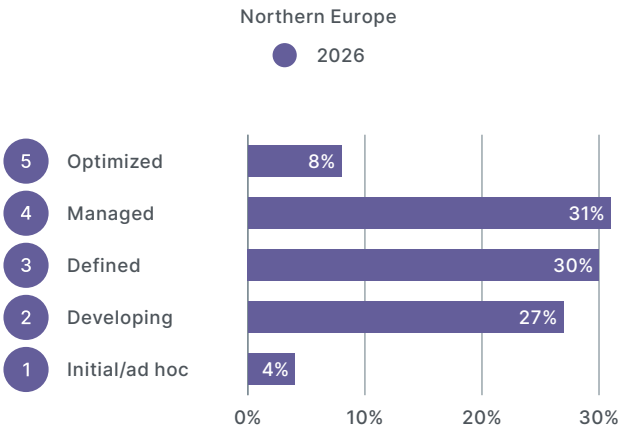
73%

have invested in increased employee training and security awareness.

76%

do not practice their plans regularly.

How do you rate your organization's security maturity?



Higher Maturity Reveals More Risk – and Drives More Action

Security maturity in Northern Europe is concentrated in the middle levels, with most organizations rating themselves as "Defined" or "Managed." This reflects a structured approach to security, but the data shows that rising maturity increases visibility, not ease. As organizations advance, they identify more structural risks, including legacy systems, fragmented environments, and cultural gaps. These risks are often less apparent at lower maturity levels, where visibility is limited.

Higher maturity also aligns with stronger security behavior. More advanced organizations report greater adoption in the form of employee training, internal collaboration, and technical controls. They take more steps to adapt to the evolving threat landscape and tend to work in a more continuous and systematic way. The workload does not shrink with maturity; it becomes clearer where efforts are needed.

Cyberattack reporting reinforces this pattern. Higher-maturity organizations detect more events before they become incidents because they have better monitoring and broader situational awareness. Lower maturity organizations detect fewer events, which makes real exposure harder to understand. Maturity strengthens preparedness and reaction, not immunity. This is discussed further on page 13.

Regular practice is a defining characteristic of maturity. Organizations at the top levels rehearse their incident plans far more frequently, while lower-maturity organizations practice rarely. This demonstrates that maturity is an organizational discipline shaped by leadership, governance, and culture.

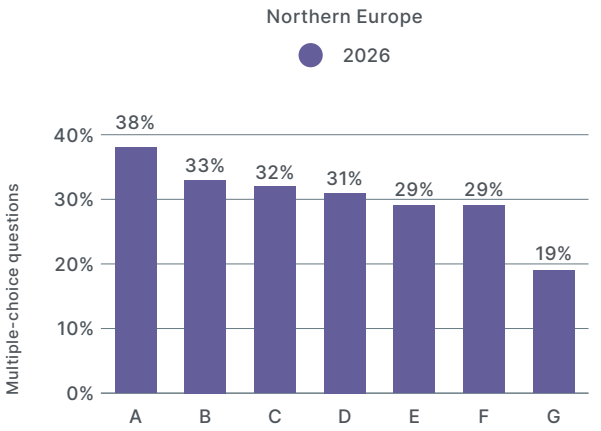
Main Takeaways

→ Organizations with a higher level of security maturity are better at identifying risks and thus realizing where action is needed.

→ Mature organizations detect more events before they become incidents because visibility improves, not because threats increase.

→ Regular practice and leadership ownership are the strongest indicators of real security maturity.

What are the primary challenges in your organization's security work?



Top challenge per security maturity level

Security maturity levels: 1. Initial/ad hoc – 2. Developing – 3. Defined – 4. Managed – 5. Optimized

A. Complex/fragmented IT environment
B. Regulatory or compliance requirements
C. Weak security culture
D. Legacy systems
E. Lack of in-house expertise
F. Insufficient budget/funding
G. Limited executive support/prioritization

Why Security Remains Harder Than It Should Be

Main Takeaways

→ Fragmented environments and legacy systems expose structural risks that tools alone cannot fix.

→ A weak security culture and compliance-driven work limit real resilience, even when investment is high.

→ In-house expertise and ownership remain essential as AI expands the threat surface.

Security work is increasingly shaped by structural barriers rather than individual incidents. The biggest challenge is the complexity of technical environments. Fragmented systems create isolated security controls and uneven visibility, making modern defense strategies difficult to implement. This forces IT decision-makers to prioritize consolidation and platformization over adding new tools.

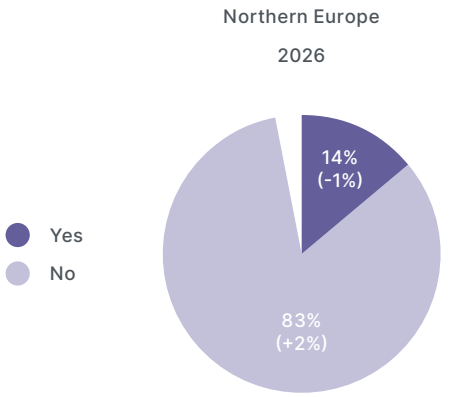
Regulatory pressure is a major driver. Many organizations are pushed into action by mandatory requirements rather than strategic intent. An approach with a strong focus on compliance increases costs but also enhances long-term resilience.

Security culture continues to be a fundamental challenge, especially for organizations with lower maturity levels. Without consistent behavior, training, and engagement across the workforce, technical investments cannot deliver their full value.

Legacy systems add another layer of risk. They are often difficult or costly to secure and appear as a more significant barrier among organizations with higher security maturity. This suggests that many underestimate the exposure hidden in older architectures. The gap between perceived readiness and actual vulnerability remains.

The lack of in-house security expertise further limits progress. While external partners can support execution, ownership must remain internal to avoid gaps in responsibility. As AI development accelerates both threats and operational complexity, gaps in governance and identity control become more visible. Public sector organizations struggle more with funding, while private sector actors face technical fragmentation.

Have you experienced any cyberattacks in the past 12 months with an impact on your organization?



Figures in brackets show the change compared with last year (percentage points).

Incidents Increase Activity, Not Immunity

Only a minority of organizations in Northern Europe have reported a cyberattack with operational impact in the past year. The data suggests that these incidents act as a catalyst for activity rather than a sign of poor security. Organizations that have experienced attacks tend to report more structural challenges, including fragmentation, regulatory pressure, weak culture, and legacy systems. An attack often forces issues to the surface that were already present but less visible.

However, increased activity after an incident does not automatically lead to lasting maturity. Many organizations update plans, revise processes, or practice responses following an attack, but the improvements are often short-term and reactive. True resilience requires sustained efforts well before an incident occurs.

Security maturity does not correlate with fewer impactful attacks. Highly mature organizations still report incidents, likely due to stronger detection capabilities and broader attack surfaces. Less mature organizations may simply detect fewer events, making "no incidents" an unreliable indicator of safety. Strong detection and monitoring are essential to understanding true exposure. Larger organizations experience more incidents, reflecting both complexity and higher visibility. Sweden stands out with higher reported rates, which may indicate stronger detection or stricter reporting practices.

Cyberattacks often highlight underlying weaknesses, especially in fragmented or legacy-heavy environments. Without strong internal ownership of security and clear continuity priorities, organizations risk becoming dependent on external partners during critical events. Preparedness must include AI-driven attack scenarios, as attackers increasingly use automation and identity-focused techniques at scale.

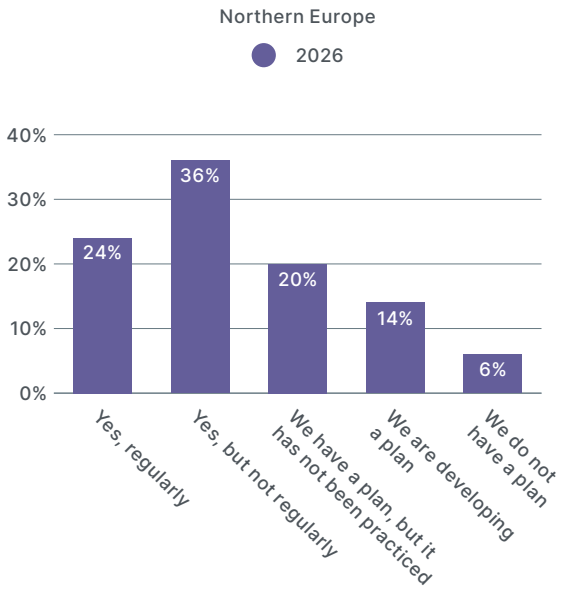
Main Takeaways

→ Cyberattacks expose structural weaknesses that remain hidden without strong detection.

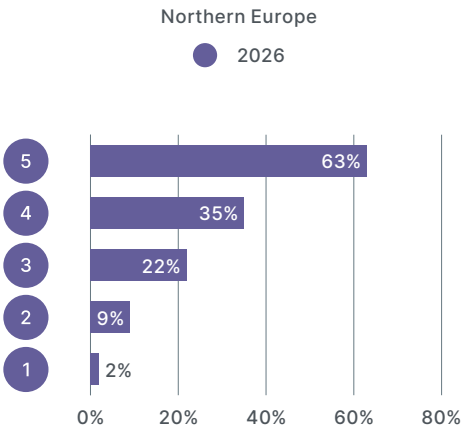
→ Increased activity after an incident signals reaction, not sustained maturity.

→ Organizations must prepare for AI-accelerated threats before an attack, not react afterward.

Have you practiced your organization's plan to deal with unforeseen events?



How many practice regularly per security maturity level?



Security maturity levels: 1. Initial/ad hoc – 2. Developing – 3. Defined – 4. Managed – 5. Optimized

Most Plans Remain Untested Until They Matter

Main Takeaways

→ A documented plan does not support real decisions until it is tested under pressure.

→ Exercises that focus only on external attacks leave important gaps in readiness.

→ Frequent practice is one of the clearest indicators of real preparedness.

