

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

THE BALTICS

No. 1

challenge for IT decision-makers:
resources.

IN-DEPTH INTERVIEWS

p. 9

National School of Arts of Latvia:
CIO Perspective:
IT in Arts.

p. 22

LTG Group:
Bringing AI
Into Rail Transformation

p. 28

Apollo Group:
When the Cloud Starts Running the
Show: How Apollo Took Back Control

Contents

4 CHAPTER 1: NAVIGATING IT LEADERSHIP IN A RAPIDLY CHANGING WORLD

- 5 The Modern IT Decision-Maker Sees the Whole Picture
- 6 Operational Pressure Keeps Security in First Place
- 7 Ambition Points Toward Transformation, Not Obligation
- 8 The Growing Strain Behind IT's Daily Work
- 9 **In the spotlight:** CIO Perspective: IT in Arts

10 CHAPTER 2: ADAPTING TO THE PRESENT WHILE PREPARING FOR TOMORROW

- 11 Higher Maturity Reveals More Risk – and Drives More Action
- 12 Why Security Remains Harder Than It Should Be
- 13 Incidents Increase Activity, Not Immunity
- 14 Most Plans Remain Untested When They Matter
- 15 Security Adaptation Strengthens Fundamentals, Not Strategy
- 16 **In the spotlight:** Preparedness in a World Without a Script

17 CHAPTER 3: UNLOCKING THE VALUE: FROM EXPERIMENTER TO PRACTITIONER

- 18 From Assistants to Agents: The Next Phase of AI Use
- 19 Fast Starts, Slower Progress: The AI Maturity Pattern
- 20 AI Value Creation Rising Slowly Despite Rapid Maturity Growth
- 21 Many Organizations Adopt AI Before They Measure Its Impact
- 22 **In the spotlight:** Bringing AI into Rail Transformation

23 CHAPTER 4: SHIFTING PERSPECTIVES ON CLOUD AND SUSTAINABILITY

- 24 From Optimism to Neutrality: Attitudes Toward Public Cloud Shift
- 25 Cloud Confidence Depends on Strategy, Not Just Technology
- 26 As Priorities Shift, Sustainability Risks Losing Its Place
- 27 High-Performing Teams Are Built, Not Born
- 28 **In the spotlight:** When the Cloud Starts Running the Show: How Apollo Took Back Control

29 CHAPTER 5: MAKING ROOM FOR WHAT MATTERS

- 30 IT Spend Rises, but Priorities Shift
- 31 Upskilling, Partnerships, and AI Shape Future Talent
- 32 Measurement Frameworks Lag Behind IT's Strategic Role
- 33 Proactivity Grows When IT and Business Move Together
- 34 **In the spotlight:** When Data Center Growth Drives IT Investment
- 35 **Preparing for Tomorrow: Lessons and Strategies**



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% from the private sector and 41% 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.

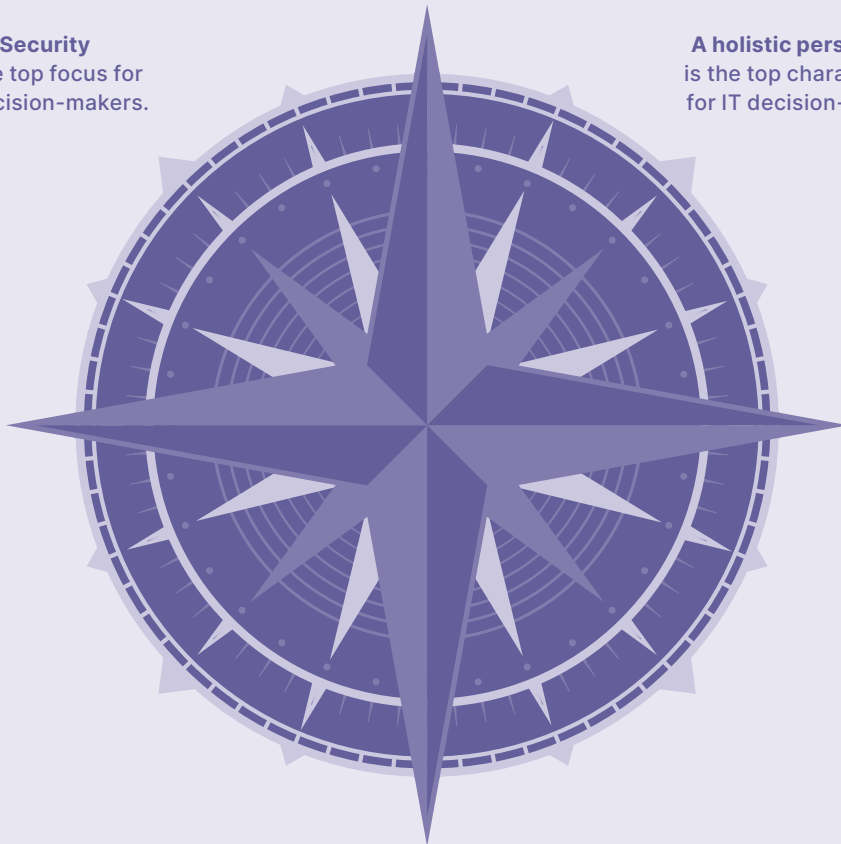
Navigating IT Leadership in a Rapidly Changing World

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.

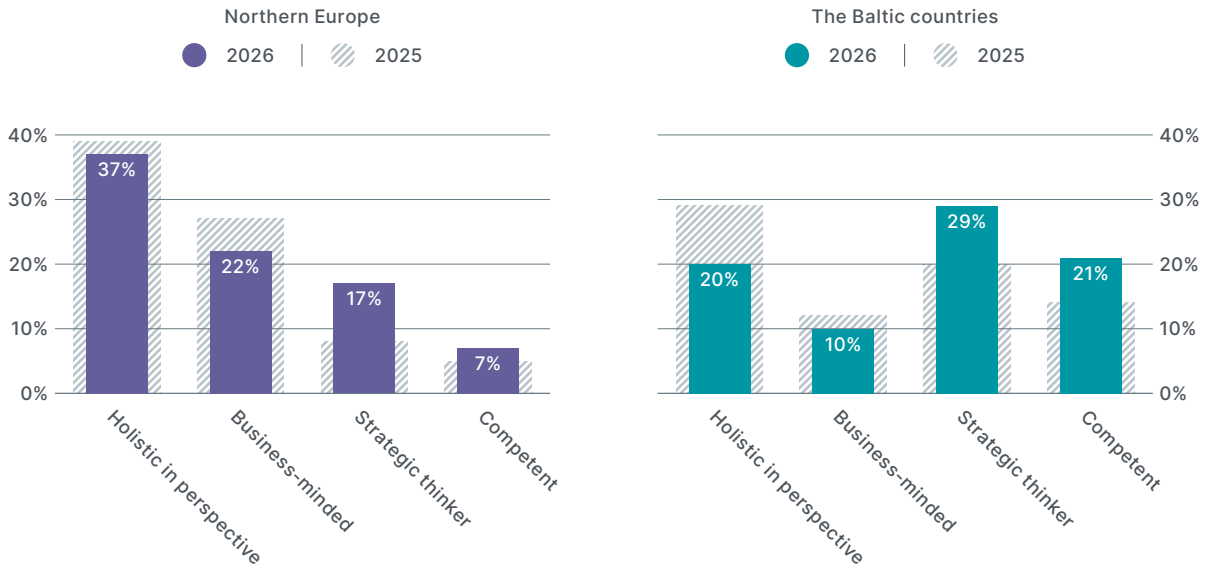
Resources
are the top challenge for
IT decision-makers.

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.

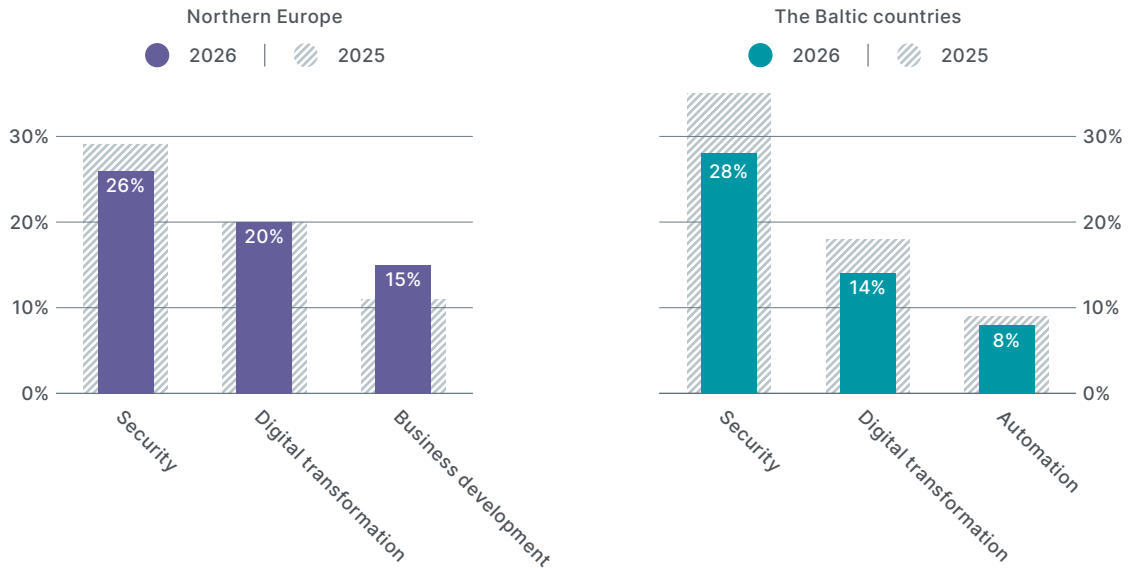
A strong business mindset completes the profile. Effective IT decision-makers understand how technology enables growth, resilience, and value creation. They align choices with business goals and challenge assumptions when priorities drift.

