Digital Transformation in Denmark 2026-2027

IT in Practice



RAMBØLL

Bright ideas.
Sustainable change.

dansk•it

Contents

Introduction

04 Welcome to Digital Transformation in Denmark 2026-2027, IT in Practice

05 About Digital Transformation in Denmark 2026-2027, IT in Practice

06 Advisory Board

Strategic Challenges

10 Build once, move anywhere: Containerising business applications for digital sovereignty

12 AI implementation requires a conscious level of ambition – it is not a race towards full automation

14 Take responsibility and manage risks as AI impacts your business

16 Avoid AI making your IT organisation better at the wrong things

Digital Agendas

20 Risk-related concerns decline as mitigation moves from agenda into governance

21 AI value realisation is increasing, but still far from the hyped levels, while agentic AI looms

22 Digital sovereignty strategically pursued by only one company in ten

23 Leadership acumen and data quality set the pace of AI value

24 Cybersecurity contingency plans are rarely rehearsed

25 AI governance is rare, and when actually in place, strongest where least complex and costly

26 Software licences beat AI as the fastest-rising cost in the digital budget

27 AI may already be reducing negative implications of digital workforce shortage

Epilogue

28 Methodology & Data

30 About Ramboll Management Consulting & Dansk IT

31 Ramboll Management Consulting supports your digital journey

32 Contact & Information







Welcome to Digital Transformation in Denmark, IT in Practice

2026-2027

For the 31st consecutive year, Ramboll Management Consulting and Dansk IT (the Danish IT Society) have conducted the joint comprehensive study: Digital Transformation in Denmark, IT in Practice, exploring trends, challenges, and opportunities encountered by Danish organisations, as they strive to create value through digitalisation.

IT and digitalisation continue to play an increasingly important role in Danish organisations, particularly when it comes to key themes such as resilience, digital sovereignty, and cybersecurity. Danish companies and public sector organisations are persistently engaged in staying at the forefront, keeping pace with, and capitalising on technological advances. IT and digital solutions not only constitute challenges but also open societal opportunities in terms of efficiency, value, security, and sustainability.

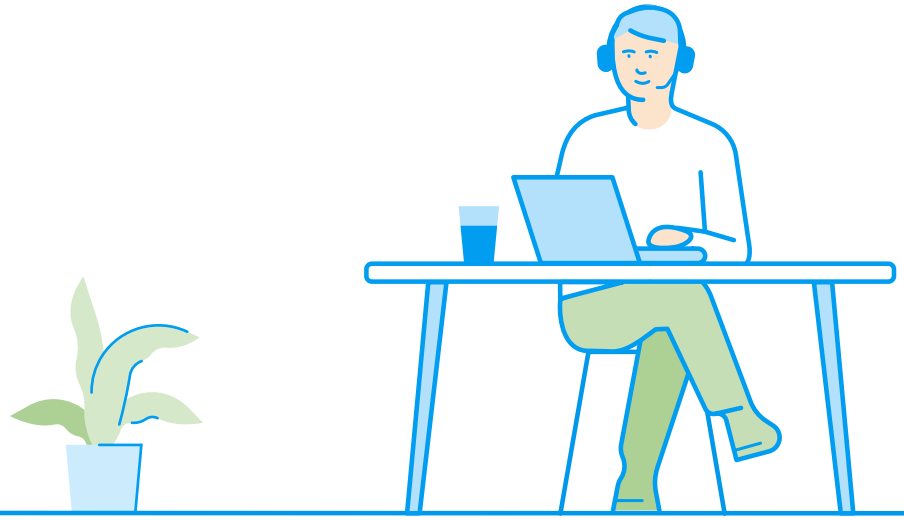
These topics are among the key areas highlighted in this edition of IT in Practice, in which Ramboll and Dansk IT share insights into digital trends, challenges, and opportunities in the digital world.

Through an in-depth survey of IT and business executives in the Danish private sector, IT in Practice provides valuable perspectives on how organisations can understand and manage digital sovereignty and strategy, cyber security, preparedness and resilience, trends in digital investment, and value realisation, risks, and governance associated with the responsible use of AI. On the following pages, you will find inspiration based on the report's insights into the strategic challenges that IT and business directors are facing, as well as the opportunity to explore digital agendas.

In addition to the English report, a Danish-language edition, Digital Transformation i Danmark, IT i praksis®, is also being published, focusing on the public sector.

Our Advisory Board comprises a number of senior executives from public sector organisations and private companies, all of whom have contributed to the themes in this year's edition of IT in Practice. A special thank you to all Advisory Board members for their valuable input and constructive feedback.

Last but not least, a big thank you to the senior executives and IT directors in public sector organisations and private companies who, year after year, share their knowledge and experience by completing our questionnaires.



Enjoy your read!

About Digital Transformation in Denmark, IT in Practice

Digital Transformation in Denmark, IT in Practice is acknowledged by leading CIOs in Denmark. CIO of the Year is a recognition awarded to the CIO who has been the best at managing technology as an engine for growth in a secure, resilient, and efficient manner.

Claus Thomsen
CIO, Lundbeck
CIO of the Year 2026

"AI is developing rapidly, and the opportunities are considerable. But one thing has become increasingly clear to us: the biggest challenge is not the technology itself. It is how we reorganise the organisation around it. It would be a mistake to treat AI as just another IT project. The technology can provide the tools, but value is created when people use them to work differently, make better decisions, and rethink processes. This requires more than just platforms and data. It requires leadership, new skills, and a willingness to challenge existing ways of working.

One of our key lessons has been that the implementation of AI cannot be driven by IT alone. We have deliberately brought together expertise in technology, business, and people, because a successful implementation is as much about behaviour and organisational change as it is about technology. AI is not a one-man project. This also means that we must make AI relevant to day-to-day work. If it becomes too complicated, too controlled, or too detached from the business, the roll-out will be slow. We need clear guidelines, simple frameworks and space for staff to experiment, learn, and share what works.

For me, this is where the real transformation takes place. AI will undoubtedly change our technological landscape, but perhaps its greatest impact will be on how we organise ourselves, collaborate, and lead. The companies that succeed with AI will not necessarily be those with access to the best technology. They will be the ones that are best at unifying technology, people, and business and turn new opportunities into new ways of working."

Claus Birkholm
CIO, NIRAS
CIO of the Year 2025

"The past year has shown us that geopolitical tensions and uncertainty can no longer be ignored in Danish IT departments. We are feeling the consequences directly, both in terms of supply chains, data security and the increased need for agility in our IT strategies. At the same time, generative AI (GenAI), easier access to ML and automation have opened up entirely new opportunities. These new threats and opportunities mean that business and IT have never been more closely linked than they are now, where the ability to quickly integrate and utilise new technologies can make the difference between being at the forefront or being left behind. This requires us as CIOs to take charge of resilience and seize the opportunities offered by GenAI and automation – from smarter data analysis to faster decision-making processes and more efficient and secure workflows. Transparency, flexibility, and the ability to adapt have become key words, and this requires both management and the IT organisation to dare to think innovatively and act with consideration. I look forward to receiving this year's IT in Practice with inspiration for how we can work together to find solutions to the complex challenges we face."

Martin Wood
CIO, Courts of Denmark
CIO of the Year 2024

"Organisations can no longer doubt the strategic importance of mastering the possibilities of digitalisation regardless of whether it is used to deliver public- or citizen-facing solutions or it is used to promote new business models and profits. Business and IT have converged in a necessary and unavoidable interaction that is crucial for success. But strategic choices and competent management of IT consists of a lot of dilemmas and difficult decisions about the future. IT in Practice offers current and relevant insights into the industry's trends and focus areas and thereby contribute to reduce uncertainty and better navigation in the dilemmas. With experience and knowledge, it becomes easier to find the courage to look for new and better ways to utilise digitalisation. Something I am proud about practising."

Susanne Schustin
Global CIO, CEVA Logistics
CIO of the Year 2023 (Blue Water Shipping)

"For a long time, the role of IT within organisations has been undergoing a profound transformation. What was once viewed merely as a necessary expenditure has evolved into the linchpin of digitalisation, innovation, and the formulation of new business paradigms. This shift mandates novel competences and greater expectations, not just from the IT personnel but also from the CIO. Our focus is transitioning from the exclusive domain of operations and service development towards guiding and advising our organisation, its leadership, and board members on the strategic potentials of digital transformation. In my journey to forge robust IT-Business Partnerships, IT in Practice has served as a valuable source of knowledge and expertise, empowering my teams to embrace and excel in this newly defined role."

Advisory Board

Members of the Digital Transformation in Denmark 2026-2027, IT in Practice Advisory Board.