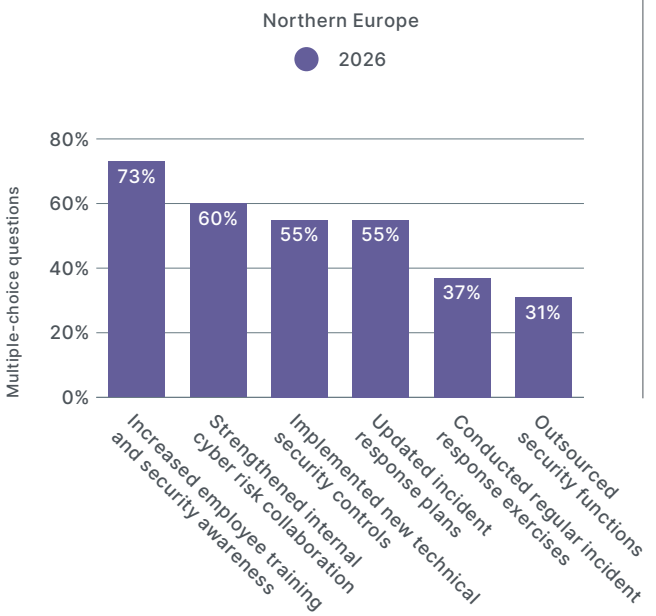
Security plan practice is uneven across Northern Europe. Only a quarter of organizations rehearse their incident response plans regularly. This means that many rely on plans that have not been tested in realistic conditions or have only been tested on a few occasions. A documented plan may outline responsibilities and actions, but without repeated practice, it cannot support timely decisions during high-pressure situations.

Current practice tends to emphasize external attacks. Scenarios involving ransomware, infrastructure breaches, or other outside threats dominate tabletop testing. Insider-related events are rarely included, even though these situations are harder to detect and require rapid assessment. This leaves a gap in readiness when incidents do not follow familiar patterns.

Effective practice must reflect business continuity. Technical response is only one aspect of handling an unforeseen event. Exercises need to cover how leaders prioritize critical services, how communication flows across the organization, and how recovery decisions are made when multiple functions are affected at once. External partners can support execution, but internal leadership must direct prioritization and communication during a real event.

This highlights a strong connection between security maturity and regular practice. Organizations at the highest maturity levels practice far more frequently, while those in early stages rarely move beyond written plans. This pattern highlights the fact that regular rehearsal is not a secondary activity, but a defining marker of true preparedness.

How has your organization adapted to the evolving threat landscape in the past 12 months?



What is most important to you in planning your security work?

Security Adaptation Strengthens Fundamentals, Not Strategy

Organizations are taking steps to adapt to evolving threats, but mostly through incremental actions. The most common actions focus on strengthening fundamentals: increased employee training, closer collaboration between IT, business, and leadership, implementation of new technical controls, and updates to incident response plans. These are necessary steps, but they do not reshape security strategies.

Training stands out as the most common adaptation activity. It supports long-term maturity by improving culture and raising risk awareness. Strengthened collaboration also plays an important role, signaling that business leaders are more engaged in cyber risk than in previous years.

Organizations with higher security maturity have implemented more measures to a greater extent. The biggest behavioral difference is in conducting regular exercises, which is discussed on page 14. This shows that adaptation work expands as maturity rises, revealing more structural risks that require ongoing attention.

AI dramatically increases effectiveness and capability with both positive and negative impacts. It accelerates the need for adaptation, but not through entirely new threat categories. AI lowers the barrier of entry for attackers with more precise targeting. These developments make existing attack vectors more effective. Organizations' use of AI may increase future exposure, but its practical impact on adaptation remains modest so far.

Overall, adaptation is happening, but unevenly. Mature organizations advance more, while smaller and less mature ones take scattered steps without a larger plan.

Main Takeaways

→ Most adapt to evolving threats by strengthening security culture through training, collaboration, and updated controls.

→ Higher security maturity drives broader and more systematic adaptation, especially through regular exercises.

→ AI amplifies existing attack methods, raising the urgency for consistent training and stronger collaboration.

Statens IT: Preparedness in a World Without a Script

Statens IT carries a central part of the digital infrastructure of the Danish state - operating at the intersection of security and resilience in an era where the unpredictable has become the new normal.

Covid. Drones. War in Europe. Critical incidents don't follow a script, and that reality has fundamentally shaped the way Statens IT thinks about security.

"Many of the services we deliver reach many, many thousands of users. It has to be secure, but it also has to be a service that makes their workday better," says Charlotte Nielsen, Deputy Director at Statens IT.

Statens IT serves a broad and diverse customer base, from ministries handling GDPR-sensitive data to institutions where physical security is the defining concern. That demands differentiated solutions, not a one-size-fits-all model.

"It makes no sense to put seven locks on the front door while the back door stands wide open. It is about maintaining focus in the right places at all times."

The customer base includes some of the most security-critical organizations in the country, and that attracts a certain type of professional.

"Demand for security competencies outstrips supply, and we feel that too. But I think we are in a somewhat privileged position. If security is your passion, you want to work somewhere where it truly matters. And it does with us."

One thing Charlotte Nielsen holds on to above all is practice: you can only act quickly and correctly under pressure if you have done it before.

"If you need to do something fast and effectively, practice is the path to mastery. Time is a critically important parameter. And when we practice, we also gain new insight. We discover things we perhaps did not know we needed to know."

Statens IT holds ISO certification and meets requirements for regular preparedness exercises, supplemented by its own internal exercises. The geopolitical threat landscape has sharpened the approach, and frameworks like NIS2 have done the same. Charlotte Nielsen doesn't see it as a burden.

"Some people treat it as bureaucratic box-ticking. I don't buy that. Regulation forces you to confront reality: Is something critical here, or is it not? The speed requirements exist for a reason. You have remarkably little time before things go seriously wrong."

"In reality, you're training for something you don't know the shape of yet. In the old days, it was a rigid, step-by-step plan. Now we work with components we can assemble in different ways, depending on what actually happens."

For Charlotte Nielsen, the human dimension matters at least as much as the technical. At Statens IT, access to certain AI tools requires completing a training course first. A kind of license for digital tools. And subtle nudges in daily routines remind people to think before they act, for example, before an email reaches the wrong recipient.

"It makes no sense to put seven locks on the front door while the back door stands wide open."

Charlotte Nielsen, Deputy Director, Statens IT.

"If you compromise usability to increase security, you end up in an even worse place. People find creative workarounds, and then you haven't solved the problem."

Looking ahead, knowing exactly where your data resides and what you actually commit to when choosing a platform will matter at least as much as traditional security.

"It is about asking the question: Where is my data? Am I okay with that? And am I aware of the decisions I make when I say yes to something?" says Charlotte Nielsen.

"We advocate for sharpening that awareness, within our own organization and among our customers."

CHAPTER

3

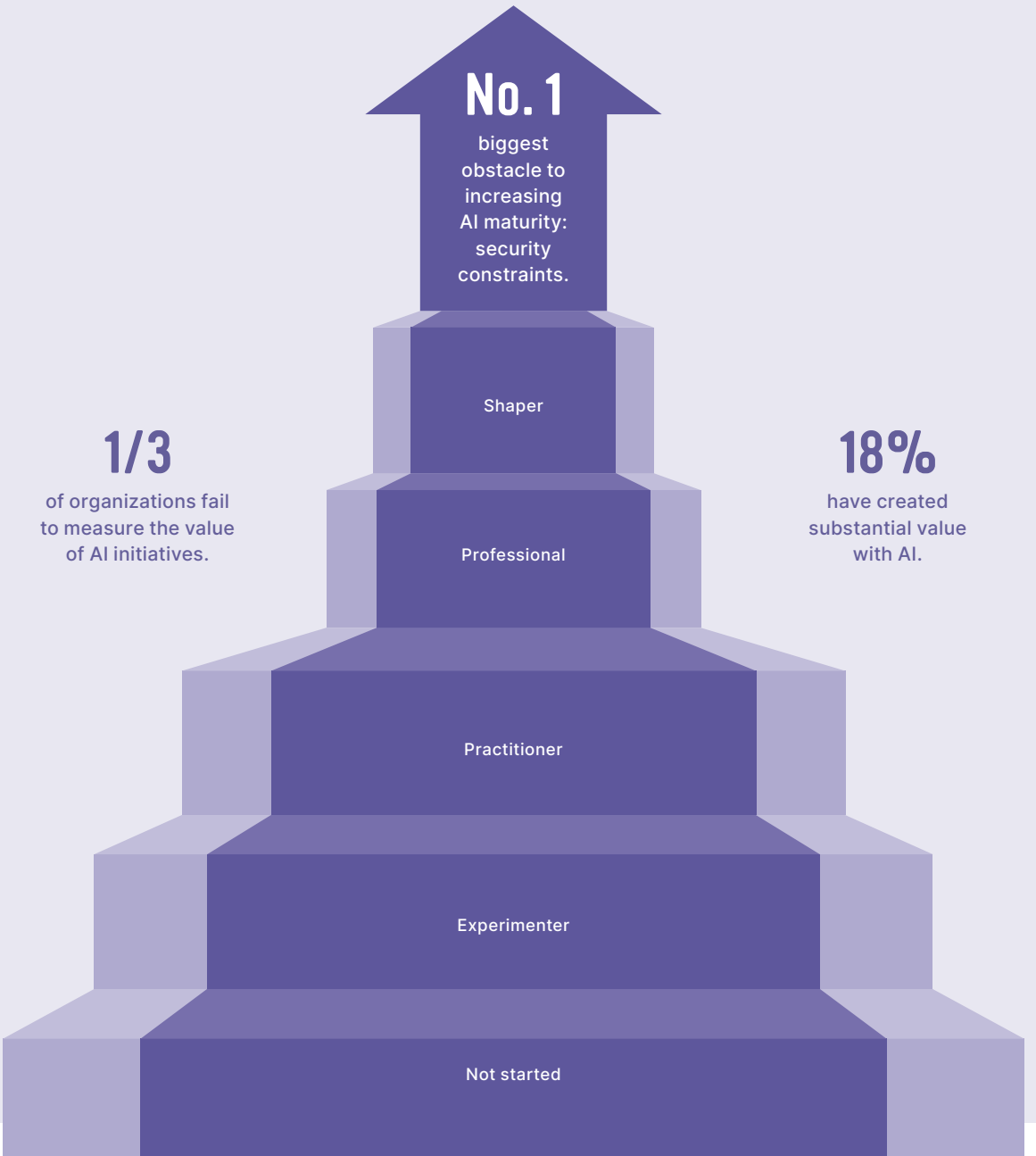
Unlocking the Value: From Experimenter to Practitioner

AI ambition is no longer defined by pilots alone. This chapter highlights how organizations progress toward real use, overcome maturity barriers, create tangible value, and assess impact, offering perspective on what separates experimentation from practical, value-driven adoption.