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.

Key Takeaways: Baltics

→ Strategic thinking is identified as the main characteristic of effective IT decision-makers in the Baltics, contrasting with a broader holistic approach reflected in other countries. The rapid shift from IT cost-centered roles to strategically aligned positions also stands out. This is influenced by small-market pressures, rapid technological advancements, and unique geopolitical contexts. Larger organizations in the Baltics focus on strategic thinking, while smaller organizations emphasize competence, revealing a correlation between company size and the characteristics of IT decision-makers.

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



Operational Pressure Keeps Security in First Place

Key Takeaways: Baltics

→ Security remains the primary focus for Baltic IT decision-makers, though attention is shifting to automation. Businesses are seeking efficiency: to make more with less. The security focus is influenced by geopolitical risks and regulatory requirements, particularly the NIS2 directive applicable to many public sector and larger organizations.

Security remains the primary focus for IT decision-makers in Northern Europe, even though its dominance has weakened slightly. Last year, 29% chose security as their top focus, compared with 26% 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.

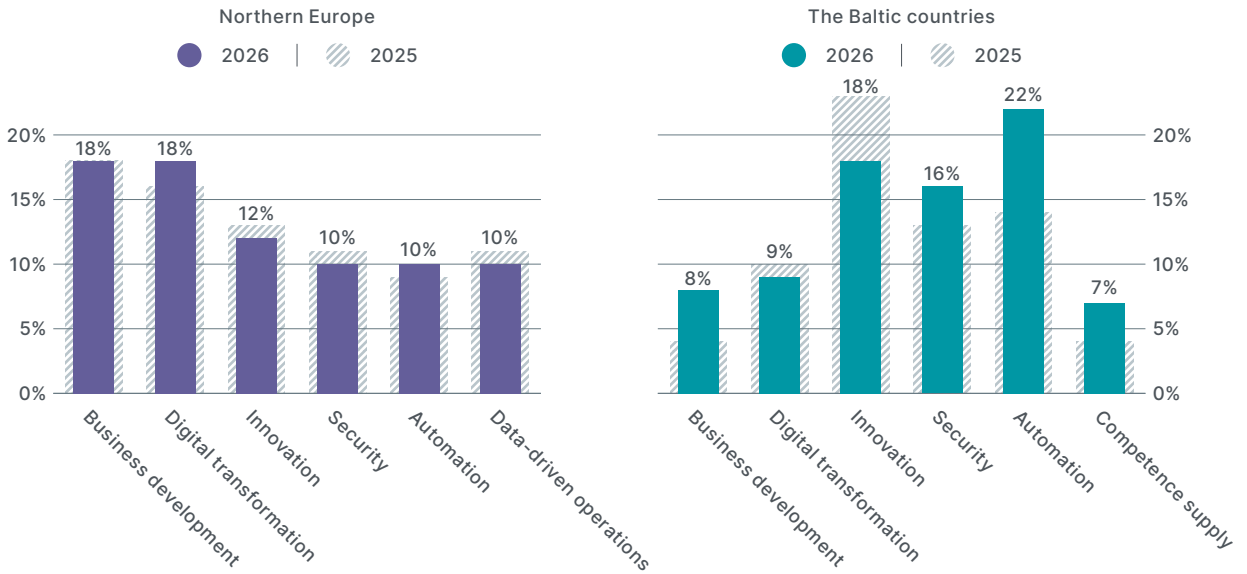
Digital transformation remains a strategic priority, but it often competes for space with operational obligations. When new security demands arise, transformation slows. Many see this as a recurring pattern: progress is possible, but rarely continuous.

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%.

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.

Key Takeaways: Baltics

→ IT decision-makers in the Baltics want to focus more on automation (22%), largely influenced by market demands for efficiency and the growing influence of AI. Organizations face resource shortages everywhere, which can be mitigated through increased automation. This is followed by innovation (18%) and security (16%).

What is your IT organization's biggest challenge?



The Growing Strain Behind IT's Daily Work

Key Takeaways: Baltics

→ Security challenges persist in the Baltics, where organizations have prioritized security for years due to ongoing conflicts next door. Baltic organizations are also facing increasing pressure to drive business growth, integrate AI, enhance automation, and strengthen continuity management. IT security remains crucial but has become one of multiple strategic pillars in the IT decision-maker's complex agendas.

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.

CIO Perspective: IT in Arts

Andrejs Bušenko works behind the scenes at National School of Arts of Latvia, where day-to-day operations, practical decisions, and long-term planning all come together. When he talks about technology, it is not about following the latest trends. It's about making sure things work smoothly so people can focus on their jobs without unnecessary obstacles.

Most of our processes are centralized, and that shapes how we work with technology on a daily basis. It creates stability, but at the same time it limits flexibility,” says Andrejs Bušenko, Project Manager at National School of Arts of Latvia. Over time, the organization has moved from a more flexible, locally managed setup to a centralized system where most IT-related decisions are defined at a higher level. “For less experienced users, this is helpful because it reduces the risk of mistakes. For more advanced users,

it can feel restrictive, as there is very little room for independent action,” he explains.

When it comes to IT spending, decisions are made within a broader budget for goods and services rather than through a dedicated IT allocation. “We evaluate what we can afford based on available resources. If there are urgent needs, such as repairs, those take priority. Any remaining funds are usually used toward the end of the year for additional improvements,” Andrejs Bušenko says. At the same time, additional funding from the Ministry can support specific purchases, such as new equipment. However, rising costs, particularly for utilities, continue to reduce flexibility and limit investment opportunities.

When asked about priorities, the answer is simple: computer equipment remains a consistent focus. “Hardware needs to be updated regularly, especially in areas where specialized software is used. In some cases, performance is critical for daily work,” he notes. Technological advancements also influence decisions, with older solutions gradually being replaced by more modern alternatives as needs evolve.

A key challenge in the current setup is the speed of problem resolution. “Even simple technical

issues can take longer to resolve because everything goes through a centralized process involving multiple departments,” he says. This marks a clear shift from earlier systems, where local responsibility allowed for faster responses. While centralization ensures consistency and control, it can also slow down day-to-day operations and create unnecessary complexity.

Budget constraints add further pressure. “We have a defined budget, but external factors, such as rising costs, directly affect what we can and cannot afford. There are also mandatory expenses that must be covered regardless of the situation,” Andrejs Bušenko explains. This requires constant prioritization, where essential needs take precedence over long-term improvements.

Looking at his daily work, he highlights the need for a more balanced approach between control and usability. “There should be more trust in employees. Not every small action should require approval,” he says, noting that excessive restrictions can slow down processes without significantly improving security. In his view, systems should maintain necessary safeguards while still allowing employees to work efficiently, with trust in their capabilities. ●



"There should be more trust in employees. Not every small action should require approval."

Andrejs Bušenko, Project Manager,
National School of Arts of Latvia.

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%

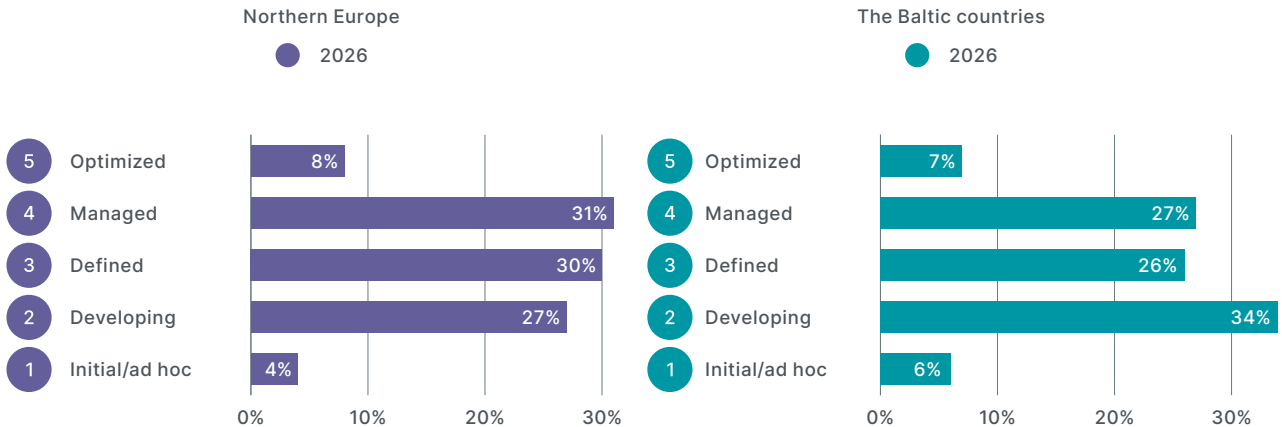
have invested in increased
employee training
and security awareness.