Public Sector

Anders Carlsen
Head of Security, Collections and Debt
The IT and Development Agency of the Danish Ministry of Taxation

Klaus Larsen
Program Director for Digital Health Data
Danish Health Data Authority

Kristian Vengsgaard
CEO
KOMBIT

Lars Frelle-Petersen
Permanent Secretary
Danish Ministry of Climate, Energy, and Utilities

Lone Juric Sørensen
Head of IT and Digitalisation
City of Aarhus

Mette Lindstrøm Lage
Director and Head of the Digital Taskforce for Artificial Intelligence
Danish Ministry of Digitalisation

Michael Ørnø
Director
The Agency for Governmental IT Services

Mikkel Hemmingsen
CEO
Sund & Bælt

Peter Bruun Nielsen
Deputy Director
AU-IT, Aarhus University

Rikke Hougaard Zeberg
Director
The Danish Agency for Climate Data

Willy Kofoed
Director
Department of the Ministry of Food, Agriculture, and Fisheries

Private Sector

Alan Jensen
CIO & Executive Vice President
Salling Group

Carl-Erik Vesterager
CIO
Nordic RCC

Charlotte Hersdorf
CIO
Nordea Finans

Daniel Skovsbo Erichsen
CDO
N1

Haktan Bulut
CITO
ATP

Jens Hartmann
CIO & Group Vice President
Grundfos

Kasper Sckerl
Vice President & Head of IT
Operations & Platforms
Danfoss

Nicolas Skovmand
CIO
Bestseller

Pernille Geneser
Professional board member
& former CIO

Rasmus Lundgaard Pedersen
CIO
OK a.m.b.a.

Ronni Cavling
Data, Automation, and AI Lead
Andel

Steen Guldborg
Group IT Manager
Per Aarsleff

Søren Kofoed Weeke
Former CIO & Executive
Vice President
SOS International

Torben Bonde
Professional board member
& former CIO

Torben Kjær
Professional board member
& former CIO



Strategic Challenges



Digital Transformation in Denmark, IT in Practice highlights strategic challenges that characterise an era of geopolitical uncertainty and constant technological development. This indicative direction requires action if companies are to remain competitive. In addition, there is an obligation to comply with the frameworks governing responsible use of AI. As focus on digital sovereignty and AI grows, IT in Practice introduces tools and action items to address these challenges.

The digital age presents a range of strategic challenges that must be successfully managed by public organisations and private companies in order to conduct their core business and increase their value creation. This year's strategic challenges in the field of digitalisation have been identified by Ramboll through client projects and in dialogue with business leaders, thus highlighting key focus areas that are essential for management in both public organisations and private companies. This section presents insights into the solutions and tools that can support public organisations and private companies in addressing these challenges.

The current geopolitical landscape places further demand on public organisations and private companies. IT in Practice emphasises, particularly the challenges involved in achieving digital sovereignty, where striking a balance between flexibility and integrated solutions requires strong strategic prioritisation and risk management.

Furthermore, focus on AI continues to grow, presenting a range of challenges relating to ethics and accountability. Closely connected to this, IT in Practice also focuses on how we can measure AI implementation in our organisations, providing an effective model for this.

On the following pages, each strategic challenge is presented individually and supplemented with a conceptual framework and practical instructions for addressing the given challenge.

Strategic Challenges in Digital Transformation in Denmark, IT in Practice

01 Build once, move anywhere: Containerising business applications for digital sovereignty

02 AI implementation requires a conscious level of ambition – it is not a race towards full automation

03 Take responsibility and manage risks as AI impacts your business

04 Avoid AI making your IT organisation better at the wrong things

Build once, move anywhere: Containerising business applications for digital sovereignty

Digital sovereignty is not something you either have or lack – it is a scale you move along. Though containerisation alone is not sufficient to achieve sovereignty, it may be the most practical way to turn exit plans into actual capability, whilst modernising legacy systems along the way.

Ask a board whether the organisation could relocate its critical systems to another provider, the answer is usually: "In theory". In practice, very few could do it within months, let alone weeks. The gap between theory and practice is where digital sovereignty is won or lost.

Sovereignty is a scale, not a status

Digital sovereignty is not something you simply have or lack. No organisation will operate entirely on technology it controls, nor should it try. A realistic goal is a level of supplier lock-in the board finds acceptable; one where switching, should it ever become necessary, would be demanding but possible. Services can be repriced, restricted, or withdrawn overnight. The value lies in the option to switch. You may never exercise it, but having the option strengthens both your negotiating position and your resilience. It is also a management responsibility. The Danish NIS2 law places supply chain risk firmly with management, and DORA already requires financial entities to hold exit strategies for critical IT providers.

What is containerisation?

Think of a shipping container. Before its prevalence, every cargo was loaded differently. Now, the same cargo can move from ship to train to truck without being repacked. Software containers do the same for applications. Each application is packaged with everything necessary into a standardised unit based on open industry standards and built with tools such as Podman or Docker. An orchestration platform – today almost always open-source Kubernetes – then runs and manages these units at scale. Since a container does not care what lies beneath it, the same workload can run on a hyperscaler, a European provider, or in your own data centre.

Portability as a sovereignty currency

Most sovereignty debates ask where data lives. Containerisation opens up a more useful question: how easily can we relocate? When workloads are containerised and run on standard Kubernetes, the cloud provider becomes a replaceable layer rather than a foundation. Exit plans stop being documents and become something you can test. Hybrid setups become realistic, with sensitive workloads on sovereign or on-premises infrastructure and remaining data wherever it makes most sense. And the supplier dialogue changes, because both sides know you can switch.

More than one win

The sovereignty case grows stronger with three further benefits:

- *Modernisation and skills.* Containerising legacy systems is a chance to move them onto technology already familiar to today's graduates, while expertise in ageing platforms is retiring. However, the change impact does not disappear – it moves, as operations teams face a real shift in how they work.
- *Security.* Containers are no fortress, as they share the underlying operating system. But standardised builds, faster patching, and clearer segregation between systems allow for greater control and transparency than a sprawling legacy landscape.
- *Resilience.* The ability to redeploy workloads elsewhere is a genuine continuity capability. When a provider, region, or data centre fails, portability becomes recovery.

A reality check

Containers make workloads portable, but lock-in does not vanish – it moves. It moves into the managed databases, identity services, and proprietary features wrapped around your containers. It moves into vendor-specific flavours of Kubernetes. And it moves into your data, which is heavy and costly to relocate. Sovereignty is only as strong as your least portable dependency. Containerisation must therefore be paired with deliberate choices at every layer of the stack: open standards, portable data services, and identity you control. Freeing the cloud layer while staying locked in elsewhere simply relocates the problem.

Nor should everything be containerised. Mainframe workloads, large monoliths, and commercial software without vendor support are often better left alone or replaced. And Kubernetes is complex. Without a dedicated platform team delivering containers as a service, complexity can quickly outweigh the gains.

The bottom line

Containerisation is not a sovereignty solution in itself – it is a lever. Used effectively, it turns exit strategies from merely words into real capability, while modernising your system landscape and strengthening security along the way. Used carelessly, you simply swap one form of lock-in for another. The difference lies in the choices made around it. Where your data lives matters – but how easily you can relocate matters even more.

Where containerisation moves the lock-in needle

Containerisation has its greatest effect in the middle of the tech stack. Overall level of sovereignty in the organisation is set by the layers with the highest dependency. Therefore, every layer calls for a deliberate choice.

TECH STACK	DEPENDENCY	CHANGES & BENEFITS
SaaS & end-user tools	**High**	No direct effect, though frees capacity to tackle these separately
Applications	**Low**	Packaged as portable, standardised units, allowing for modernisation; skills that match new talent
Identity & security	**Medium** Identity often tied to provider	No direct effect on identity; clearer separation between systems, though potential for faster patching
Orchestration (Kubernetes)	**Low** If standard; high if a proprietary flavour	One common control layer across environments, allowing for the same way of operating everywhere
Cloud platform (IaaS)	**Low**	Provider becomes a replaceable layer, enabling exit options, hybrid set-ups, and negotiating power
Data	**High** Data gravity, egress costs	Databases can run in containers, but data must still be moved, though open options such as PostgreSQL become more practical
Physical infrastructure	**Medium** Hardware supply chains	Same workloads run on own or third-party hardware and repatriation becomes possible

Action Items

- Measure your exit-readiness, not intentions. Identify critical workloads, assess how long, costly and disruptive a relocation would be, and let the board decide what level of lock-in is acceptable.
- Standardise on open foundations: open container standards and certified, vendor-neutral Kubernetes. Treat proprietary platform flavours and managed add-ons as calculated trade-offs, not defaults.
- Look beyond the cloud layer. Map lock-in at every level of the stack – data, identity, security, and SaaS. Your sovereignty is only as strong as your least portable dependency.
- Establish a platform team that delivers containers as a service, and invest in retraining operations staff, so the change impact is managed rather than merely moved.
- Secure the supply chain and test the exit plan. Keep software in trusted, ideally self-hosted repositories, verify its origins, and regularly prove portability by actually relocating a workload.

AI implementation requires a conscious level of ambition – it is not a race towards full automation

Most companies are already working with AI across multiple degrees of implementation in parallel – from employee prompts to the first workflows carried out by AI agents. Ramboll's level of AI implementation model allows you to determine your organisation's current degree of implementation, objectives, and prerequisites.

Most organisations have embraced AI extensively and are continually exploring how best to derive value from it. IT in Practice reports, for instance, that 47 per cent of public sector organisations currently use AI to analyse documents and record minutes. As experience is limited and technological development rapid, implementation is taking place in such a way that usage varies greatly across the organisation: some employees use AI on a daily basis, others have integrated AI into their tools, and select departments are experimenting with partially autonomous agents to carry out simple tasks.