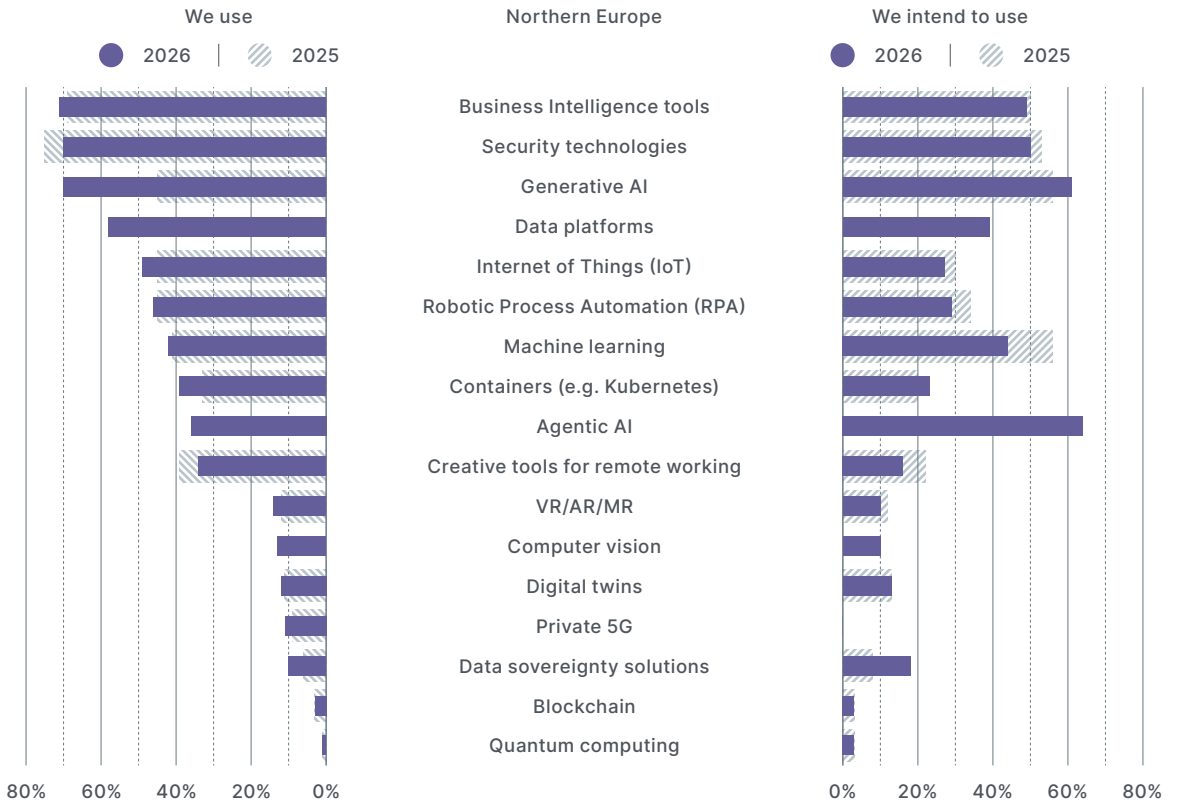
No. 1
biggest obstacle to increasing AI maturity: security constraints.

1/3
of organizations fail to measure the value of AI initiatives.

18%
have created substantial value with AI.



We use/intend to use the following technologies in production:



From Assistants to Agents: The Next Phase of AI Use

Main takeaways

→ Generative AI adoption is rising sharply; agentic AI is positioned for the next wave of growth.

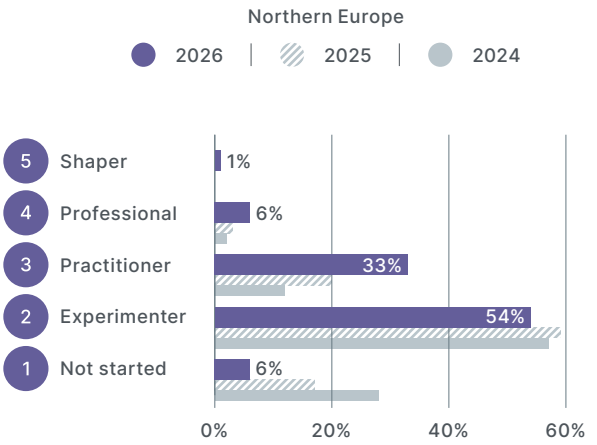
→ Machine learning remains central for organizations with higher maturity and value creation.

→ Previously hyped technologies receive limited priority as organizations focus on proven operational impact.

Technology use in Northern Europe is shifting sharply toward AI. Generative AI shows the strongest growth and is now widely used in production, while organizations plan a significant expansion of agentic AI over the coming years. AI-mature organizations already using more advanced AI tools plan to scale them further. Machine learning remains a core value driver, especially among high-maturity organizations that have integrated it into operations. Meanwhile, several technologies once surrounded by strong market expectations, such as VR, digital twins, blockchain, and broad computer vision, have not become the strategic priorities many anticipated. Instead, organizations focus on tools that support productivity and automation.

Current AI use also helps explain the value distribution. Content creation, coding support, internal chatbots, and cybersecurity applications are now common. More advanced users integrate AI into operations, forecasting, and automation, where gains are larger and easier to quantify. Machine learning and agentic AI stand out as the technologies most associated with creating high value, although planned growth is strongest for agentic AI.

How do you rate your organization's AI maturity?



What are your main obstacles to increasing AI maturity?

Multiple-choice question

1. Security constraints
2. Upskilling/reskilling end users
3. Data management

What do you use AI for today?

Multiple-choice question

1. Content creation
2. Coding assistance
3. Internal chatbots

Fast Starts, Slower Progress: The AI Maturity Pattern

AI maturity in Northern Europe is moving upward. The share of organizations at the "not started" stage has decreased significantly, and many now progress through the early maturity levels at a steady annual pace. The movement from beginner to practitioner is consistent, with experimentation giving way to more formalized AI capabilities and clearer ambitions.

Progress slows at the practitioner level. This is the stage where organizations begin to operationalize AI and integrate it into processes, but scaling requires governance, monitoring, and new operating models. These capabilities take time to build. The slow increase in organizations reaching the professional level shows that the leap from structured experimentation to transformation is the hardest part of the maturity journey.

Finland shows a notably higher concentration of mature organizations, with 62 percent at levels 3 to 5 compared to the regional average of 40 percent. Organizations in these maturity levels also report greater value creation. Lower-maturity organizations continue to experiment without consistently evaluating their results.

Upskilling remains the most frequently mentioned challenge, particularly among organizations that have already created value and want to progress. Regulatory uncertainty and security constraints also limit momentum, especially in sectors where compliance and sovereignty concerns are pronounced. This explains why early movement is rapid while progress beyond practitioner requires time, clarity, and stronger organizational foundations.

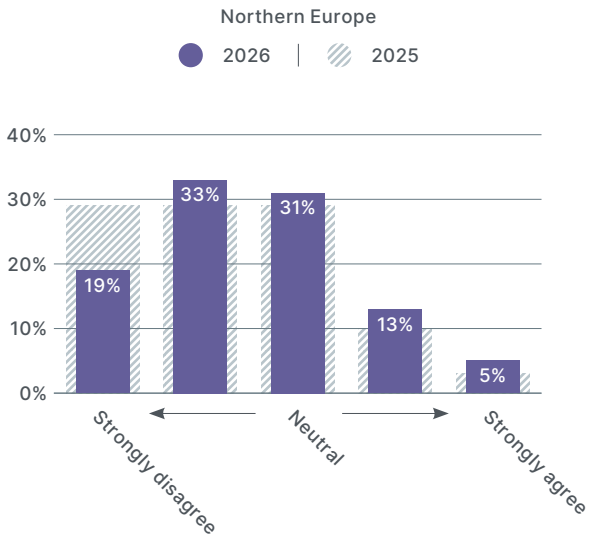
Main Takeaways

→ AI maturity is rising quickly in its early stages, but slows when organizations begin scaling and governance work.

→ Higher maturity strengthens value creation because AI becomes integrated, measured, and aligned with business goals.

→ Upskilling/reskilling, regulatory uncertainty, and security constraints limit advancement beyond practitioner level.

My organization has created substantial value with AI.



Value per AI maturity level	1	2	3	4	5
5. Shaper	0	0	0	0	100
4. Professional	0	7	29	48	17
3. Practitioner	2	21	48	24	5
2. Experimenter	25	44	24	5	2
1. Not started	65	28	4	2	1

→ 65% of respondents who chose "Not started" in the AI maturity question selected 1 in the substantial value question.

→ 100% of people who said they are at "Shaper" level in AI maturity rated the value question at 5.

→ Purple marks the most common responses for each AI maturity level.

AI Value Creation Rising Slowly Despite Rapid Maturity Growth

Main Takeaways

→ AI value is growing slowly as most organizations are still at the experimenter level, and many also have difficulties moving on from the practitioner plateau, where pilots dominate and scaling is limited.

→ The highest value appears when organizations reach advanced AI maturity and integrate AI into operations and transformation.