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.

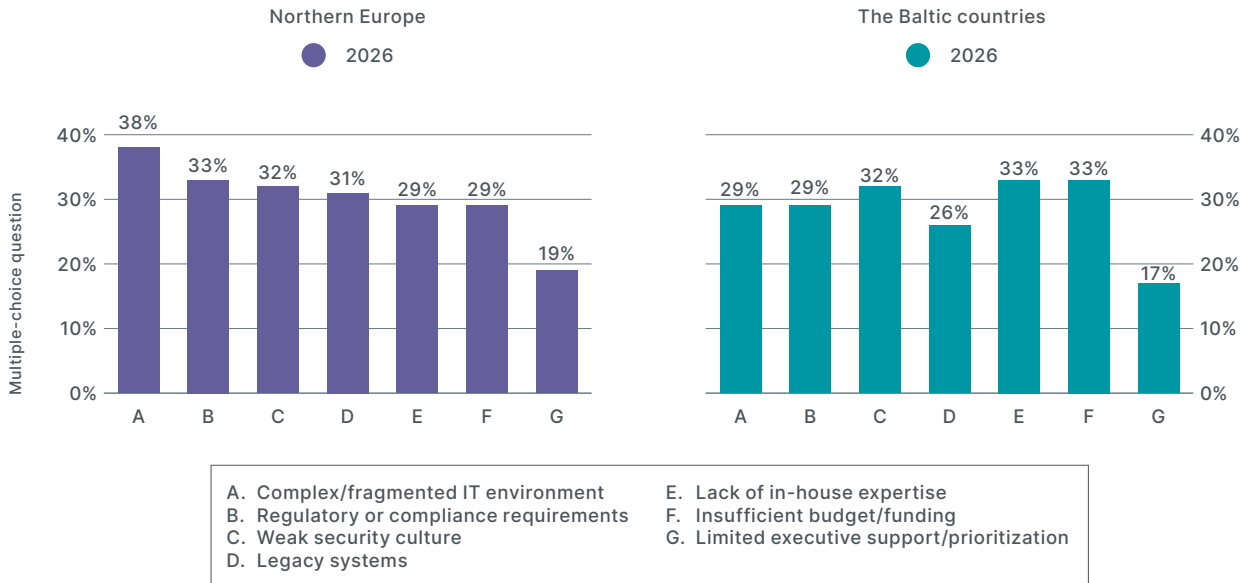
Cyberattack reporting reinforces this pattern. Higher-maturity organizations detect more events before they become incidents because they have better monitoring and broader situational awareness. Lower maturity organizations detect fewer events, which makes real exposure harder to understand. Maturity 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.

Key Takeaways: Baltics

→ In the Baltics, IT security maturity is lower due to small market sizes, limited budgets, and a shortage of security professionals. Many focus primarily on essential security measures, channeling their scarce resources toward business resilience, growth, and technology-driven transformation. Organizations must shift from a reactive cybersecurity approach to a strategic priority, focusing on talent development and effective continuity planning. Recognizing cybersecurity as essential for resilience will enable operational strength and strategic maturity. Security and resilience are closely intertwined and should not be divided into separate budgets.

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



Why Security Remains Harder Than It Should Be

Key Takeaways: Baltics

→ Lack of in-house security expertise, a weak and inconsistent security culture, and insufficient budgets are significant challenges for Baltic IT decision-makers. Baltic organizations demonstrate low security maturity, indicating that they have begun their efforts but have much work ahead, in many cases including developing incident response plans. It is crucial to address these challenges strategically. Organizations are urged to cultivate internal talent. Additionally, outsourcing and forming partnerships could help overcome resource shortages and enhance security competence.

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

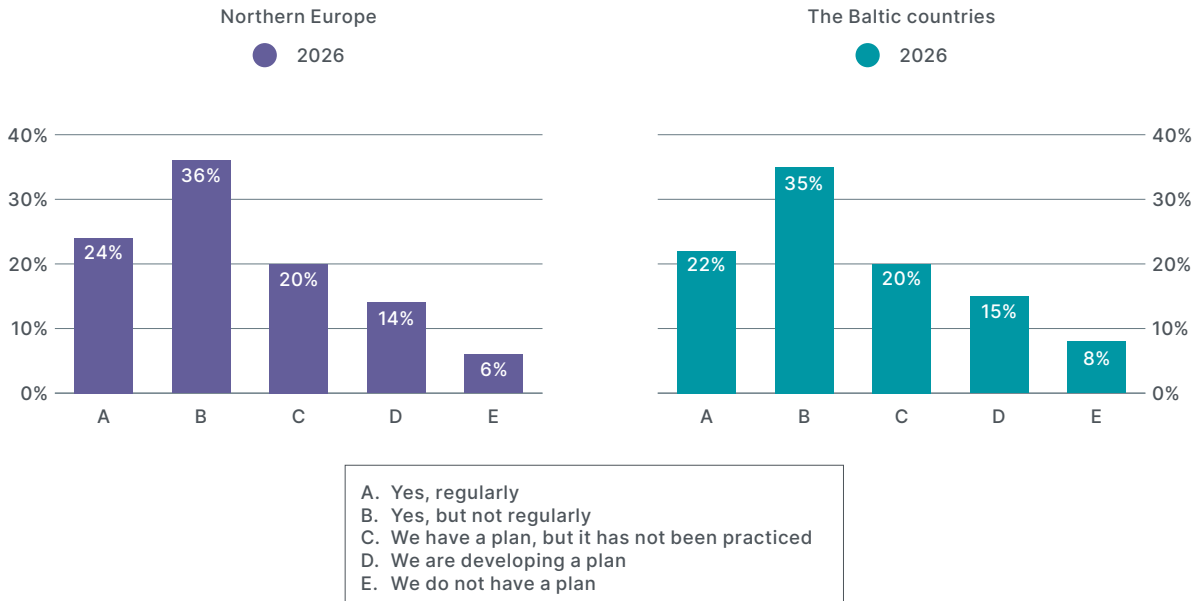
incidents, likely due to stronger detection capabilities and broader attack surfaces. Less mature organizations may simply detect fewer events, making “no incidents” an unreliable indicator of safety. Strong detection and monitoring are essential to understanding true exposure. Larger organizations experience 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.

Key Takeaways: Baltics

→ In the Baltics, the experience of cyberattacks has dropped from 26 to 14% and is now on a par with the rest of Northern Europe. AI is enhancing the speed and sophistication of these attacks and is recognized by the European Union Cybersecurity Agency (ENISA) as a significant risk. Many organizations struggle to distinguish between corporate and personal use of AI tools, creating potential unassessed risks.

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



Most Plans Remain Untested Until They Matter

Key Takeaways: Baltics

→ 8% of the Baltic organizations lack any plan for unforeseen events, which exceeds the Northern European average, while 15% are in the process of developing one. This points to a lower security maturity level. The lack of incident or business continuity plans heightens the need for continuity management, especially amid geopolitical risks and previous continuity issues.

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.

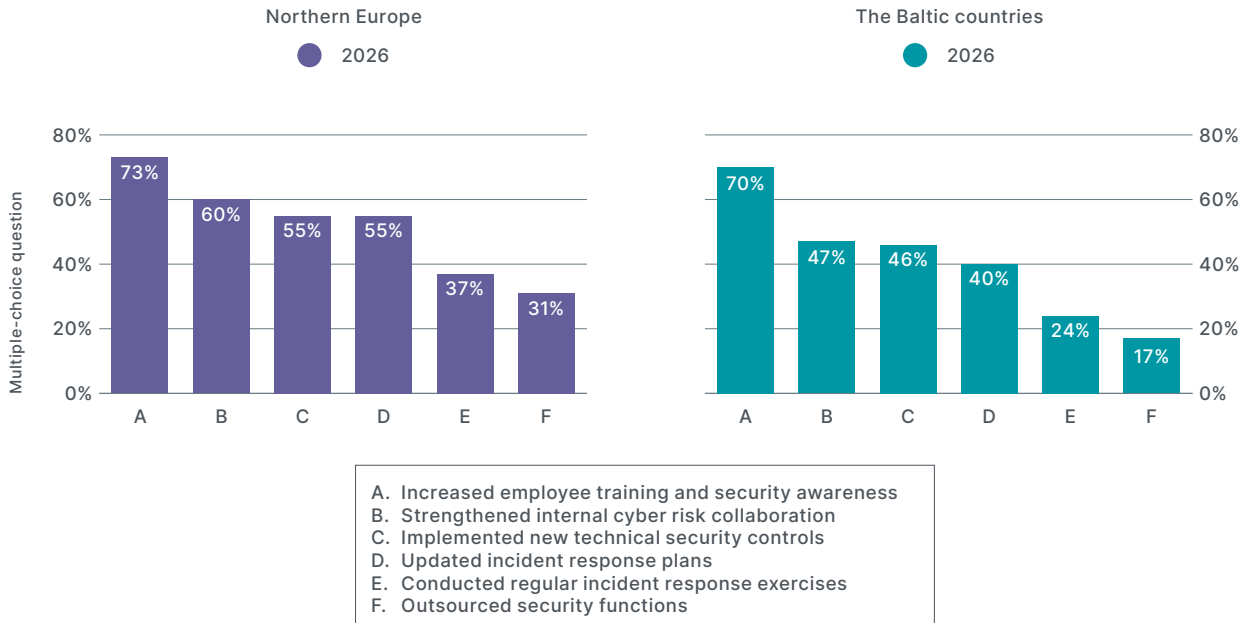
Current practice tends to emphasize external attacks. Scenarios involving ransomware, infrastructure breaches, or other outside threats dominate tabletop testing. Insider-related events are rarely included, even though these situations are harder to detect and require rapid assessment. This leaves a 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 unfore-

seen 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?