As AI applications move from pilot projects to live operation – and when, simultaneously, these applications become more sophisticated – it places greater demands on both the AI solutions available to employees, and the implementation and governance models that must be in place to ensure the organisation's success.

In order to define what is required of the organisation, it is important to have established objectives for the use of AI within the organisation as a whole or within individual business areas and support functions. Ramboll's level of AI implementation model can be used as a basis for this work and enables the organisation to guide the discourse on projects, prerequisites, and expectations. With a common framework, the organisation avoids AI efforts being driven by individual initiatives and supplier promises rather than the organisation's own goals.

Three groups – six levels

The model groups six levels of implementation into three categories, describing the role of AI and the user, the adoption model, and the technical requirements for each level.

At prompt levels 1 and 2, AI improves individual steps in a work task, with each task being initiated by an end user. At this level, the user controls and reviews all steps in the task, and often it may simply be a single step in a work process that is carried out with the help of AI. Adoption occurs locally through inspiration for prompts and specific use cases, and is based on AI support using approved standard tools with little or no integration with the organisation's other IT systems.

At workflow levels 3 and 4, an AI agent carries out a work process under human supervision at every significant stage. It is clearly defined how the workflow is initiated – e.g. a defined action such as the receiving of an email or an alert – and the agent stops again once the workflow has been completed. With automation in task execution, it is essential that the organisation has the necessary governance in place. This typically requires agents to be developed in a coordinated and standardised manner before being rolled out to local teams. At the same time, this places demands on the organisation's IT platform, which must establish an IT architecture including, amongst other things, an agent platform and integrations with necessary systems.

At autonomy levels 5 and 6, AI agents carry out a work task or an entire service area, whilst maintaining supervising their own work processes. Once AI agents are deployed, they perform tasks until they are cut off or discontinue the task themselves due to specified built-in principles. The organisation's role is to establish policies and maintain control over the system. This level of autonomy requires close governance and monitoring, and the agents are typically developed and managed centrally via a shared agent platform that is fully integrated into the organisation's IT platform, including via an identity model that sets the appropriate parameters for the individual agents' scope of action.

Viewed holistically, the responsibility for execution shifts from the employee to the system, deployment changes from local to centralised, and the requirements evolve from those of a tool to those of a platform. Therefore, each level places greater demands on the organisation – not just on the technology.

Identify the focal point

The first step is to understand where the organisation is today by mapping specific AI applications onto the model: Where is AI used as a personal tool? Where is AI integrated into a workflow? And are there areas where agents are already working autonomously? The figure shows where and how the majority of value is created today. This mapping exercise may, e.g., reveal that certain initiatives are operating at a level higher than can be supported by the foundation. An agent operating without a shared platform and without adequate governance is a typical example.

Not everyone has to reach level 6

It is tempting to view the model as a staircase, where the goal is reaching the top. However, the aim is to find the right level. Consequently, both technological developments and the organisation's improved capabilities over time may mean that the goal changes. This might be the case, for example, if a large proportion of the organisation's tasks are rule-based and well-defined. If human judgement is required for key decisions, the workflow levels may be the natural focal point for AI ambitions – even in the long term. The benefit lies in ensuring that processes run securely and efficiently, not in removing human influence completely.

There is also an external limitation. Autonomous agents operating continuously and at scale require significant computing power. Given current data centre capacity, it will not be possible for all organisations to focus their efforts on level 6, even though the solutions exist.

From goals to initiatives

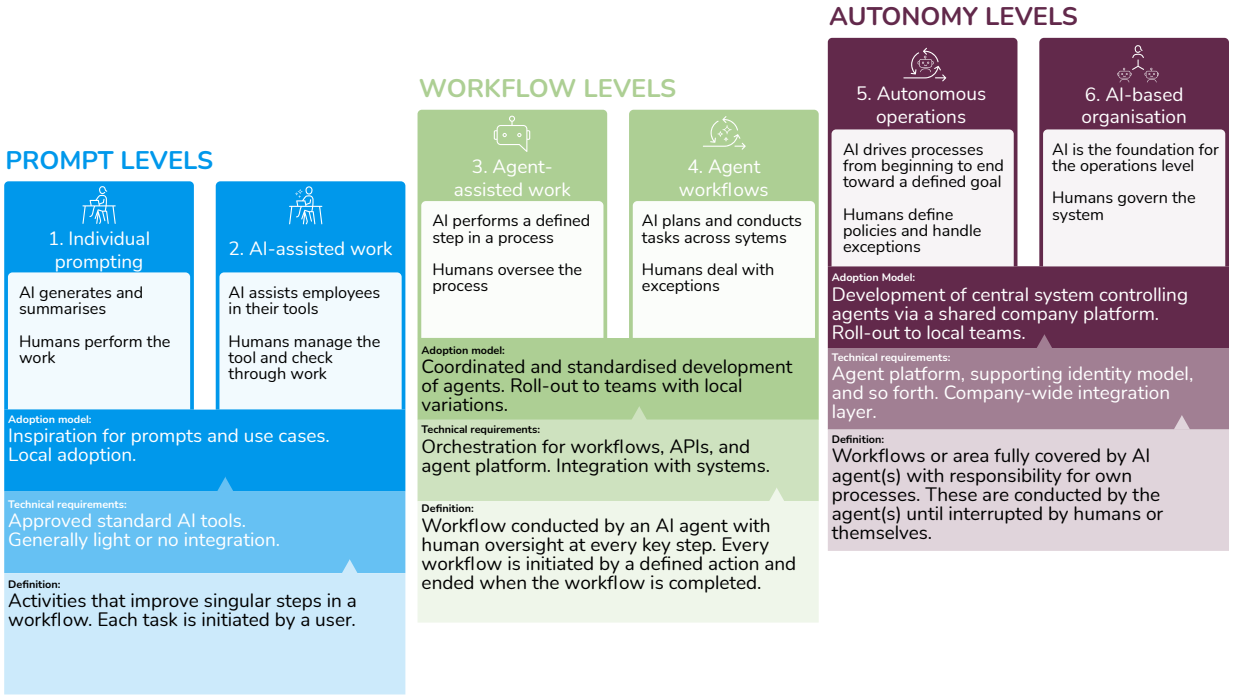
Once the company's goal is clear: What does the organisation currently aim to achieve with AI? Next, the model sets the course: What level do the goals require? What does this level entail in terms of technology and organisation, and what initiatives need to be implemented so that the company can deliver what is required?

This ensures that investments can be justified by specific goals, and that the foundation built is neither larger nor smaller than defined by the ambition.

The level of AI implementation is about reaching the right level and knowing what it takes to get there.

Level of AI implementation

AI applications can range from basic to advanced, fully autonomous use. Each level is suited to its own types of tasks and places increasing demands on technical support and the governance of AI services.



Action Items

- Map current AI applications and identify the focal point – the level at which most of the value is created today.
- Set short- and long-term objectives for AI and determine what level of capability these objectives actually require.
- Identify what the desired level requires of the organisation – both in organisational and technical terms.
- Prioritise initiatives that collectively create the necessary technical and organisational conditions and secure thee foundations before increasing the level of autonomy.

Take responsibility and manage risks as AI impacts your business

AI has begun to transform the global economy, and no one will be left unaffected. This places new demands on how organisations should manage the risks associated with the use of AI – not only within the organisation, but also regarding the environment, people, and society. The concept of 'responsible AI' provides guidance on how to address risks and opportunities responsibly.

No one is off the hook

Regardless of where a company sits in the AI value chain – whether a provider of data and AI models or a user of off-the-shelf AI solutions – it must address the consequences of the decisions it makes. Or of a failure to take tangible action. Responsible AI provides a framework for how organisations can manage this responsibility in a systematic and structured manner, with the OECD setting the standard for responsible business conduct, global AI principles, and most recently, its guidance on responsible AI.

Those organisations that have made the most progress with AI adoption see responsible AI as a catalyst rather than an obstacle. Nevertheless, it is Ramboll's experience that Danish companies are generally still at an early stage of maturity. The hasty roll-out of AI without mature risk management challenges organisational resilience, whilst also potentially impacting the environment, people, and society.

From principle to practice

Ramboll's model for responsible AI is based on the OECD's due diligence framework, which provides a practical, six-step approach; from embedding responsible AI in policies and management systems to managing adverse impacts when they arise. These steps are also reflected in the ISO/IEC 42001 requirements for leadership anchoring and risk assessment, or the EU Directive on Corporate Sustainability Due Diligence. Organisations using the model can achieve a more effective and systematic approach to managing current impacts and risks, tailored to their organisation and associated requirements – regardless of the legislation or standards to which they otherwise adhere. This also means that companies can use the model to assess and document the organisation's maturity in its work with responsible AI.

Responsible AI must be interpreted broadly

Although the six steps in the OECD's due diligence framework also provide a basis for managing risks affecting the organisation itself, the fundamental aim is to ensure that the organisation can effectively manage the potential negative consequences of AI for the environment, people, and society. The better and timelier the handling, the fairer and more legitimate the AI transition will be perceived, whilst also allowing for optimisation of the positive outcomes of AI. The AI transition, including development and use, extends beyond purely technical considerations or the issue of IT security. You need to stay ahead of the curve and assess the impacts as early as possible.