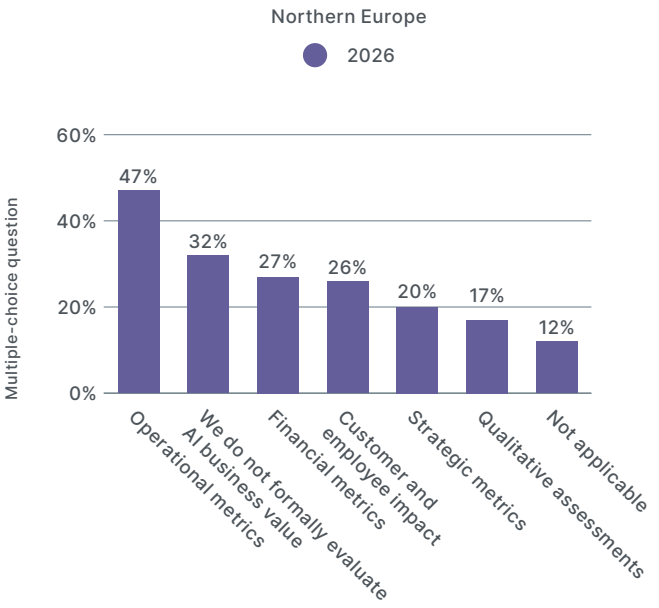
→ AI-mature organizations prioritize operational metrics for measuring impact instead of financial results, facilitating alignment of AI initiatives with everyday processes.

Organizations in Northern Europe report gradual progress in creating value with AI, but the increase is slower than the growth in AI maturity. While more organizations have moved into the "Practitioner" level and above, the share that strongly agrees they create substantial value has only increased modestly. This reflects a pattern where early maturity brings structure and ambitions, but not yet a broad business impact.

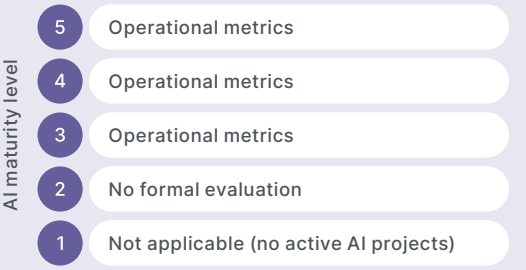
The data shows a clear link between maturity and value. "Practitioner"-level organizations report more value than beginners, yet most remain in a plateau where pilots and early-use cases dominate. Meaningful value appears later in the journey. "Professional"- and "Shaper"-level organizations report the highest value by a significant margin, indicating that business transformation, integration, and scaled use cases are the true drivers of measurable outcomes. Read more about AI maturity on page 19.

Less mature organizations struggle to evaluate value at all. Limited active projects and experimentation make it difficult to measure productivity gains, time savings, or operational improvements. Mature organizations focus their measurement on operational metrics rather than financial results, which lowers the barrier to showing impact and aligns AI initiatives with day-to-day processes.

How does your organization evaluate the business value of its AI initiatives?



Top evaluation method per AI maturity level



AI maturity levels: 1. Not started – 2. Experimenter – 3. Practitioner – 4. Professional – 5. Shaper

Many Organizations Adopt AI Before They Measure Its Impact

Organizations in Northern Europe mainly evaluate AI through operational metrics. They look at productivity gains, process automation, and time savings to judge whether initiatives deliver value. This is especially true for mature organizations, where AI is embedded in day-to-day operations. Results are visible in how work flows, not only in financial reports.

At the same time, roughly one third of IT decision-makers state that their organization does not formally evaluate the business value of AI at all. Evaluation maturity still trails AI adoption. Many have moved ahead with pilots and tools without deciding how success should be tracked.

The gap is clearest at lower maturity levels. Experimenters and early practitioners often lack structured frameworks for evaluation. Their projects are exploratory, with narrow scope and unclear baselines, which makes it difficult to quantify impact in a consistent way. As a result, leaders struggle to compare initiatives or argue for scaled investment.

More AI-mature organizations incorporate value considerations when they design and validate use cases, not only after deployment. Metrics are defined early, updated as the solution evolves, and used to adjust or stop initiatives.

The overall picture is mixed. Many IT decision-makers have moved AI into production, yet a significant share still lack a clear view of whether AI makes the organization more effective. Closing this evaluation gap will be critical for deciding which AI initiatives deserve to scale and which should remain experiments.

Main Takeaways

→ Operational metrics such as productivity, automation, and time savings are the dominant way to evaluate AI.

→ Around one-third of organizations do not formally measure AI value, which leaves management without a clear basis for prioritization.

→ AI-mature organizations design metrics into AI projects from the start, turning evaluation into an ongoing management tool rather than an afterthought.

LTG Group: Bringing AI Into Rail Transformation

When digital transformation reaches the railway sector, it quickly moves beyond software. It reaches tracks, stations, inspection routines, and critical infrastructure. At LTG Group, that means bringing software, data, and AI into the physical realities of rail operations.

LTG Group manages Lithuania's rail infrastructure, freight, and passenger rail services. With 5,617 employees, 5.9 million customers/passengers per year, and annual revenue of approximately 500 million, it operates at a scale where reliability is non-negotiable and transformation is judged by how well the system works every day.

For Vytautas Bitinas, Chief Technology Officer at LTG Group, that is the starting point. Rail, he says, is now facing the kind of transformation that telecom, banking, and energy went through earlier. "We are continuously transforming," Bitinas says. "The question is not whether we change, but how."

That view comes from the scale of change already underway. LTG is moving through electrification, infrastructure renewal, and growing pressure to operate more efficiently while maintaining critical services. Rail is also gaining new strategic relevance through sustainability goals and military mobility. For Bitinas, this raises the bar for every technology decision: new solutions have to work in a demanding operational environment, not just look promising on paper.

One example is rail infrastructure monitoring. LTG uses a diagnostic train equipped with cameras and sensors to assess track conditions, while AI-supported analysis helps identify anomalies faster and more precisely. Another pilot involves quadruped robots that inspect trains in narrow spaces and collect visual data in all weather conditions.

"We are continuously transforming. The question is not whether we change, but how."

Vytautas Bitinas, Chief Technology Officer, LTG Group.

LTG is also using AI in internal support functions. One example is an assistant that helps employees navigate HR-related policies and documents faster.

"Our modus operandi is to explore, polish the solution, understand exactly what it costs, and what value it creates," he says. "Only then do we move toward a production decision."

This discipline also reflects the constraints LTG operates under. Investment decisions have to be weighed carefully, especially in a capital-intensive sector where modernization competes with other strategic priorities, including military mobility and major infrastructure programs. At the same time, the organization must introduce new solutions without disrupting critical operations, while carrying the burden of old Russia-linked systems and building newer Western platforms in parallel.

Together, these realities make LTG's transformation especially complex. Cybersecurity, governance, and data control shape every discussion, while many projects involve sensors, robotics, communications, and operational technology alongside software. "What problem does this solve? Where do we save? What gets better?" Bitinas says, describing the questions behind each decision.

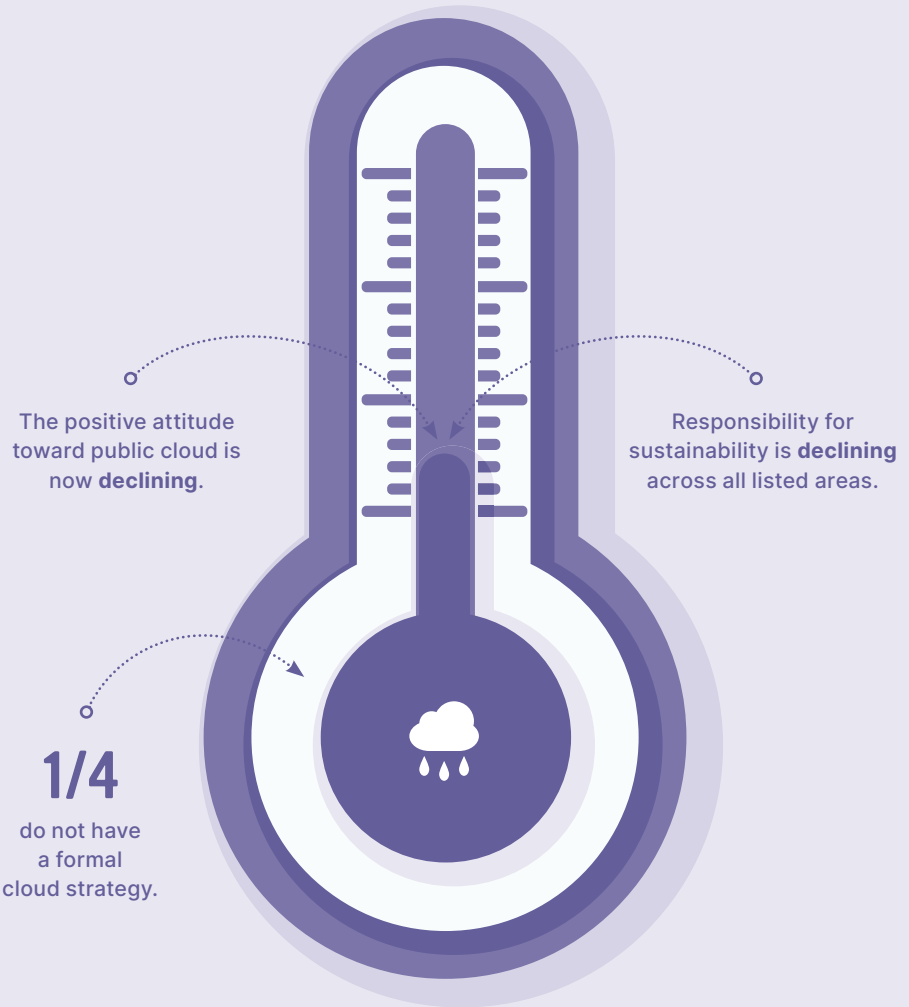
Over the next three years, LTG plans to expand automation and digital support across the network. Among the areas under exploration are remote support for selected functions in smaller stations and longer-term opportunities related to autonomous rail technologies. "The main goal is to change processes, so they become qualitatively different," Bitinas says.

Bitinas does not speak about transformation as a slogan, but as a series of decisions, tests, and trade-offs inside a critical system that has to keep moving. In that respect, LTG's direction is a practical rethinking of how a modern railway should run.