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.

Key Takeaways: Baltics

→ Baltic organizations typically enhance employee security training to address evolving threats, as it is both cost-effective and compliant with regulatory requirements, particularly in governmental sectors. However, overall adaptations to threats are constrained by low maturity levels in security responses. Effective resource management in the new context is essential, and organizations are encouraged to explore EU funding programs for IT and cyber security.

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



"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.

act, for example, before an email reaches the wrong recipient.

"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."

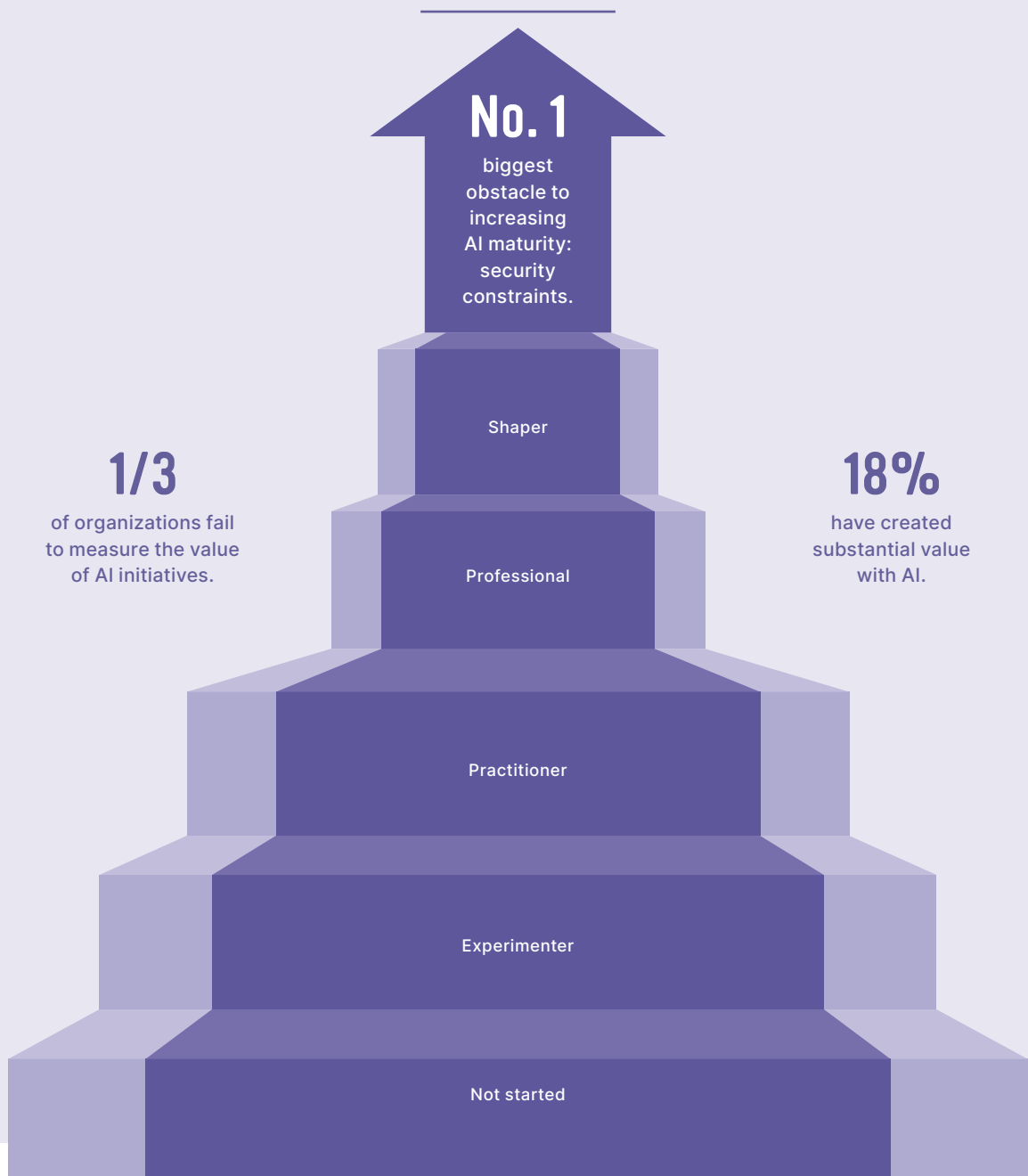
Looking ahead, knowing exactly where your data resides and what you actually commit to when choosing a platform will matter at least as much as traditional security.

"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.

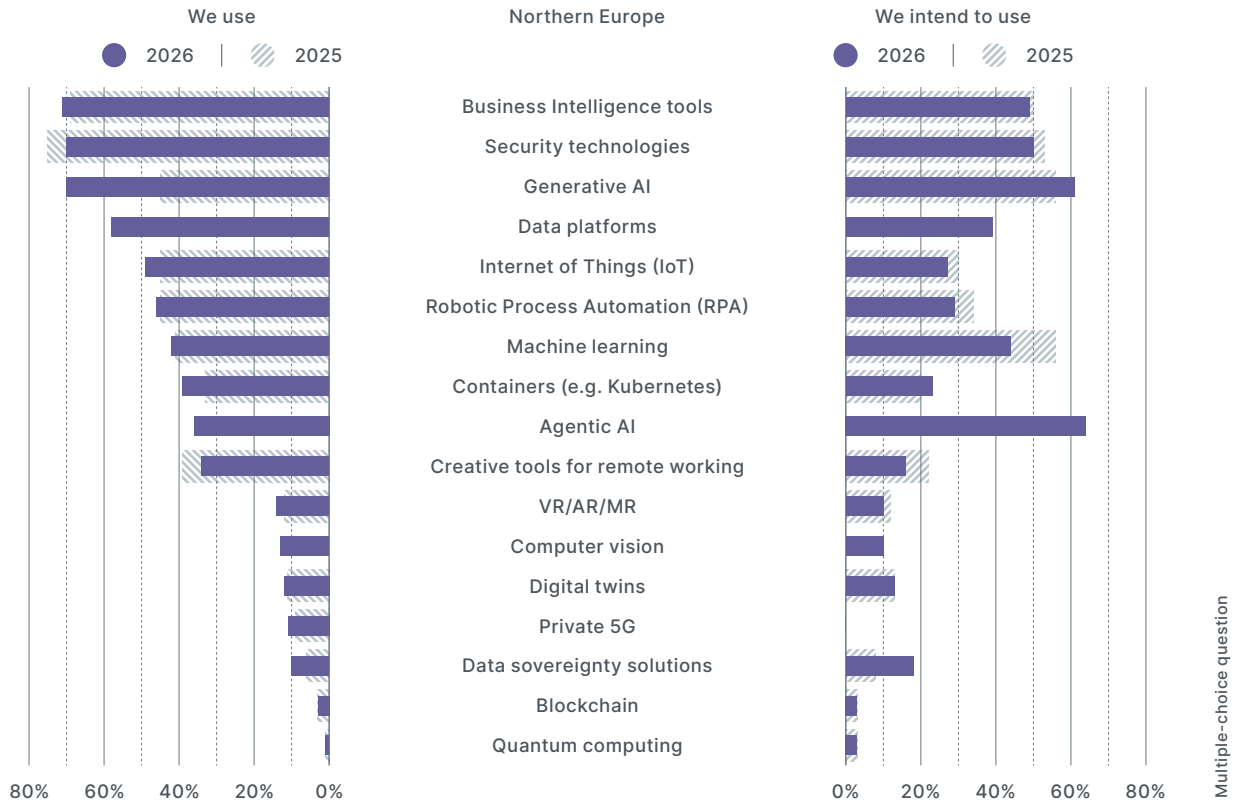
"We advocate for sharpening that awareness, within our own organization and among our customers." ●

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.