Maturity is more than just a policy

A mature and resilient organisation is not characterised by isolated AI policies, but by the embedding and ownership of responsible AI at the highest levels of management. At the same time, it must permeate the entire organisation and not operate as a separate track alongside the business, as illustrated in step 1 of the model.

Clear roles must be defined, and responsible AI must be integrated into existing governance, policies, processes, systems, KPIs, operational controls, and risk management. Dependencies across the organisation or in relation to external partners should be identified in order to understand where risks and impacts of AI may arise and how they can be handled. AI-related incidents can be serious not only for the organisation itself, but also in relation to the delivery of services to partners and customers. A mature and robust organisation is created by ensuring that employees are equipped to meet the challenges and can act effectively with a clear mandate. It is also important that the necessary resources and incentive structures to support this are in place.

Risk assessments, which form an integral part of step 2 of the model, must be conducted as early as possible – during the design phase or before new AI solutions are implemented – and should be updated regularly in line with technological advances. This particularly applies to agentic AI, where autonomous agents make and execute decisions themselves. We see an increasing number of examples of AI agents being deployed with built-in vulnerabilities or without clear boundaries as to what the agent is authorised to do and when a human should step in. This can have major consequences, ranging from reduced delivery capacity to unintended negative impacts on people or society, such as eroding trust in key societal institutions. Here, the periodic and output-based monitoring that many companies currently use in their governance models is no longer sufficient. Instead, there is a need for a continuous governance model that is technically embedded throughout the agent's lifecycle, e.g. by ensuring that monitoring is built into the agent from start to finish. This involves authority limits (what the agent is permitted to decide), escalation thresholds (when a human must intervene), and logging (traceability of decisions), supported by tools such as automated 'red teaming' , i.e. a systematic, repeated testing of the system's weaknesses, and AI tools that monitor and maintain an overview of the organisation's technology. These processes must be in place to mitigate negative consequences and risks as part of steps 3 and 4 of the model.

Part of organisational maturity is seeing the full scope of the risk landscape. This extends far beyond the technology itself and may impact the environment (such as increased energy and water consumption), people (including the organisation's own employees, who may experience surveillance or exclusion) and society (for example through bias or misinformation).

This broader risk landscape also forms the basis for understanding where the organisation is most vulnerable and where action can be taken to strengthen organisational resilience, e.g. in the event of regulatory sanctions, loss of trust, operational continuity issues, or reduced delivery capacity.

Engagement is not an afterthought

Timely and ongoing involvement of stakeholders (employees, customers, and affected groups) is embedded in all six steps of the model. Such engagement minimises risks, increases the transparency of the use of AI solutions, and strengthens the organisation's legitimacy and competitiveness. In practical terms, this involves genuine feedback channels – from employees who use AI solutions in practice, to customers and citizens affected by the decisions behind them.

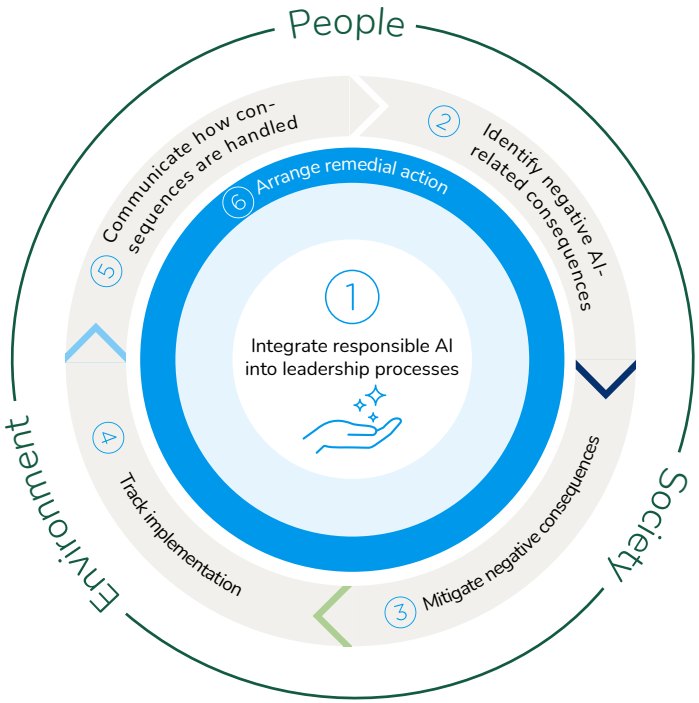
We generally observe that organisations with clear complaints procedures gain early insight into risks and weaknesses before they escalate and potentially become more costly to rectify; similarly, communication with stakeholders can help strengthen trust, address concerns, and create a space for discussion on how AI can be used to the best effect.

Responsibility pays off

Responsible AI not only addresses negative impacts on the environment, people, and society, as well as regulatory compliance, such as the EU AI Act but also goes much deeper. Companies will discover that working systematically with responsible AI contributes to value creation across the entire organisation. This may take the form of greater internal and external trust, a more credible brand, and competitive advantages; it may also mean better insurance terms for those who can demonstrate genuine AI governance and preventive measures. Hence, responsible AI is the foundation for scaling AI safely, both for the company and for the wider world.

The OECD due diligence framework

The OECD due diligence framework supports compliance with legal requirements, including the EU AI Act. The steps are concurrent and iterative – not a linear checklist.



1. Integrate responsible AI into policies, leadership systems, and processes.
2. Identify and evaluate AI-related negative consequences related to operations, value chains, and partners, e.g. by mapping AI-value chains as a first step.
3. Mitigate negative consequences, e.g. by introducing tools to support the handling of risks in the AI system's lifecycle.
4. Track implementation, e.g. by consistently tracking whether the AI system is working as expected.
5. Communicate how consequences are handled, e.g. by communicating around the use of 'red teaming' or what the AI system can, cannot, or should be used for.
6. Arrange or collaborate on remedial action when relevant, e.g. ensure that complaint mechanisms are designed to handle complaints surrounding AI system use, with AI value chains as the first step.

Action Items

- Embed responsible AI in a policy that reflects the OECD AI principles and has been approved by top management. Integrate it into existing governance, decision-making processes, and management systems – not as an isolated compliance function.
- Identify the risks broadly for each individual AI solution in relation to the environment, people (including your own employees), and society, whilst also assessing the organisation's resilience.
- Establish monitoring and reporting procedures. Maintain an ongoing overview of AI applications, incidents, controls, and performance.
- Develop a continuous governance model for agentic AI with clear boundaries of authority, escalation thresholds and logging throughout the agent's entire lifecycle.
- Involve stakeholders early and continuously – thus mitigating risks and strengthening the legitimacy of both the AI solution and the organisation.

Avoid AI making your IT organisation better at the wrong things

AI is reshaping what suppliers deliver, what business teams can do, and where IT creates value. CIOs must rethink the division of work, investment priorities, and strategic control — or risk optimising an Operating Model built on assumptions that no longer hold true.

The biggest AI-driven change to your IT organisation may come from the outside

Software providers are embedding AI into their products. Technology suppliers are reinventing how services are delivered and priced. Business teams can increasingly configure solutions, automate workflows, and act without waiting for IT. Meanwhile, IT departments are using AI to become faster and more productive.

Yet, improvements across the digital value chain do not automatically add up to better business results. AI is changing not only how work gets done, but who should do it, where the next investment matters, and what must remain under the control of the company.

The risk is not that IT fails to adopt AI. It is that IT becomes better at delivering services the business now needs differently – or no longer needs IT to deliver at all.

Two shifts that change the equation

AI is reshaping suppliers, internal IT, and the business at different speeds. Two shifts challenge the assumptions behind today's IT Operating Models.

First, AI changes relative delivery advantages. It changes what each actor can deliver, at what cost, quality, and speed. A service once best performed internally may now become a standard feature of a supplier's product. Conversely, AI may make selected activities more attractive to bring in-house. Neither outsourcing nor insourcing is the inevitable answer.

Consider application management. If a supplier uses AI to deliver the same service with far less effort, who captures the gain? Customers may still be paying according to yesterday's economics. And if internal IT can handle certain changes more effectively, should the sourcing boundary remain untouched? AI turns established contracts and delivery choices into assumptions that need retesting.

Second, AI changes where additional capability unlocks the most business value. Making one activity faster does not necessarily accelerate the whole value chain. If AI speeds up software development while integration, release decisions, or business adoption remain slow, more development capacity may add little value. The next investment may be in a different capability – perhaps outside IT's traditional remit.

The distinction is crucial: who can now deliver work best does not tell you where the next investment will create most value. A CIO may rationally outsource more execution while strengthening internal integration expertise. Or bring selected development work in-house without investing in a larger development function.

Reposition IT – don't just optimise it

These shifts demand more than an AI productivity programme. CIOs must redraw delivery boundaries as relative advantages change, and redirect capabilities and investment towards what now holds back business results. The aim is not to maximise IT output, but to improve what the company can achieve combining digital capabilities.

CIOs must also rebalance strategic control. As suppliers and business teams gain AI-enabled autonomy, ability to execute, authority to take decisions, and accountability for outcomes can become separated. Formal decision rights offer little protection if the organisation cannot understand critical dependencies, change course, or intervene when necessary.

Strategic control does not mean IT approving every solution. It means placing decisions where they belong while preserving the company's practical ability to observe, change, stop, or recover critical digital activities.