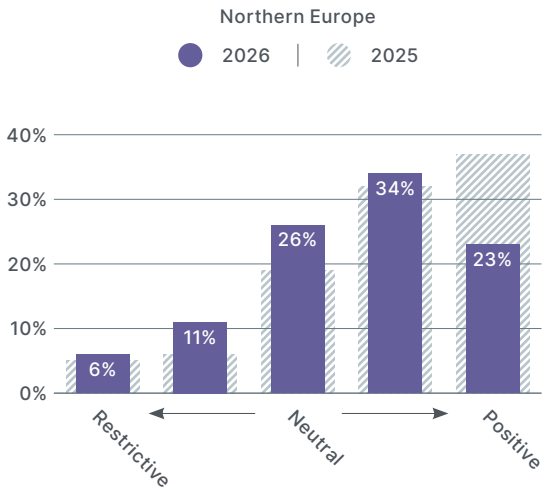
4

Shifting Perspectives on Cloud and Sustainability

Perspectives on cloud and sustainability continue to shift. This chapter reveals how organizations view public cloud, define strategy, balance their teams, and connect IT decisions to broader sustainability and organizational responsibility.



What is your organization's current attitude to using public cloud solutions?



What are your main drivers for using public cloud solutions?

Multiple-choice question

1. Scalability
2. Availability
3. Functionality that we cannot produce internally

What are your biggest barriers to using public cloud solutions?

Multiple-choice question

1. Security aspects
2. Sovereignty and geopolitical concerns
3. Legal uncertainty

From Optimism to Neutrality: Attitudes Toward Public Cloud Shift

Main Takeaways

→ Cloud remains essential, but security, geopolitical, and sovereignty concerns now shape confidence levels more than before.

→ Security, sovereignty, geopolitical risk, and legal uncertainty constitute the primary barriers.

→ Scalability, availability, and unique functionality remain the strongest drivers behind continued public cloud adoption.

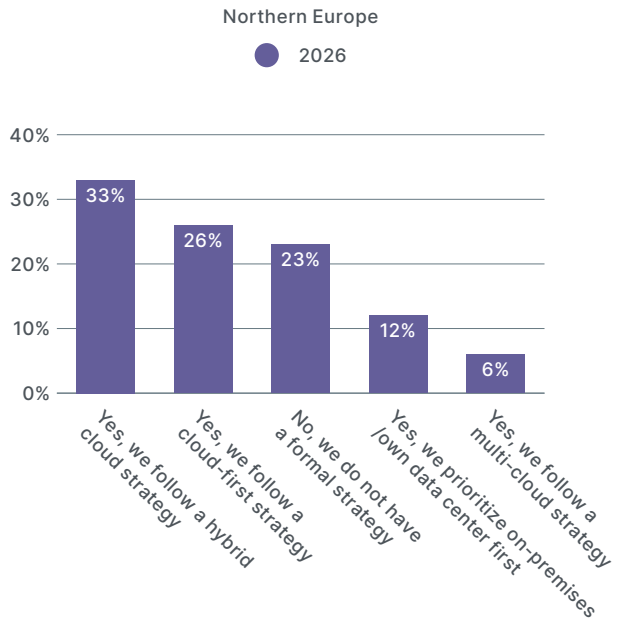
Attitudes toward public cloud in Northern Europe have moderated in 2026 after several years of increasing positivity. Most organizations remain generally positive, but fewer describe their stance as very positive. Instead, more respondents place themselves in neutral or cautiously positive positions. The shift reflects growing hesitation rather than reduced cloud usage.

The pattern differs across sectors. The private sector shows a steeper decline in strong positivity, falling from 45 to 26 percent. Meanwhile, the public sector has decreased from 26 to 18 percent, indicating different starting points and degrees of change.

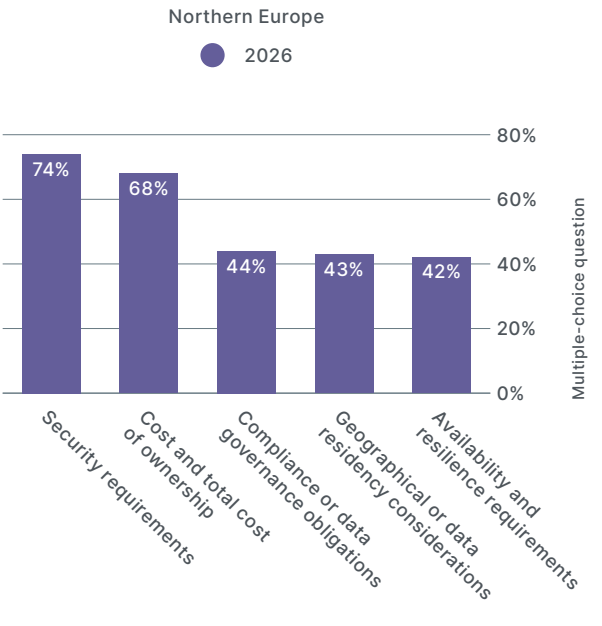
The shift aligns with how organizations view the barriers to public cloud. Security concerns remain the most frequently cited barrier and continue to influence confidence. Sovereignty and geopolitical considerations have increased in relevance, with many organizations now assessing exposure to cross-border dependencies and the strategic implications of cloud concentration. Legal uncertainty is still a major barrier, even though its relative importance has decreased over time. The cost and unpredictability of cloud spend also continue to surface as practical concerns.

Despite these barriers, the main drivers for using public cloud remain intact. Organizations continue to rely on public cloud for scalability, high availability, and access to specialized services they would struggle to produce internally. The decline in strong positivity does not reflect reduced reliance, but rather a more cautious, risk-aware approach to decision-making.

Does your organization have a defined cloud strategy?



What factors does your organization consider when making decisions about where to run workloads?



Cloud Confidence Depends on Strategy, Not Just Technology

Cloud adoption strategy varies significantly across Northern Europe, and the divide between organizations with and without a defined strategy is one of the strongest patterns in the data. Only 16 percent in the private sector lack a strategy. The corresponding share in the public sector is 32 percent. This reflects structural differences in how cloud decisions are organized.

Respondents without a formal strategy tend to be less positive toward public cloud. Those prioritizing on-premises approaches are the most restrictive. In contrast, organizations with defined cloud strategies express higher confidence and a more deliberate approach to integrating public cloud services.

When deciding where to run workloads, two considerations dominate: security requirements and the total cost of ownership. These factors consistently shape workload placement across countries and sectors, forming the core of cloud strategy decisions. While sustainability is often promoted as a cloud advantage, it carries little decision-making weight (10 percent) compared to security (74 percent) and cost (68 percent).

Despite security being a top workload factor, workload-specific risk assessments are limited (17 percent). This indicates an assumption that cloud platforms are secure by design, and highlights an overreliance on implicit trust rather than structured evaluation. Sensitivity to data residency and sovereignty varies by country, underscoring that cloud strategies must balance operational benefits with local governance realities.

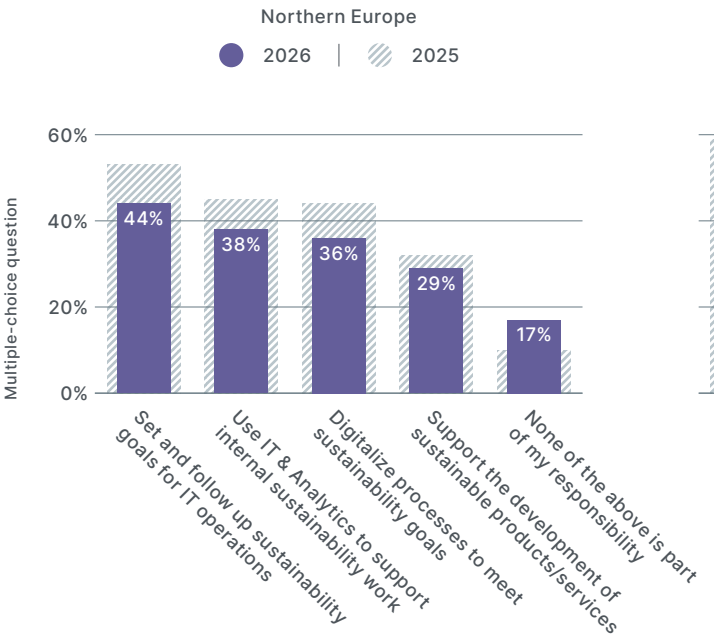
Main Takeaways

→ Organizations without a cloud strategy are consistently less positive toward public cloud, and on-premises prioritizers are the most restrictive.

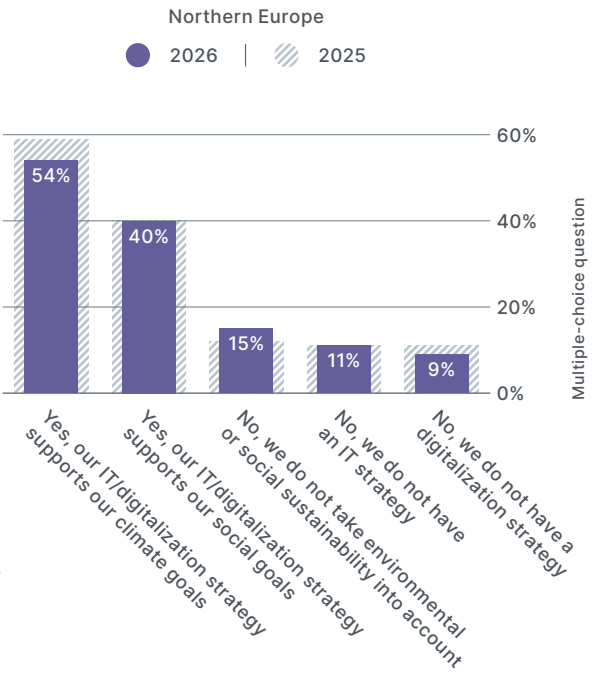
→ Defined cloud strategies correlate with clearer direction and higher confidence in adopting public cloud.

→ Security, cost, and compliance dominate workload placement, while structured risk assessment remains underdeveloped.

What do you consider to be your responsibility as an IT decision-maker when it comes to the company's sustainability goals?



Is your IT/digitalization strategy aligned with the company's sustainability goals?



As Priorities Shift, Sustainability Risks Losing Its Place

Main Takeaways

→ Responsibility for sustainability is declining across all listed areas, with more IT decision-makers opting out entirely.