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



From Assistants to Agents: The Next Phase of AI Use

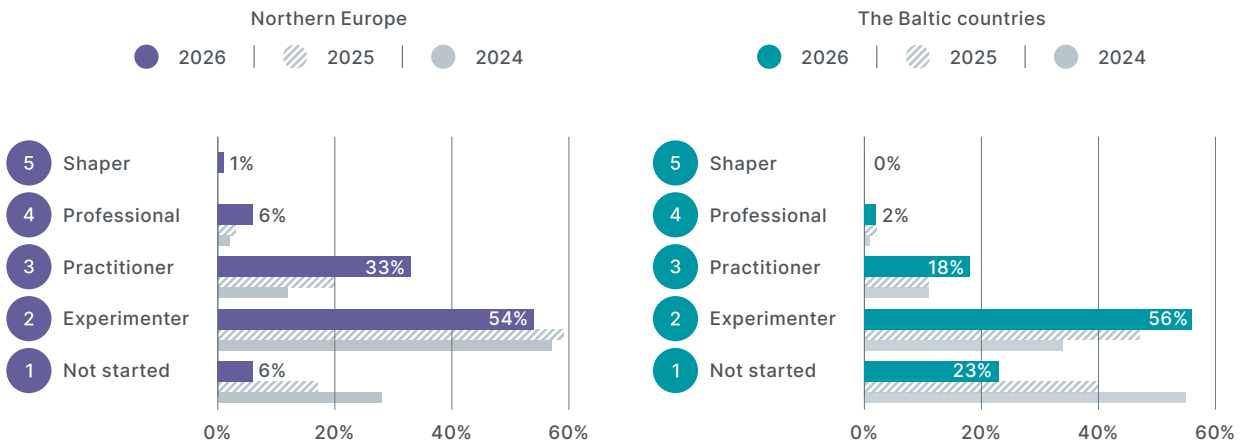
Key Takeaways: Baltics

→ IT decision-makers in the Baltics say they will use security technologies more in the future. They will also use more robotic process automation, which is seen as safer and easier than AI-driven methods. Generative AI and agentic AI are on the rise. Machine learning adoption is declining slightly, due to more pre-built solutions available in the market, negating the need for custom development.

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?



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% at levels 3 to 5 compared to

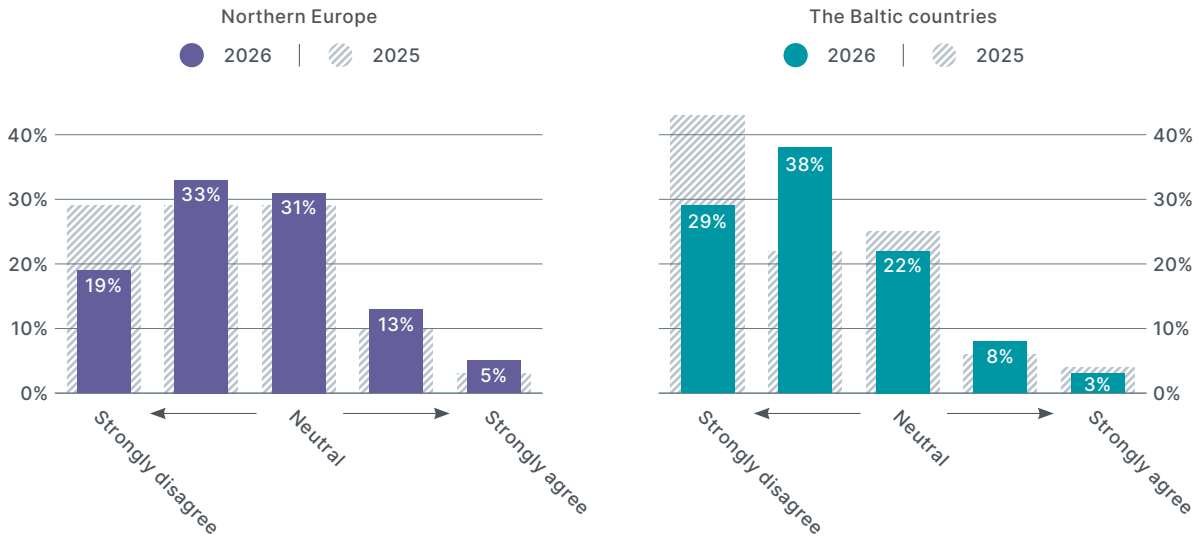
the regional average of 40%. Organizations in these maturity levels also report greater value creation. Lower-maturity organizations continue to experiment without consistently evaluating their results.

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.

Key Takeaways: Baltics

→ Baltic organizations are making progress in AI adoption, yet the maturity level remains low, with many still experimenting and 23% not yet engaged. Current AI use focuses predominantly on content creation and coding support. In countries further ahead the value of AI is still lagging, so there is potential for Baltic organizations to leverage lessons from others for safer progress. Data management challenges are less prevalent in the Baltics (25%) compared to Northern Europe (34%), but may rise as developments continue, presenting an opportunity for proactive solutions now.

My organization has created substantial value with AI.



AI Value Creation Rising Slowly Despite Rapid Maturity Growth

Key Takeaways: Baltics

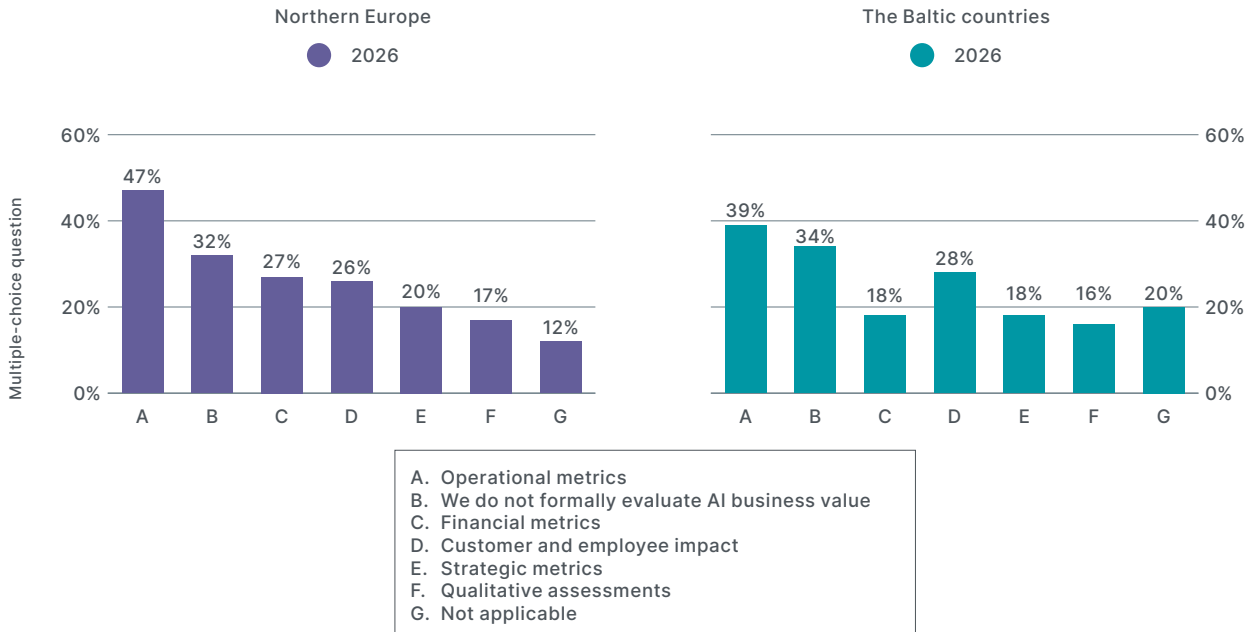
→ As a natural consequence of the lower AI maturity in the Baltics, most Baltic organizations perceive limited value from AI. Many are in an experimental phase without measuring its impact. Additionally, the measurement of AI's value varies by sector, with larger organizations better positioned to allocate resources to AI initiatives. Smaller organizations find AI too expensive or complex to generate benefits. Views on value differ: the public sector emphasizes modernization, while the private sector aims for economic gains, which are harder to realize due to cost pressures and competitive forces.

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?



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.

Key Takeaways: Baltics

→ In the Baltics, financial metrics are less utilized for assessing AI initiatives compared to the rest of Northern Europe, reflecting lower AI maturity and adoption levels. IT decision-makers in the region must adopt a more strategic approach, considering global trends, preparing for enhanced AI maturity and technology adoption in the coming year, while emphasizing value measurement through financial metrics.

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



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

Vytautas Bitinas, Chief Technology Officer, LTG Group.

quadruped robots that inspect trains in narrow spaces and collect visual data in all weather conditions.

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.