Consider AI embedded in business software. A team may be best placed to configure and use it, while its data flows, automated decisions, and dependencies affect the wider organisation. The answer is neither to block local initiatives nor to leave each team on its own. It is to combine autonomy with shared data, integration, visibility, and clear accountability.

The same applies to suppliers: delegating execution should not entail surrendering the knowledge, contractual rights, or alternatives needed to change direction.

IT may therefore become strategically more important, even as it directly delivers less. Its contribution increasingly lies in bringing internal, external, and business-owned capabilities together — without insisting that every decision or transaction passes through IT.

The cost of standing still

An Operating Model can have been right when it was designed and still become wrong as AI changes the capabilities and economics around it. The risks are:

- *Wrong work:* retaining certain activities where others now have an advantage.

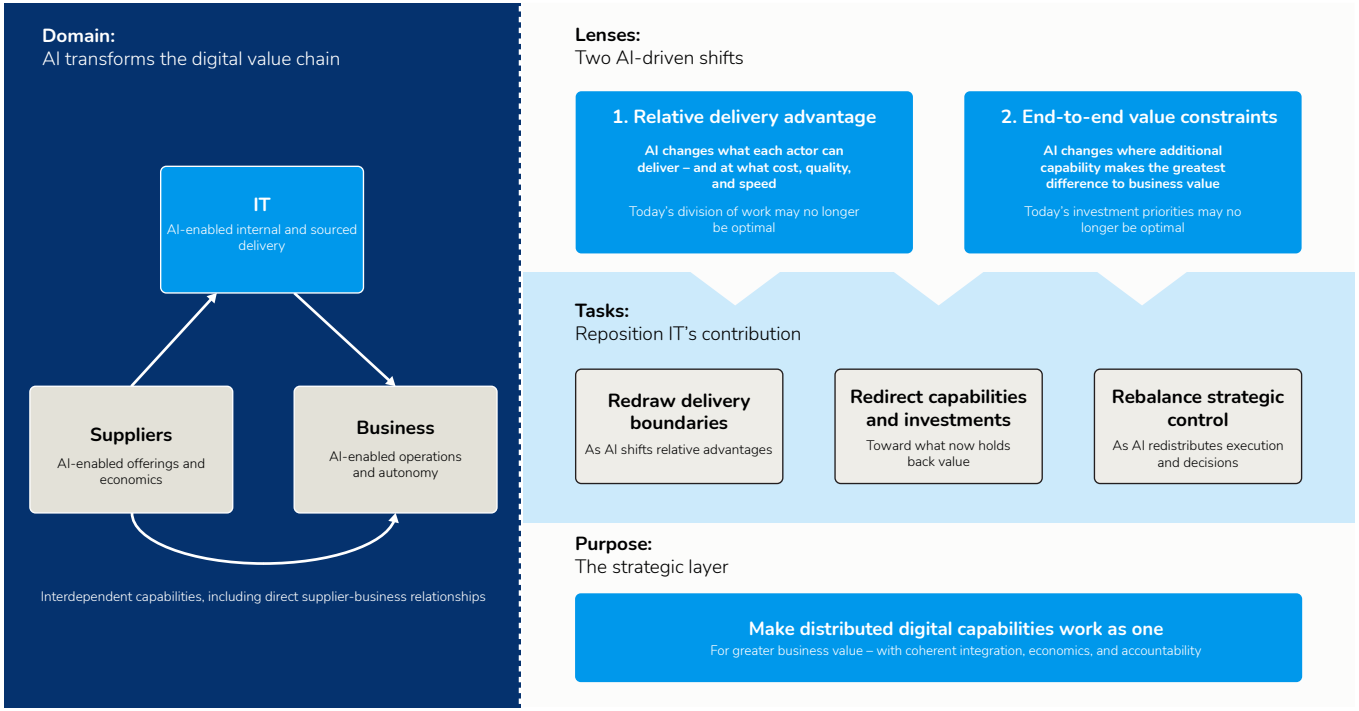
- *Wrong capacity:* investing in output that no longer removes the main obstacle to creating value.
- *Wrong control:* remaining accountable without the practical ability to influence critical outcomes.

An unproductive IT organisation is by no means an inherent precondition for any of these failures to emerge; indeed, all three can arise even as IT performance improves.

The CIO's challenge is not to defend IT's existing territory, but rather to continuously reassess where work belongs, where investment makes the difference, and what the company must be able to control. The outcome is not simply a more productive IT organisation; it is a more valuable digital value chain.

AI shifts where IT creates value

AI changes who can best deliver digital capabilities and where further investment creates value. IT must adjust delivery boundaries, capabilities, and strategic control to make the entire value chain work together.



Action Items

- Retest delivery boundaries: Compare suppliers, IT, and business teams on AI-adjusted costs, quality, and speed. Challenge sourcing decisions in both directions, including opportunities for selective insourcing.
- Invest where value is being held back: Identify what now prevents faster delivery of business results. Redirect resources from isolated productivity gains towards the capabilities that improve the whole.
- Revisit supplier economics: Test whether AI-enabled productivity gains reach your business through better prices or services. Renegotiate contracts and preserve credible alternatives where they do not.
- Preserve strategic control: Clarify who may decide and act, and what the company must be able to observe, change, or stop. Enable local autonomy while strengthening critical shared capabilities.

Digital Agendas



Digital Transformation in Denmark, IT in Practice focuses on the digital agendas that currently most affect Danish companies. This year's report includes topics such as strategic risk mitigation, cybersecurity, harvesting business value from AI and the risks associated with AI, developments in digital spending, digital sovereignty, as well as digital talent pools and mitigation measures.

Digital transformation, along with IT and digital skills, remain a key focus for the private sector. IT and digital solutions are key drivers, not only of value creation and efficiency gains, but also of security.

IT in Practice spotlights how risks related to cybersecurity once again top the agenda for CxOs and how private companies are rarely testing their business continuity plans. Additionally, the report explores how business value can be realised from AI, with adoption increasing. Continuing with the AI topic, the risks and barriers linked to AI usage are also explored, as is AI governance.

Also highlighted are the increasing IT costs across the board, creating further challenges. This year's report takes note of how private companies engage with digital sovereignty and how they choose (or do not) to prioritise it. Finally, IT in Practice continues to focus on how to mitigate the digital workforce shortage.

IT in Practice addresses the topics at the top of the agenda for the private sector, based on input from top executives and CIOs.

On the following pages, each digital agenda is presented individually and supplemented with quantitative highlights from the survey.

Digital Agendas in Digital Transformation in Denmark, IT in Practice

01 Risk-related concerns decline as mitigation moves from agenda into governance

02 AI value realisation is increasing, but still far from the hyped levels, while agentic AI looms

03 Digital sovereignty strategically pursued by only one company in ten

04 Leadership acumen and data quality set the pace of AI value

05 Cybersecurity contingency plans are rarely rehearsed

06 AI governance is rare, and when actually in place, strongest where least complex and costly

07 Software licences beat AI as the fastest-rising cost in the digital budget

08 AI may already be reducing negative implications of digital workforce shortage

Risk-related concerns decline as mitigation moves from agenda into governance

Fewer companies now rank talent, geopolitics, regulation, and top management's digital acumen as critical mitigation factors than they did one year ago – yet each of these factors still holds a significant minority, with several cited by around half of companies. Only cybersecurity is a near-universal priority. The same CxOs call leadership acumen the most significant obstacle when it comes to realising AI value.

Cyber security has become a permanent issue on all strategic risk agendas. Alignment at that level is rare and should be considered not only a company asset but a societal one as well. Yet, contingency plans and executive teams are seldom tested under realistic conditions, top management least of all. Consensus has materialised into rehearsed capability.

Many CxOs appear to be taking a more moderate approach to mitigating the impact of shortages of digital talent. The causes are both cyclical and structural, a distinction essential for long-term workforce strategy.

While fewer (but still a majority of) CxOs signal that they see business risk stemming from insufficient digital awareness among top management, the same CxOs rank leadership acumen gaps as the greatest obstacle in terms of AI value creation.

Half of CxOs still find it critical to mitigate digital risk from geopolitical scenarios. Reliance on non-EU providers remains the baseline condition of European (and especially Danish) enterprise IT, and only a small minority have formulated a strategic position to address this.

While less than half of companies now consider addressing new regulation to be a strategic concern, this is unlikely to reflect a lighter burden. Many pieces of regulation fall within the same planning horizon. It is also possible that regulatory matters have been absorbed into compliance routines and quietly de-escalated as a management topic, a shift facilitated by EU-level signals of simplification.