→ Organizations with maturity in governance and capabilities report higher ownership, while low-maturity teams increasingly see sustainability as outside their remit.

→ IT can reclaim influence by focusing on enabling actions that improve sustainability, while strengthening operations and reducing cost.

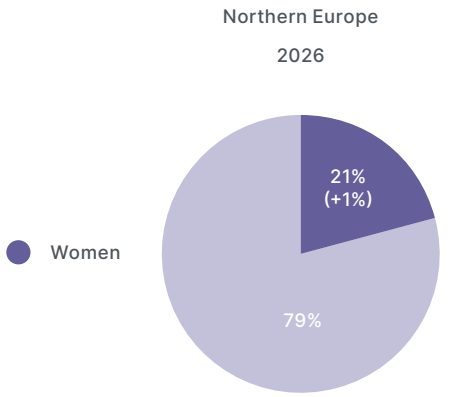
There is a clear decline in how many IT decision-makers view sustainability as part of their responsibility. This comes at a time when other pressures dominate, including security demands. Some IT decision-makers may also feel that sustainability is now integrated into everyday operations and is not a separate responsibility.

The downward trend appears across every listed sustainability area. Fewer IT decision-makers now set or follow up sustainability goals for IT operations, support internal reporting, digitalize processes to achieve sustainability targets, or contribute to sustainable products and services. These declines have continued for three consecutive years, suggesting a broad shift in focus rather than isolated movement in individual areas.

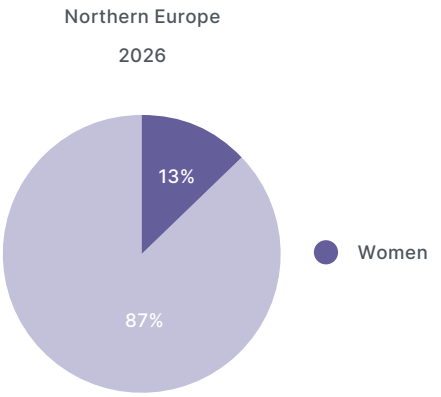
Organizational maturity, the size of the organization, and IT decision-makers being part of management matter. Such organizations show higher sustainability responsibility. This indicates that maturity in governance and capabilities supports, rather than replaces, sustainability ownership.

The trend raises an important question: Is IT stepping too far away from sustainability? Reclaiming a role here does not mean owning sustainability outright. Instead, IT can strengthen its position as an enabler through data quality, lifecycle management, cloud architecture choices, and systems that support accurate reporting. This will improve sustainability performance while also delivering operational and cost benefits, and creating a positive path forward for IT leaders who want to contribute without adding new standalone initiatives.

How many women work in your IT department?



Women among the survey respondents



Figures in brackets show the change compared with last year (percentage points).

High-Performing Teams Are Built, Not Born

The share of women in IT departments across Northern Europe remains stable at around 20 to 21 percent. Thirteen percent of the IT decision-makers responding to this survey are women. On their own, these numbers do not indicate maturity or performance. However, reports and studies – for example, McKinsey: Diversity matters even more, 2023 – show that organizations with more balanced teams tend to demonstrate better results and higher maturity in many areas. This suggests that gender balance functions as an indicator of underlying team qualities rather than a driver by itself.

High-performing teams are created through deliberate leadership choices. Teams with different perspectives cover complexity better, challenge assumptions more effectively, and distribute workload in a way that prevents bottlenecks. This matters more as digital environments become more interconnected, and the pressure on IT increases.

When organizations broaden their recruitment language, they report more varied profiles and better team balance. Communication is another foundational capability. Teams that align frequently and maintain clear, intentional communication perform better. This is not because they contain more women, but because they operate with shared understanding and psychological safety.

Sector and size differences exist, but teams with greater representation of women are more likely to show higher maturity and broader alignment. This correlation is not causal, but it highlights that balanced teams are often the result of thoughtful leadership decisions that show up in organizational performance.

Main Takeaways

→ Gender balance acts as a signal of deliberate team design, not as a standalone performance metric.

→ High-performing teams are built through conscious recruitment, inclusive communication, and complementary competencies.

→ Organizations with more balanced teams tend to show higher maturity in security, AI, and strategic alignment.

SEB Builds High-Performing Teams Through Clarity and Diversity

Building high-performing teams requires clarity, cognitive diversity, and development opportunities. That is the view of Petra Ålund, HR Director at SEB for the past year and a half, following her previous role as Chief Technology Officer for just over five years.

In her role as HR Director, Petra Ålund actively shapes organizational culture and establishes the conditions that foster employee growth and development.

"Our focus on development is not something we just say. We truly mean it. Despite being around for 170 years, we are a bank that always wants to stay at the forefront. If someone has no interest in developing, SEB is probably not the right bank for them. Right now, we are working to give all 19,000 employees the chance to learn more about AI."

Over the years, Petra Ålund has played a pivotal leadership role, leading multiple teams both within and outside the IT sphere. She believes high-performing teams are built on trust and clarity.

"In today's fast-changing working life, we operate with a great deal of uncertainty. This makes clear mandates essential for ensuring everyone understands their role and the outcomes we aim to deliver. When the outcomes are clear, work feels more meaningful and motivates people to show up. It also makes prioritization easier and prevents people from taking on more than they can handle."

Diversity matters too. For Petra Ålund, diversity extends beyond gender to include a broad range of perspectives and experiences. She actively fosters inclusion by bringing in teams with diverse backgrounds, experiences, and viewpoints, drawing on talent from across roles and organizations. Less homogeneous teams within the company reduce the risk of product deliveries missing the mark. Petra Ålund shares an example from her time as CTO.

"Great talent attracts more great talent. And dare to be honest about what you are hiring for. Do not oversell a role or overpromise. It will only lead to a quick departure."

Petra Ålund, HR Director, SEB.

"We were developing a more digitalized mortgage process. We assumed many young people wanted it, but we were completely wrong. Older people, who had already bought three or four homes, wanted a digital experience. Younger, potentially nervous first-time buyers preferred meeting us in person at the bank. As a result, by broadening our team's earlier on, we would likely have understood our target audience's needs much sooner."

This year's CIO Analytics report reveals that fewer IT decision-makers see sustainability as part of their responsibility. Petra Ålund considers this the consequence of short-term thinking.

"Twenty years ago, few people considered energy consumption when choosing a car. Now, it is a deciding factor. Soon, sustainability will drive choices in other sectors. Companies that ignore sustainability in product development risk losing customer appeal. We know sustainability impacts market differentiation."

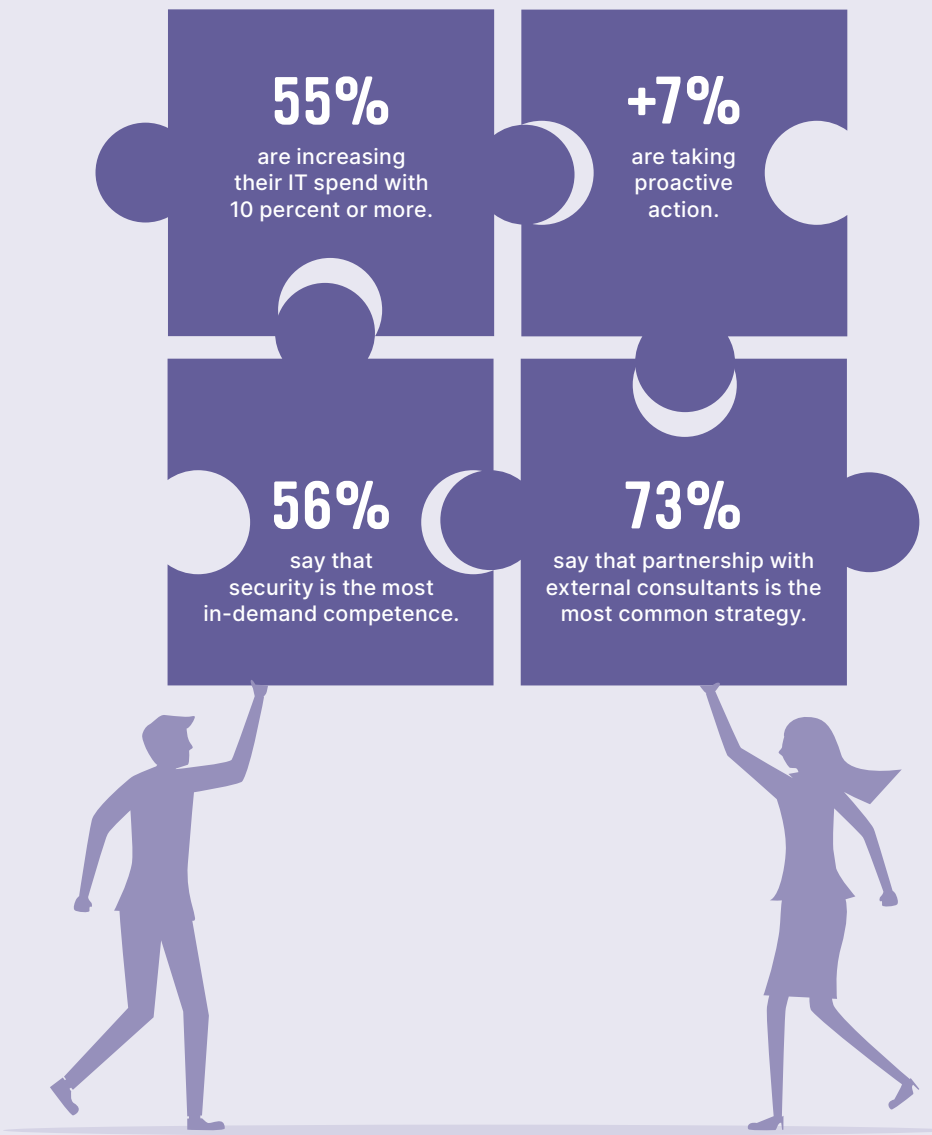
Petra Ålund closes with advice for CIOs looking to build high-performing teams going forward:

"Work closely with your HR leader. Develop an employer branding strategy together that defines the types of people you want to attract. Great talent attracts more great talent. And dare to be honest about what you are hiring for. Do not oversell a role or overpromise. It will only lead to a quick departure." ●