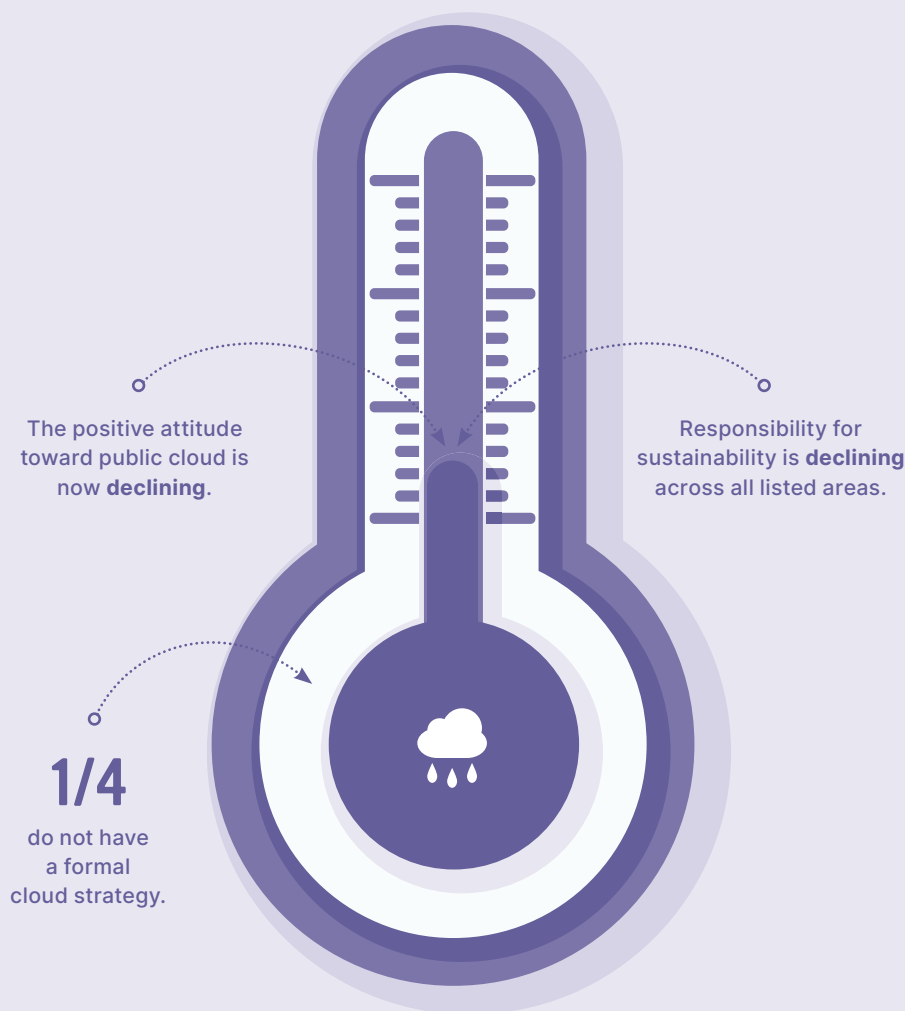
Together, these realities make LTG's transformation especially complex. Cybersecurity, governance, and data control shape every discussion, while many projects involve sensors, robotics, communications, and operational technology alongside software. "What problem does this solve? Where do we save? What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

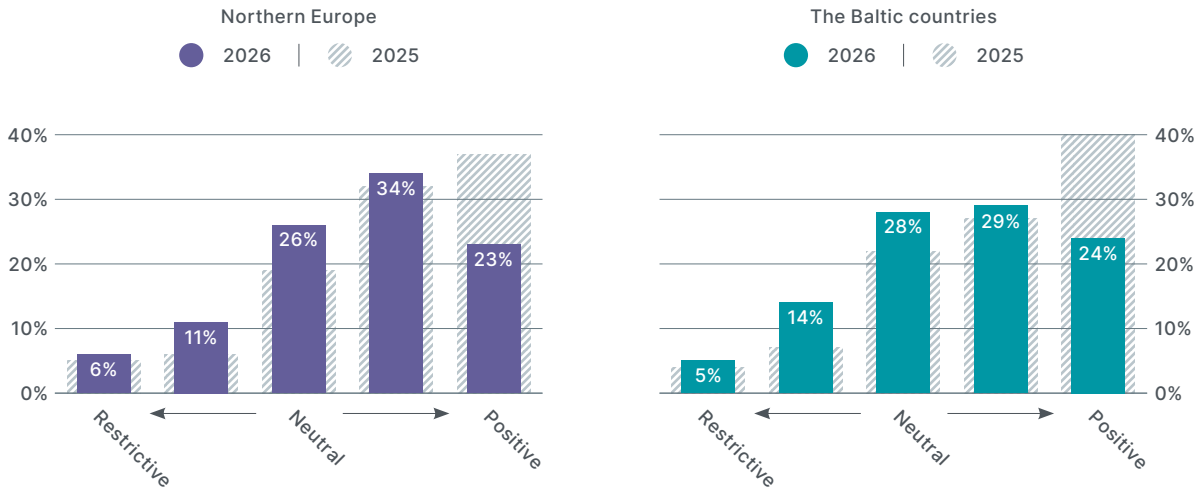
Bitinas does not speak about transformation as a slogan, but as a series of decisions, tests, and trade-offs inside a critical system that has to keep moving. In that respect, LTG's direction is a practical rethinking of how a modern railway should run. ●

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?



From Optimism to Neutrality: Attitudes Toward Public Cloud Shift

Key Takeaways: Baltics

→ Security concerns are the main barrier to public cloud service adoption in the Baltics. On the other hand, it is interesting that only 13% perceive sovereignty and geopolitical concerns as the biggest barrier, compared with the 40% average for Northern Europe, while high cost (38%) exceeds the Northern European average (30%). Key motivations for public cloud use include availability, scalability, and functionality not achievable in-house. Additionally, public cloud is viewed as an operationally efficient alternative to traditional IT.

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.

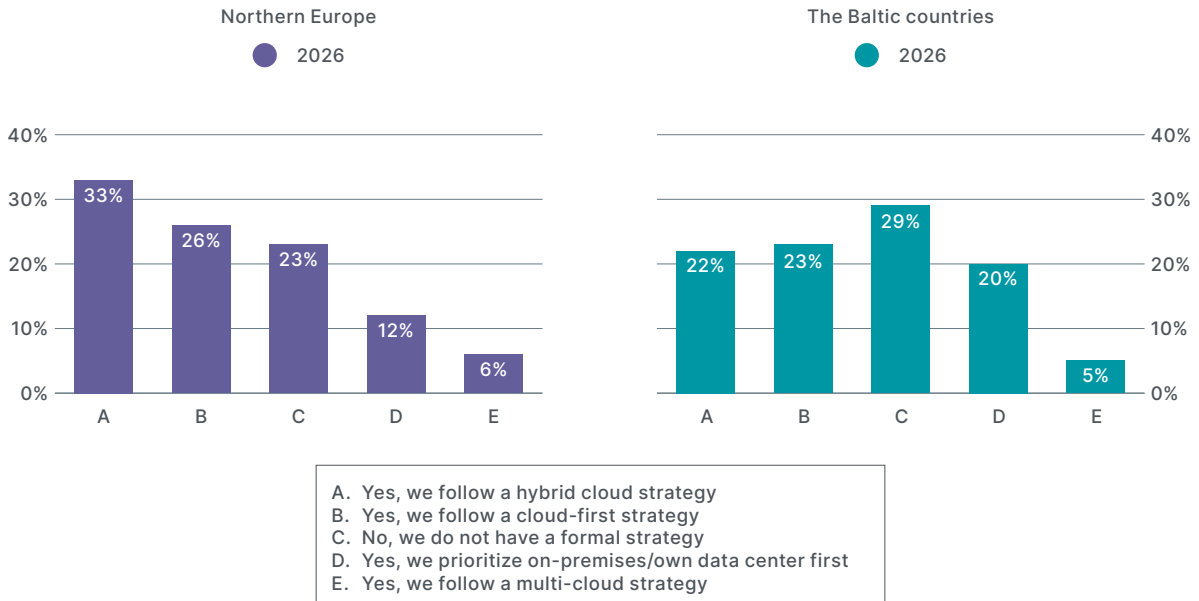
The pattern differs across sectors. The private sector shows a steeper decline in strong positivity, falling from 45 to 26%. Meanwhile, the public sector has decreased from 26 to 18%, indicating different starting points and degrees of change.

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?