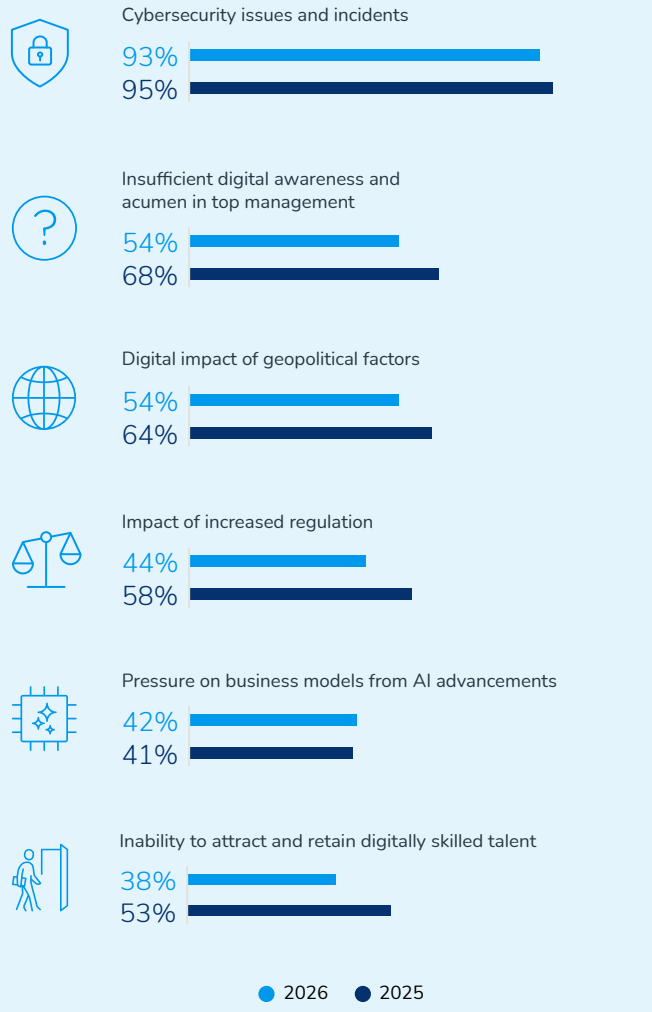
For a majority, AI is managed as an adoption issue targeting incremental value creation, rather than a competitive or existential threat. This may prove a risky approach if AI technologies are on the steep section of an exponential trajectory.

Risks appear to be de-rated at a faster rate than they are resolved, indicating the absorption of risk areas into governance and process. For a CEO, the question is not which scenario poses the greatest risk, but rather which ones have quietly left the agenda while the actual risk exposure remains unchanged or increased.

Strategic importance of mitigating digital risk scenarios

Fewer CxOs rate mitigation of digital risk scenarios as strategically important compared to one year ago, with exceptions in cyber security and AI.

Strategic ranking of CxO risk scenarios



AI value realisation is increasing, but still far from the hyped levels, while agentic AI looms

Market-purchased GenAI tools are driving only modest increases in value realisation from AI adoption, while value from bespoke AI solutions remains unchanged. Companies are occupied with selecting, governing, deploying, and adopting the fast-paced market offerings in GenAI.

AI value is being realised, but in increments rather than leaps. Even the most prominent AI value creators, i.e. purchased GenAI and GenAI embedded in vendor-provided productivity suites, are still reported by less than one-third of all companies. Year-on-year growth rates remain in single or low double-digit territory. A year of arguably unprecedented advances in technological capability has produced only modest gains in business value, indicating that factors other than the purely tech-related come into play with regards to value realisation.

While value gained from freely available tools is at a complete standstill, one-third of companies now report achieving significant value from purchased enterprise GenAI. This is reflective of the very limited scope of legal business use of freely available tools.

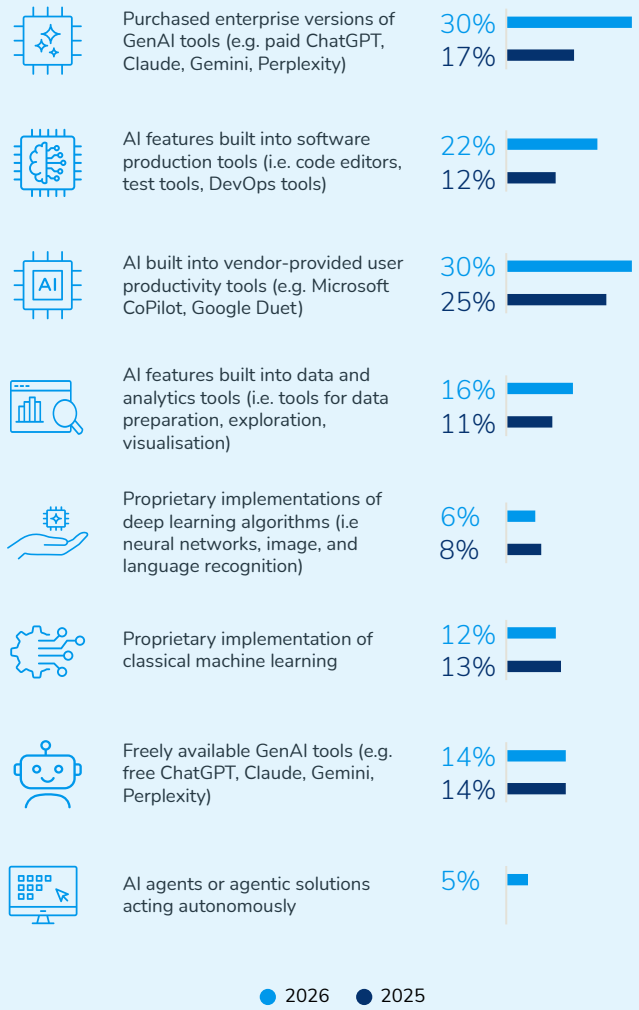
Growth in value from AI features embedded in applications and tools in the data and software production spaces is also visible in the form of defined workflows, measurable outputs and technically capable users. Value from proprietary classical machine learning and deep learning implementations has barely shifted over one year, clearly indicating that algorithmic sophistication is not what drives value; instead selection, governance, deployment, and adoption are key factors here.

One CxO in twenty reports significant value harvested already from autonomously acting agentic AI. Given the relative recent arrival of agentic AI onto the stage, this might be indicative of a significant leap in value over the short term. Agentic AI solutions do not answer questions – they pursue objectives. Given a goal, access to systems and data, they plan, execute, and adapt across multiple steps without human involvement in each step. Agentic AI is not a tool, but an acting entity. Not assisted productivity, but actual execution of delegated work, processes, or functions. Adoption and value realisation from AI agents rely on permission and authorisation structures, identity management, and oversight/audit concepts, rather than licences.

Now is the time for companies to begin deciding who delegates what, to which systems, and under whose accountability – before these technical capabilities arrive in earnest, forcing improvised responses and ad hoc decision-making.

Business value realisation from AI adoption

Value realisation from AI shows modest increases – primarily in Corporate GenAI tools, software production, and analytics. Agentic AI appears on the stage. Ranked by percentage point difference.



Digital sovereignty strategically pursued by only one company in ten

Although one in three companies have performed formal risk assessments, only one in ten have formulated a strategic position in response to their findings. The available toolbox of mitigative actions is used sparingly; even more manageable instruments like encryption and containerisation are not widely deployed.

Reliance on US-based providers of cloud services and Software-as-a-Service (SaaS) is the norm among Danish companies. Seemingly sound commercial decisions taken over the course of decades have produced this shared point of digital strategic exposure. While awareness has caught up, governance has not. Roughly one-third of companies have formally assessed the risks of relying on non-EU providers, yet only one in ten has turned it into a clear strategic position with the aim of reducing this dependency, should regulation or geopolitical developments require it. Few assessments explicitly address extraterritorial legislation such as the U.S. CLOUD Act, which is arguably the most likely trigger for a major sovereignty crisis.

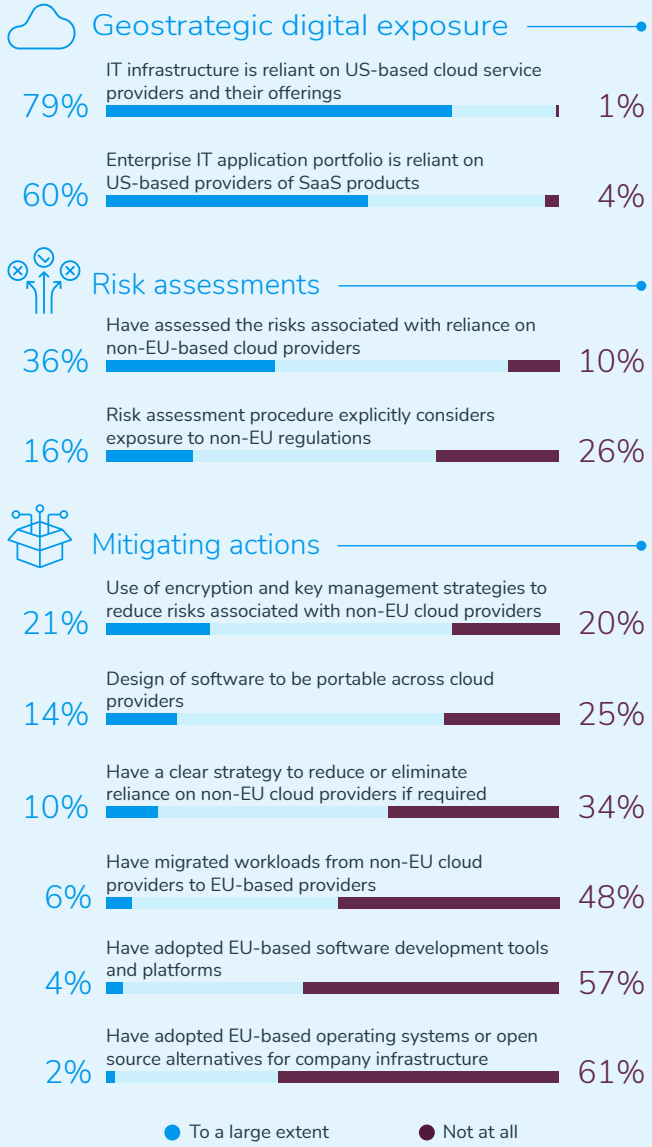
The dependency mitigation toolbox available to companies is used sparingly. Mature, reversible measures that enhance both resilience and negotiating leverage include: Encryption using customer-held keys, and container-based designs portable across compute providers. Yet, only a minority of companies pursue these to any appreciable degree, and a notable share of CxOs cannot even say with certainty whether their organisation does so. Measures such as migrating workloads to EU-based providers or abandoning preferred tools and applications of US origin in the name of digital sovereignty remain a rarity.