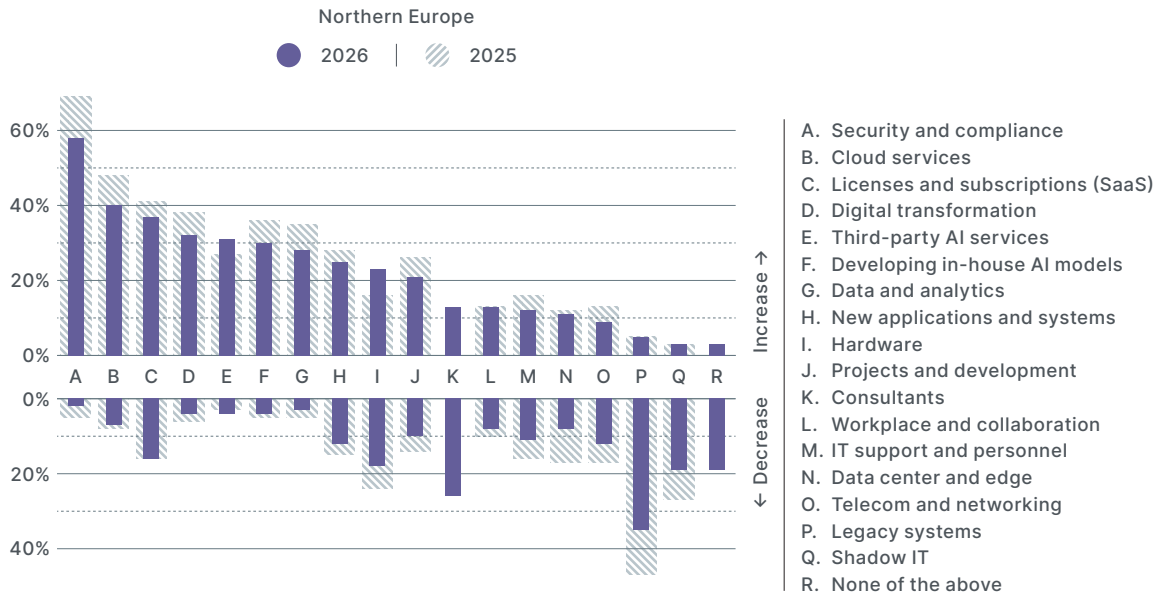
5

Making Room for What Matters

The ability to move forward depends on people and priorities. This chapter sheds light on spending direction, emerging competence needs, access to skills, and how IT organizations are evaluated and perceived in terms of their level of proactivity.



The IT spend will increase/decrease this year in the following areas...



IT Spend Rises, but Priorities Shift

Main Takeaways

→ IT budgets grow, but rising costs force sharper focus and fewer investment priorities.

→ Security and compliance absorb the largest increases as threats and regulation intensify.

→ AI spending is rising, but foundational limitations slow value creation.

IT budgets in Northern Europe continue to rise, with over half of organizations increasing spending by 10 percent or more. Yet the growth is concentrated in fewer areas than last year. Rising hardware prices, inflation, and reprioritization force IT decision-makers to distribute budgets more selectively.

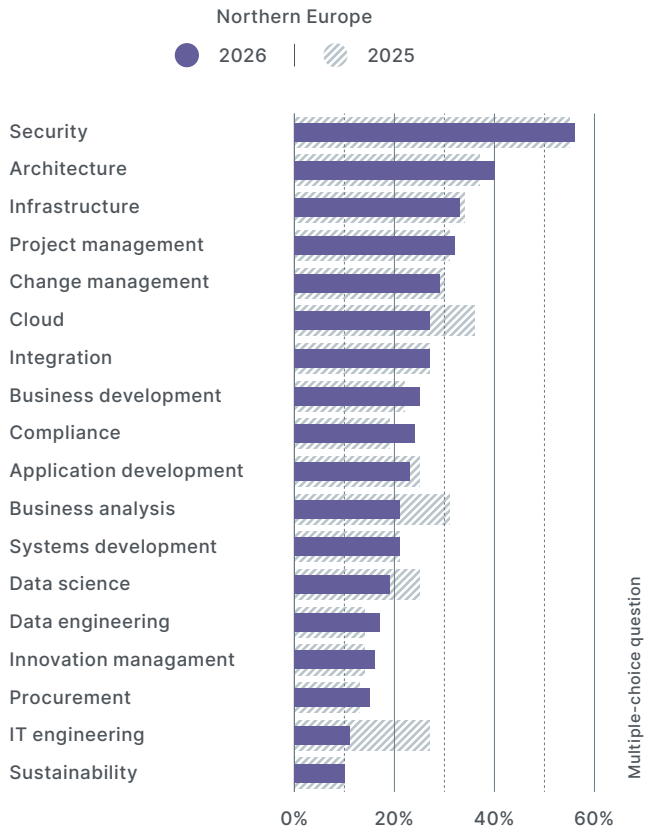
Security and compliance dominate the increases. Heightened threats and new regulations push organizations to strengthen controls, governance, and monitoring before scaling automation or AI. Many lack the skills needed internally, which increases reliance on external partners and managed services.

AI spending also grows, though many organizations remain early in their AI maturity, investing in foundations like data quality, governance, and security before they can realize operational returns. This is discussed further on pages 19 and 20.

Cloud services, subscriptions, and third-party AI tools continue to rise as vendor-driven price increases shape spending. Meanwhile, consulting spend declines, often because it is the easiest category to cut, even when the underlying need remains.

Legacy system spending declines further. Easier AI-driven integrations make it tempting to "work around" aging platforms, but at the risk of increasing technical debt and weakening security over time.

What IT-related competence(s) will your organization need within the next 12 months?



Upskilling, Partnerships, and AI Shape Future Talent

Security remains the most in-demand competence as organizations face regulatory pressure and tougher threats. Architecture follows closely, reflecting the need for strategy, structure, and sustainable operating models across cloud, AI, and modernization. Demand is high across almost all competence areas, showing how stretched IT teams have become.

To ensure future capabilities, organizations rely heavily on two strategies: partnering with external consultants and upskilling internal staff. Partnerships help fill critical skill gaps, but many also plan to reduce consultant spending, creating tension between cost and capability. Upskilling becomes essential as AI reshapes roles, increasing the need for senior architects and security experts, and reducing the need for traditional developers. Discussion between experts also highlights the need for decision-making, communication, and change leadership skills – competencies required far beyond IT.

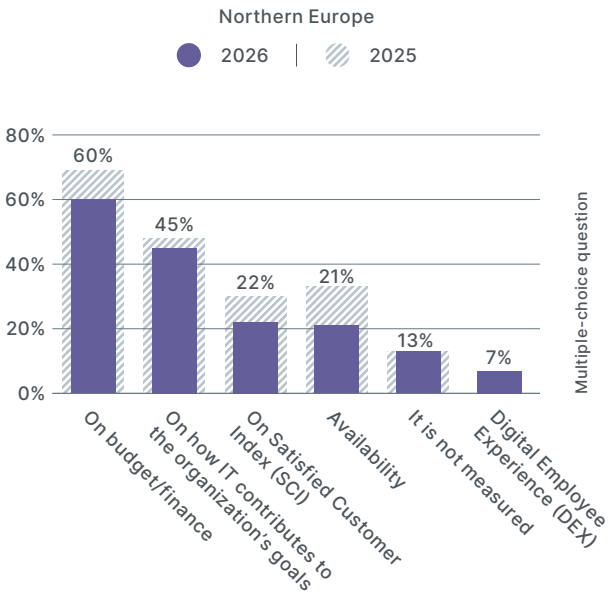
Main takeaways

→ Security and architecture dominate competence needs as complexity increases.

→ Organizations rely on external partners while simultaneously trying to reduce consultant spending.

→ AI drives demand for senior roles and broad upskilling across IT and business.

How is the IT organization measured and evaluated?



Measurement Frameworks Lag Behind IT's Strategic Role

Main Takeaways

→ Budget remains the primary KPI, even as organizations aim to measure IT by value and outcomes.

→ Investment patterns shape measurement: increased spend enables value-based evaluation, while cuts reinforce cost-driven KPIs.

→ Limited measurement maturity keeps IT positioned as a support function rather than a strategic partner.

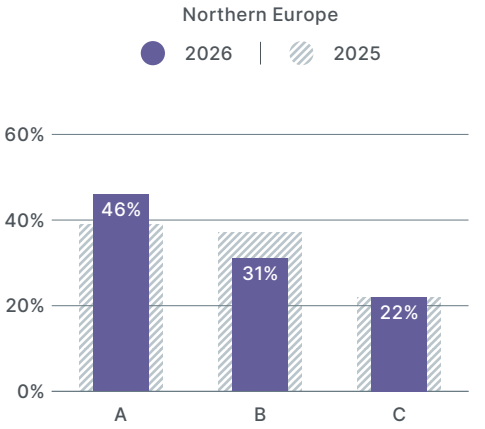
Budget and finance remain the dominant way IT organizations are measured, despite a growing desire to demonstrate IT's contribution to business outcomes. Measurements tied to availability, customer satisfaction, and business value have all decreased compared with last year, raising questions about whether evaluation methods are keeping pace with rising expectations on IT.

Organizations increasing their IT spending rely less on budget metrics and more on value-oriented measures. When the business chooses to invest significantly in IT, it expects strategic contribution, not only cost control. Organizations that reduce IT spending face increased budget scrutiny, lower proactivity, and a focus on cost savings rather than business development. This creates a self-reinforcing loop: budget cuts drive budget-focused measurement, which lowers business impact and can lead to further cuts.

Several responses indicate that IT is still viewed as a support function rather than a strategic partner. Many IT decision-makers say they are evaluated on cost efficiency rather than transformation outcomes. This reflects not only IT's internal practices but also the maturity of business units. Value-based KPIs require shared ownership, and business structures are often not ready to co-own results.

Newer KPIs are emerging, such as digital employee experience metrics, but usage remains limited. The underlying challenge persists: financial KPIs are simple to measure, while value, innovation, and transformation are harder to quantify. This measurement gap continues to constrain IT's strategic role.