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% in the private sector lack a strategy. The corresponding share in the public sector is 32%. 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

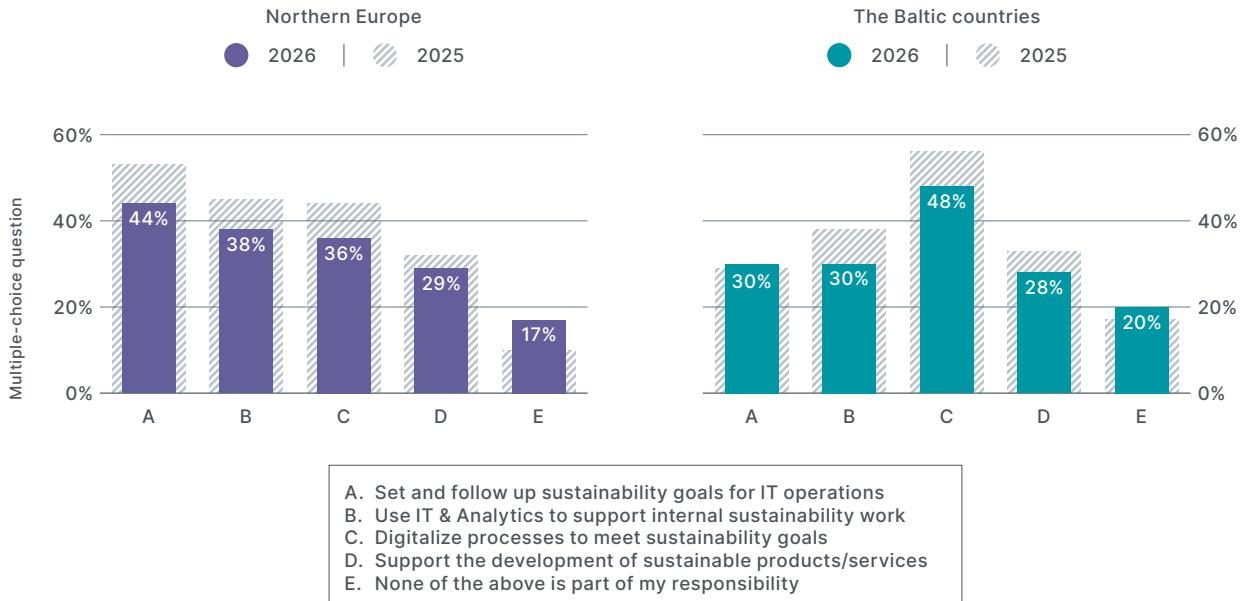
the core of cloud strategy decisions. While sustainability is often promoted as a cloud advantage, it carries little decision-making weight (10%) compared to security (74%) and cost (68%).

Despite security being a top workload factor, workload-specific risk assessments are limited (17%). 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.

Key Takeaways: Baltics

→ 70% of Baltic IT decision-makers prioritize security requirements when deciding on cloud workload placements. The next most important factors are the total cost of ownership (67%) and technical capabilities (36%). 29% of the Baltic organizations don't have a formal cloud strategy, compared to the Northern European average of 23%, and as many as 20% prioritize on-premises and own data centers, much higher than the 12% average for Northern Europe. This could be a security issue, but it may also be a matter of maturity.

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



As Priorities Shift, Sustainability Risks Losing Its Place

Key Takeaways: Baltics

→ In the Baltics, IT decision-makers face security and resource pressures, often sidelining sustainability as a primary focus. However, sustainability is increasingly integrated into operations through digitization of business processes and system improvements. Automation is a key priority in addressing limited resources, offering opportunities to enhance sustainability by utilizing it alongside digital transformation for efficiency and better reporting. Effective governance leads to better sustainability outcomes, showing that resilience and security contribute to ongoing sustainability efforts.

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?



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%. 13% 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.

Key Takeaways: Baltics

→ This report shows that Finland has the highest proportion of women in IT (24%) and Norway the lowest (17%). The Baltics show a modest 19% representation. Major factors contributing to this gender gap include educational stereotypes and a lack of internships. IT education is often focused on programming, limiting awareness of diverse job roles. This leads to an approximately 80% male student demographic in IT studies, according to statistics from the universities, reflecting into the job market. Stereotypes surrounding IT as a male profession also hinder female visibility, discouraging new entrants.

When the Cloud Starts Running the Show: How Apollo Took Back Control

Apollo Group has come a long way from its roots as a bookstore, first opened in Tallinn in 2000. Since then, the company has expanded into cinemas and restaurants, growing into a leading entertainment operator in the Baltics. Today, the group employs over 4,000 people, serves more than 1 million club members, and generates a net profit of €3.8 million, while pursuing ambitious expansion in Finland. Behind the scenes, that means an IT environment where downtime isn't really an option and where systems need to scale as quickly as the business does.

For Apollo's Head of IT, Vsevolod Boikov, the cloud is less about technology and more about discipline.

"At one point, we realized we didn't fully understand what was going on anymore," he says. "The infrastructure was growing, but the benefits weren't keeping up. Costs told the story. To maintain the same level of service, the team kept adding resources — even though the number of users hadn't changed. Nothing dramatic at first. Just an extra €500 a month. Then another. And another. Until hosting alone was costing close to €50,000 per month — a level we find hard to justify."

The turning point came with a closer look at their cloud architecture — and a conscious effort to build in-house expertise. Within a year, Apollo had cut its cloud costs nearly in half.

But cost wasn't the only issue. Reliability was, too. A single technical failure or DDoS attack could take the entire service offline globally. The fix was structural: systems were split and segmented so that one failure wouldn't bring everything down with it.

Today, Apollo's stance on the public cloud is firmly positive. Microsoft Azure, in particular, has become a core part of the company's infrastructure, enabling both scale and speed. But the mindset has shifted.



"It's very easy to add resources. What's much harder is understanding whether you actually need them."

Vsevolod Boikov, Head of IT, Apollo Group.

If the early promise of the cloud was speed, the reality, Boikov says, is control.

"Without actively managing it, you lose visibility, and once that's gone, efficiency follows."

That shift has also changed how the team works. Cloud management is no longer a shared responsibility across development teams; it now sits with a dedicated DevOps function. According to Boikov, the impact has been clear across the board — from cost to performance to risk.

Even so, cost control remains the hardest part.

"It's very easy to add resources," he says. "What's much harder is understanding whether you actually need them."

That tension — between performance and cost — doesn't go away.

It becomes part of the day-to-day.

The cloud offers flexibility and speed, but it doesn't remove responsibility. Some things, like scalability, are best left to the cloud. But architecture and cost discipline, Boikov argues, can't be outsourced.

Not everything belongs in the cloud anyway: some systems like HR or finance, for example are still simpler and cheaper to run on-premises. Legacy systems and licensing constraints can also make full migration impractical.

Apollo's experience is a reminder that moving to the cloud is not the same as mastering it.

"The cloud gives you tools," Boikov says. "It doesn't necessarily solve all your problems."

The real work lies in finding the right balance — and having the capability to manage it. ●

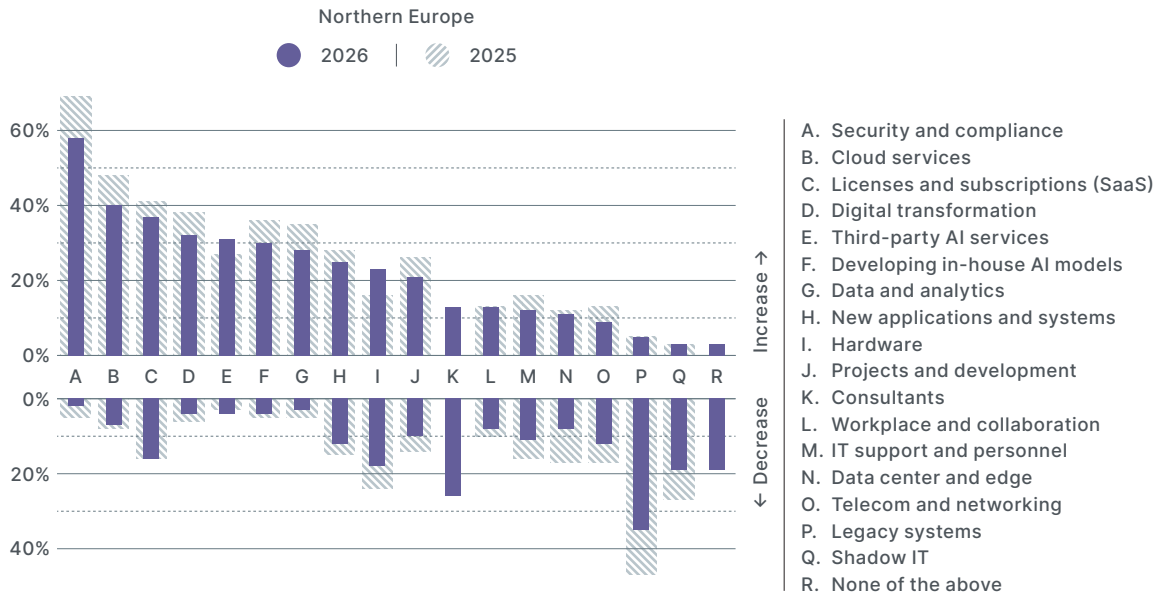
Making Room for What Matters

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...



Multiple-choice question

IT Spend Rises, but Priorities Shift

Key Takeaways: Baltics

→ The Baltics show a higher proportion of organizations maintaining their IT budgets compared to Northern Europe. Despite this, 47% plan to raise IT spending by 10% or more. Spending on hardware varies among organizations, influenced by price increases for some and past investments for others. Future IT spending is expected to focus on security and cloud services, while spending on legacy systems will decrease less than in other countries.

IT budgets in Northern Europe continue to rise, with over half of organizations increasing spending by 10% 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.