CxOs and their boards should consider adopting a more active and explicit position when it comes to digital sovereignty, even if they do not ultimately take steps to actively pursue reduced reliance. Absent a well-formulated strategic position, architecture will default to even deeper lock-ins. Be aware that digital sovereignty and reliance reduction jointly make up a very long play – one plausible strategy is to gradually invest in optionality and flexibility, while not pursuing outright independence. This might entail, for example, funding and initiating an encryption and key control effort to prove feasibility or calculate cost scenarios for shifting workloads via containerisation.

Whatever the risk, corporate risk registers and risk processes should move towards incorporating a digital sovereignty perspective – with owners, triggers, and response plans – into their preparedness strategy.

Digital sovereignty – exposure, assessments, and mitigations

Companies are beginning to take concrete mitigating actions in the long play towards decreased dependency on non-EU based providers.



Leadership acumen and data quality set the pace of AI value

Companies struggle to keep up with rapidly evolving AI, many occupied with creating matching managerial structures and governance. Lack of adequate skills and leadership acumen to cope with these developments is almost universally reported. AI journeys end up greatly inhibited by weak data foundations.

The most reported causal inhibitors to AI business value realisation are not failures in governance, but rather the prerequisites.

Gaps in AI-related skills, capabilities, and leadership acumen are reported by four in five CxOs. Internal technical skills will develop quickly and can be sourced if needed. The gap in leadership acumen is perhaps the greatest barrier, and the one most difficult to address. This gap cannot be filled by recruiting from below leadership levels or delegating to specialists. Leadership acumen accumulates only with exposure, and management should make it a top priority to ensure this.

The ability to sense and judge where AI can and should be applied to radical business change is developed over time through decisions taken. Approaches to governance must ensure that experience is collected, directed, and put to use.

Driven by powerful GenAI tools, AI is quickly proliferating in most business contexts, and the content created goes far beyond text, graphics, and slideware. Thanks to GenAI tools, it is now possible to create functioning applications with business use case features in mere minutes, without having to rely on a software developer. However, two out of three companies report lacking the data foundations and platforms necessary to fully utilise these new AI capabilities. What user-driven AI requires in terms of data is quality, lineage, unambiguous definitions, clear semantics, and well-managed access.

While it might be an easy business win to create AI-generated light applications on top of managed and structured data, such as in legacy ERP, it becomes far more problematic in instances where data definitions are vague and contradictory. Even in companies not focused on unstructured data, some sort of data platform layer will be required to funnel and manage the datasets made available to AI. This is a different exercise entirely compared to traditional business intelligence and reporting and will keep data teams occupied for some time. AI-driven application development on top of data sources known to be of poor quality and consistency should be approached with care.

Inhibitors to the realisation of business value from AI initiatives

Many obstacles inhibit AI adoption and value creation – insufficient skills and acumen first and foremost, but data foundations also spark several concerns.

AI strategy & governance



Insufficient executive alignment and ownership of AI priorities across functions — 54%



Fragmented governance and unclear decision-making for AI investments — 44%

AI portfolio & use cases



Lack of clear linkage between AI initiatives and measurable business value — 65%



Limited ability to scale succesful AI use cases across the organisation — 62%



Difficulty prioritising high-impact AI use cases over low-value experimentation — 53%

Foundation & prerequisites



Gaps in AI-related skills, capabilities, and leadership acumen across the organisation — 81%



Insufficient data foundation and data platforms to support scalable AI deployment — 64%

Cybersecurity contingency plans are rarely rehearsed

Only a minority of companies report to be making use of real-life simulations to test their contingency plans. Experience from real cyber incidents shows that tabletop approaches are insufficient. Live testing exposes gaps in roles, escalation, dependencies, and communication, revealing whether the organisation can respond under pressure.

Cyber incidents are not hypothetical. One in twenty has experienced cybersecurity related incidents with major business impact. For years, IT in Practice has documented the ongoing maturation and refinement of contingency plans. While plans and intentions might be in place, practicing and rehearsing them is an exercise done by few. Only one in four CxOs reports having live-tested cyber attack response plans and business continuity plans to any substantial degree. IT continuity plans, by nature more technical and easier to test, undergo simulations at a slightly higher frequency.

While tabletop reviews might instil a sense of comfort, live simulations are what produce evidence. Forensic breakdowns of real cyber events show that discrepancies in role clarity, escalation paths, third-party dependencies, and mis-managed internal and external communication under time pressure always aggravate negative business impacts. These parameters can only be continuously improved using real-life or simulated testing.

Perhaps the most significant rehearsal gap sits with management. Only one in four top management teams have rehearsed what to do in a cyber-related crisis. This is the case in most companies, even if this management level owns escalation thresholds, regulatory notification clocks, customer and market communication, supplier pressure, and a hypothetical ransom situation.

Both regulations, such as NIS2-implementation (DK) or DORA (EU), and commonly used voluntary frameworks such as NIST (US) rather explicitly codify the need for testing and validating cyber response plans broadly, even if falling short of dictating live exercises with top management teams. The main barrier to live testing may be cultural – to avoid what seems like a needless burden for stakeholders, especially at the executive level. Ramboll's experience is that such reluctance is often misguided; that C-suite and top management are generally very positive and enthusiastically involved if presented with a realistic rehearsal and gamified simulation setting, especially when formally debriefed on their performance and improvement requirements.

Use of live or simulated testing of cybersecurity contingency plans

Only a minority of companies have engaged in realistic exercises testing their cybersecurity contingencies against simulated cyber events or incidents.

Cybersecurity incidents



Have experienced one or more major cybersecurity incidents within the last year

5%

Live testing of cybersecurity contingencies



We have live tested our IT continuity plans within the last year

36%



We have live tested our cyber attack response plans within the last year

26%



Top management has experienced a live test of their cyber incident roles within the last year

26%



We have live tested our business continuity plans within the last year

23%

AI governance is rare, and when actually in place, strongest where least complex and costly

IT in Practice reveals not only significant maturity gaps in AI management and governance frameworks, but also that even companies with mature setups are more effective at setting direction and collecting ideas than at executing and realising value.

The practices companies have in place to govern AI are strongest in terms of intention and direction but weaker when it comes to actual delivery and value realisation. One in three companies claim to have a business AI strategy in place, but far fewer have implemented mechanisms to prioritise use cases and investments, execute on use cases, and track value. The areas where governance is least mature are also those reported to present the greatest barriers to value creation.

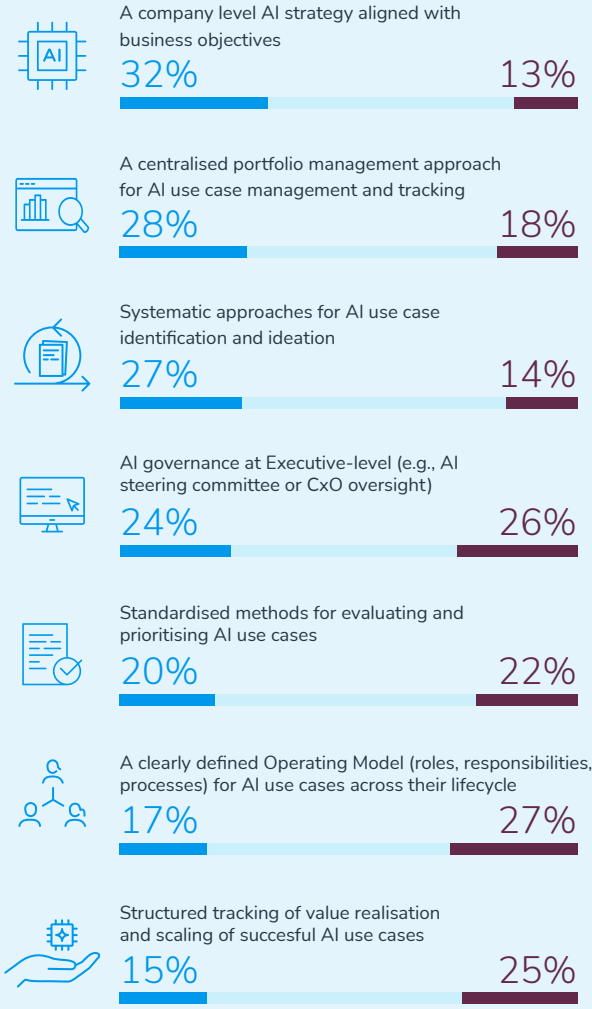
IT in Practice data shows that while a large group of companies are maturing their AI governance mechanisms, a group almost as large are at maturity level zero. One quarter of CxOs indicates solid executive AI oversight, while another quarter reports having no oversight mechanisms in place whatsoever. The same quarter entirely lacks mechanisms to govern, initiate, and manage any value realisation from AI.