Do you consider your IT organization to be proactive in terms of what your business needs?



A. Yes, the IT organization proactively meets the needs of the business.
B. No, but the IT organization is moving toward a more proactive way of working.
C. No, the IT organization acts more reactively when it comes to what the business needs.

Proactivity Grows When IT and Business Move Together

More IT organizations in Northern Europe now consider themselves proactive. The share has grown from last year, and close to half believe they anticipate business needs rather than reacting to them. Yet 22 percent still describe their IT organization as reactive.

IT decision-makers in top management rate their organizations as more proactive, while respondents outside top management or outside the IT department are more likely to describe IT as reactive. This raises questions about shared understanding: what proactivity looks like, whether IT communicates its work clearly, and whether the business recognizes the value delivered. Perception shapes trust and prioritization, making this gap significant.

Organizations that are increasing their IT budgets are less focused on budget metrics and more on value contribution. They also describe themselves as more proactive. Organizations reducing their IT spending tend to be more reactive, more budget-driven, and less able to invest in the capabilities required for forward-leaning IT. Read more about IT spending on page 30.

Several themes highlight what proactivity requires. IT cannot become proactive alone; business roles, processes, and ownership structures must evolve too. Higher AI maturity also correlates with greater proactivity, likely due to stronger data foundations, governance, and experience linking technology to business value. Human capabilities matter as well: courage, communication, influence, and the ability to challenge are essential ingredients in moving from reactive behavior to strategic partnership.

Main Takeaways

→ More IT organizations see themselves as proactive, yet a sizable minority remain reactive, signaling a maturity divide.

→ Proactivity rises when IT is measured on value and supported with investment; budget-driven organizations stay reactive.

→ True proactivity requires shared ownership across IT and business, supported by communication, governance, and AI readiness.

Green Mountain: When Data Center Growth Drives IT Investment

Green Mountain designs, builds, and operates high-security, energy-efficient data centers for global enterprises. The company has facilities in Stavanger, Rjukan, Enebakk, and Hamar in Norway, and is building a new one at Undheim in Rogaland. All data centers run on 100 percent renewable energy, with high energy efficiency as a core design principle.

Behind this infrastructure sits an increasingly business-critical IT organization. Its role is to ensure stable operations, manage growing complexity, and support continued expansion.

"There are no areas where our IT costs are declining. Everything grows with the business. When we build new data centers, we add more systems, more hardware, and more networking. Over time, this drives the IT budget upward and makes it difficult to realize traditional efficiency gains in the short term," says Ole Kristian Risa, IT Director at Green Mountain.

As a result, a significant share of IT investments is directed toward upgrades and consolidation, rather than traditional cost optimization.

"We are essential to making our data centers function. If our systems stop, operations stop. At the same time, much of the infrastructure was built around each individual data center, and that adds complexity when we grow as fast as we do," Risa explains.

"Many of our solutions were originally designed for data centers in the 5–10 megawatt range. Today, we are building facilities of 50–100 megawatts. This means we invest heavily in reducing technical debt, modernizing platforms, and improving integration across systems. The objective is to build an IT landscape that can handle the scale we know is coming."

For the IT organization, this creates a persistent tension between ensuring stable operations, further developing existing systems, and supporting new projects.

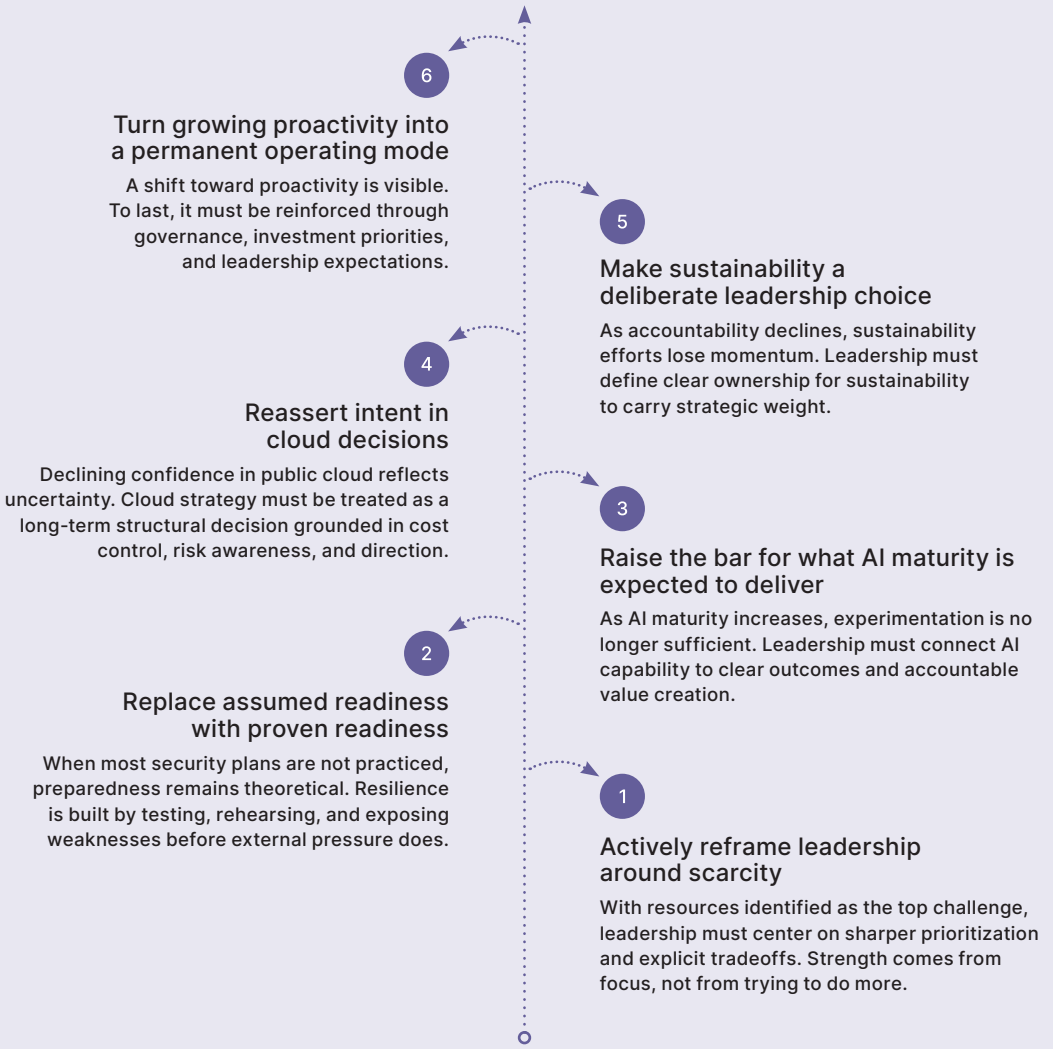
"We are constantly stretched. We need to ensure stable operations and high uptime while also evolving existing systems and supporting new data centers under construction. All of these areas are urgent at the same time, which makes it challenging to prioritize and plan capacity. New projects can move quickly, and we need to be ready to respond."

Looking ahead, Risa highlights a growing need for expertise in security, networking, and compliance, and over time, data and AI, particularly at the intersection of IT and operational technology. For a company experiencing rapid growth, making the right IT investments is critical.

"It comes down to building a foundation that allows us to keep growing without letting complexity run ahead of us. That is where we are focusing our efforts now," Risa concludes.

"We invest heavily in reducing technical debt, modernizing platforms, and improving integration across systems. The objective is to build an IT landscape that can handle the scale we know is coming."

Ole Kristian Risa, IT Director, Green Mountain.



Call to action for IT leaders

Preparing for Tomorrow: Lessons and Strategies

This report emphasizes the role of IT leadership as an active practice, where IT decision-makers are encouraged to function as strategic partners to businesses rather than merely serving as technical administrators. It highlights the importance of proactively identifying changes in the surrounding environment and leveraging new technologies as catalysts for development, instead of simply responding to emerging needs.

With growing security concerns, leadership should transition from an assumption of readiness to one based on proven preparedness, highlighting the importance of practicing security plans to build true resilience. Additionally, as AI technology matures, IT decision-makers are urged to connect AI capabilities with tangible outcomes.

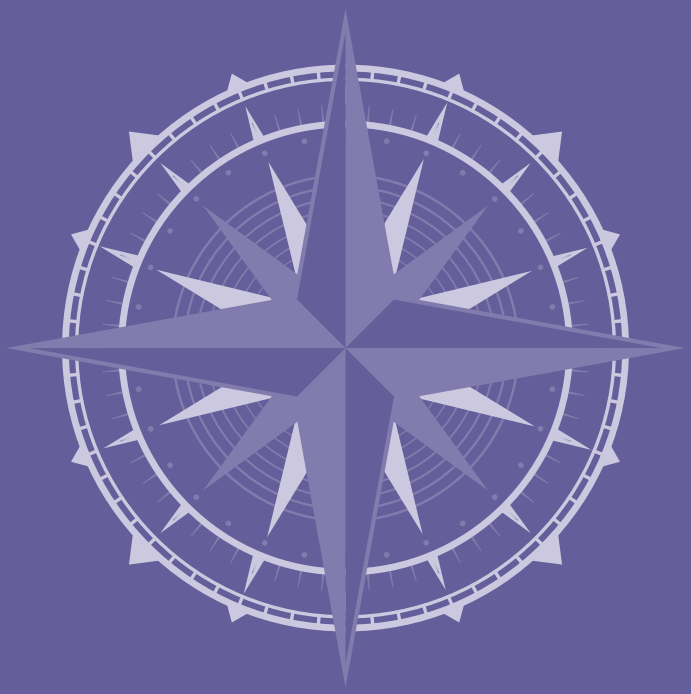
The business increasingly looks to IT for leadership, not the other way around, emphasizing the need for IT decision-makers to embrace their holistic mission. Let essential insights from this report guide you as you navigate the upcoming journey.

CIO ANALYTICS

2026

AI

maturity is increasing.



1/4

do not have a formal cloud strategy.

+7%

are taking proactive action.

55%

are increasing their IT spend.

ATEA