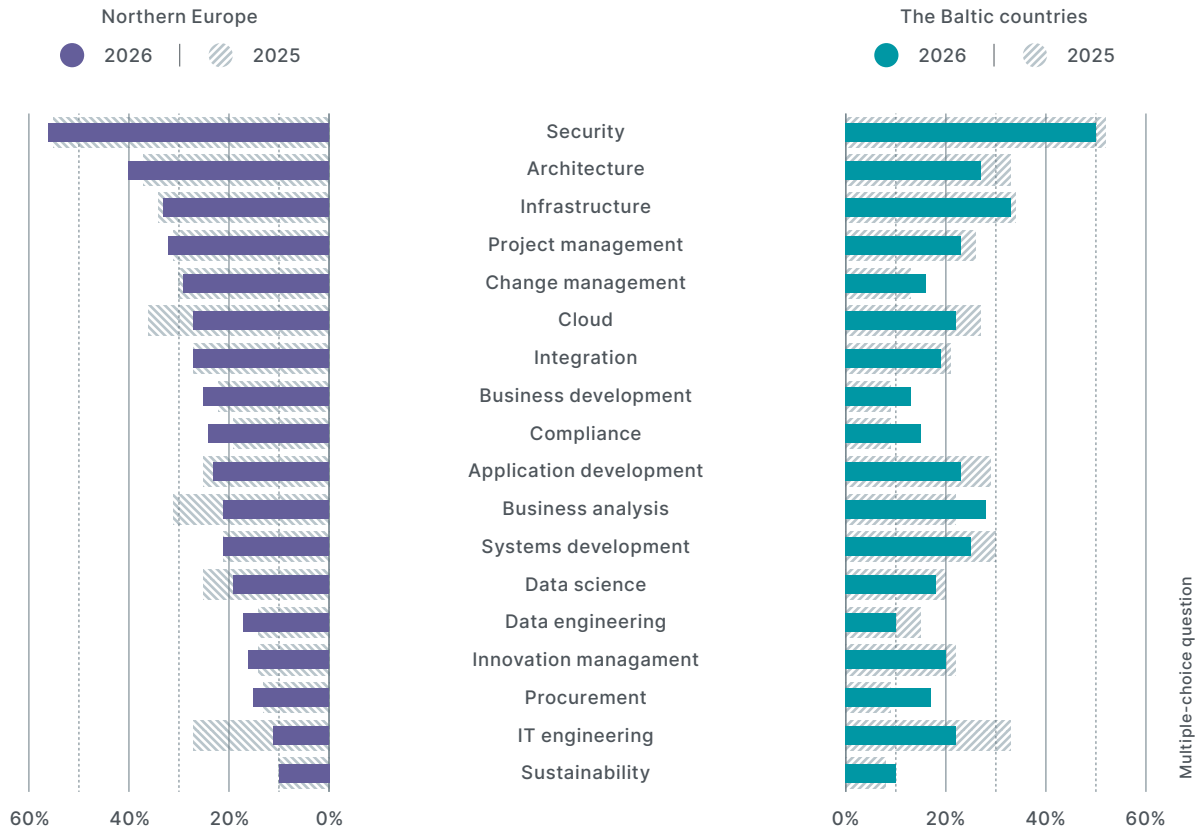
Security and compliance dominate the increases. Heightened threats and new regulations push organizations to strengthen controls, governance, and monitoring before scaling automation or AI. Many lack the skills needed internally, which increases reliance on external partners and managed services.

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.

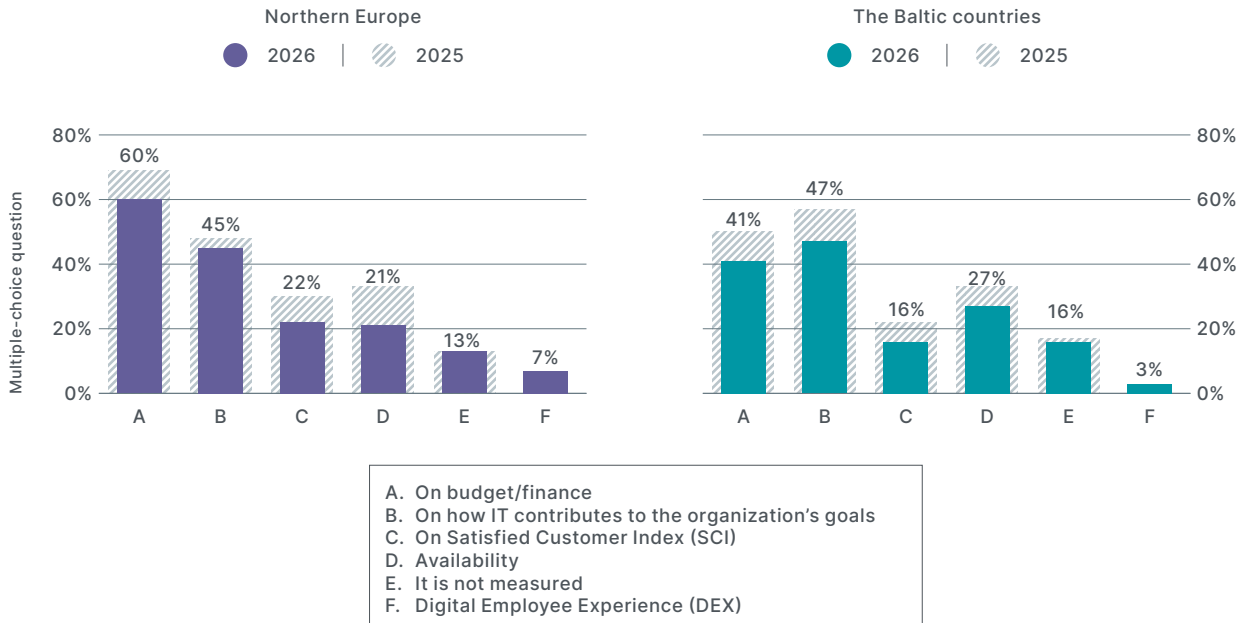
To ensure future capabilities, organizations rely heavily on two strategies: partnering with external consultants and upskilling internal staff. Partnerships help fill critical skill gaps, but many also plan to reduce consultant

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.

Key Takeaways: Baltics

→ According to experts, Baltic organizations are experiencing a talent shortage in security and AI. As a result, they often choose to upskill or reskill current employees and partner with external consultants. 32% choose to hire new talent with required skillsets, compared to the Northern European average of 51%.

How is the IT organization measured and evaluated?



Measurement Frameworks Lag Behind IT's Strategic Role

Key Takeaways: Baltics

→ Most Baltic organizations are less focused on budget measurement compared to Northern Europe, normally emphasizing how IT contributes to organizational goals, though still struggling with productivity. CEOs should prioritize measuring IT departments on goal achievement over budget compliance to foster proactive behavior. Given the smaller size of Baltic organizations, it is crucial that all functions, including IT, recognize and communicate their value beyond budget considerations.

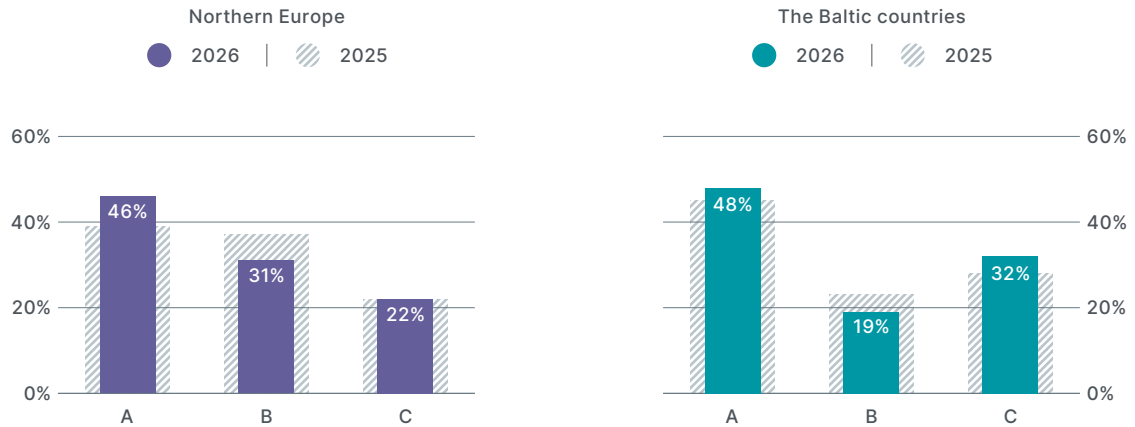
Budget and finance remain the dominant way IT organizations are measured, despite a growing desire to demonstrate IT's contribution to business outcomes. Measurements tied to availability, customer satisfaction, and business value have all decreased compared with last year, raising questions about whether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

nizations 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.

Key Takeaways: Baltics

→ In the Baltics, organizations tend to define IT as either proactive or reactive, with fewer describing an ongoing transition. This indicates clearer expectations of IT's role but also limited tolerance for partial progress. Proactive organizations more often frame IT around value creation, while reactive ones struggle to move beyond operational delivery. The private sector tends to focus on IT's contribution to organizational goals due to competitive pressures. The public sector prioritizes cost efficiency, often selecting the lowest price in procurement over other considerations.

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% 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.



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.

ATERA