AI is unusual in reaching all levels of the business at once. Any single use case appears simultaneously as an infrastructure choice, a workflow redesign, a sourcing decision, a compliance obligation, and a workforce question. These agendas are interconnected, even if each has a different natural owner. Decisions taken solely by IT, procurement, business units, or legal will counteract each other unless a single point of accountability is established.

Findings indicate that a prudent approach would be to emphasise governance of AI use case lifecycles and value tracking first, sooner than spending excessive effort on strategic level direction-setting. This includes clearly establishing executive ownership of inter-connected AI agendas. Where should the approach be centralised, and where decentralised? What are the roles of the various corporate IT and central staff functions? At present, the pace of value creation from AI is placed at the executive management table. There may well be larger than usual business penalties for followers and late movers in the AI governance space.

Use of AI strategy, governance, and portfolio mechanisms

Few companies have AI management and governance frameworks in place – execution and value realisation count among the most challenging aspects.



Software licences beat AI as the fastest-rising cost in the digital budget

The biggest driver of increased digital spending is not strategic choices, but vendor pricing. Even though cost takeouts are universally pursued by IT functions, only one CxO in twenty has managed to reduce total licence costs.

Cost takeouts targeting licencing and subscription costs are near-universal in IT functions, yet four out of five CxOs report continued increases in licence-related spending. Although AI-related licence spending might be part of the picture, spending increases on licences outpace even those related to AI. Apparent poor performance from cost takeout activities is not a lack of execution or negotiation, but a structural issue. Traditional perpetual licences converted into subscriptions, consolidation among hyperscalers and platform vendors, and AI capability bundled into tiers priced above the tier currently held are some of the changes companies are facing.

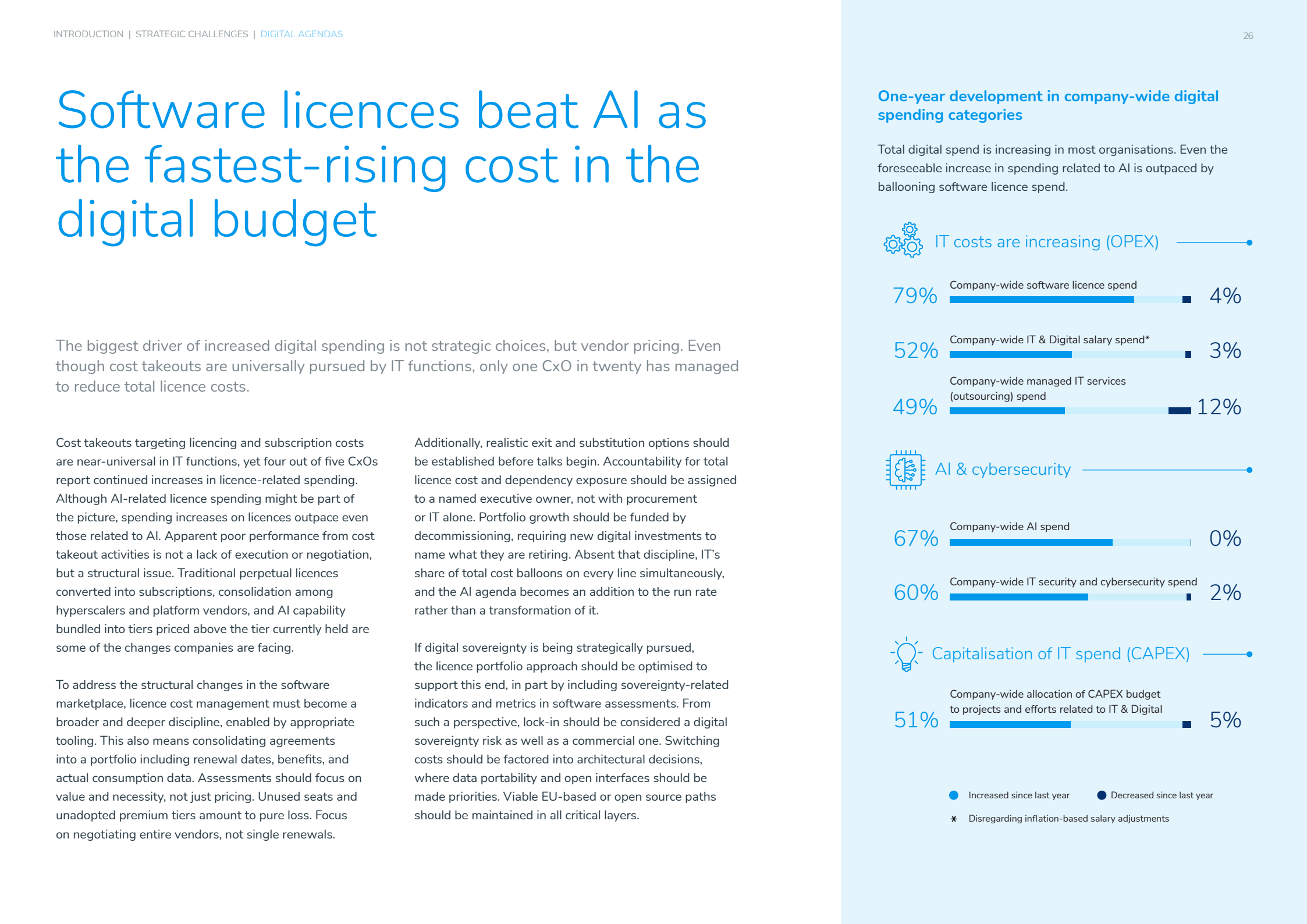
To address the structural changes in the software marketplace, licence cost management must become a broader and deeper discipline, enabled by appropriate tooling. This also means consolidating agreements into a portfolio including renewal dates, benefits, and actual consumption data. Assessments should focus on value and necessity, not just pricing. Unused seats and unadopted premium tiers amount to pure loss. Focus on negotiating entire vendors, not single renewals.

Additionally, realistic exit and substitution options should be established before talks begin. Accountability for total licence cost and dependency exposure should be assigned to a named executive owner, not with procurement or IT alone. Portfolio growth should be funded by decommissioning, requiring new digital investments to name what they are retiring. Absent that discipline, IT's share of total cost balloons on every line simultaneously, and the AI agenda becomes an addition to the run rate rather than a transformation of it.

If digital sovereignty is being strategically pursued, the licence portfolio approach should be optimised to support this end, in part by including sovereignty-related indicators and metrics in software assessments. From such a perspective, lock-in should be considered a digital sovereignty risk as well as a commercial one. Switching costs should be factored into architectural decisions, where data portability and open interfaces should be made priorities. Viable EU-based or open source paths should be maintained in all critical layers.

One-year development in company-wide digital spending categories

Total digital spend is increasing in most organisations. Even the foreseeable increase in spending related to AI is outpaced by ballooning software licence spend.



AI may already be reducing negative implications of digital talent shortage

Compared to just one year ago, dramatically fewer companies report experiencing negative impacts from digital workforce and talent shortage. AI is a partial driver of this development, but adaptation strategies, post-pandemic labour market normalisation, and less heated demand all factor in. These findings should impact commercial behaviour broadly.

The reductions in the negative implications of the digital talent shortage experienced over the course of one year are highly significant.

The number of companies reporting overall negative consequences of a shortage in digital talent has halved over the last year. While movements of this magnitude are rarely attributable to any one single cause, actual and expected AI impacts are likely starting to affect demand for talent and resources, even if not directly surveyed.

Negative effects related to sourcing have dropped dramatically, indicating that use of external capacity has moved from necessity back towards choice for a large group of companies. Scaling back digital initiatives or assigning less ideally qualified staff now factor among the leading negative consequences of the digital workforce and talent shortage, still affecting a sizeable minority.

It is uncertain exactly what impact AI-assisted deliveries have had on this encouraging one-year decrease in experienced negative effects, but it is likely to have played a significant role. This comes in addition to post-pandemic labour market normalisation and a more cyclical reduction in demand, which will eventually reverse. CxOs should act on these findings and evaluate genuine AI-enabled throughput before taking workforce-related actions. Take advantage of the shift in leverage to renegotiate prices and agreements with providers, consultants, and contractors from a stronger position, while reserving external partners for skill sets that are genuinely scarce, rather than using these for baseline capacity. Recruiting should be made more selective and narrow in response to the availability of a larger talent pool. The reduced squeeze presents an opportunity to close any qualification gaps, such as those related to critical architecture, security, and data roles. Deliberate catchups should be initiated for any deferred roadmap or portfolio ambitions.

Mitigation and implications of digital workforce shortage

IT in Practice data shows a dramatic drop in the number of companies negatively impacted by the shortage of digital talent.



Methodology & Data



Digital Transformation in Denmark 2026-2027, IT in Practice is based on a survey conducted among top executives of Denmark's largest companies, as well as a survey conducted among all Danish municipalities, regions, government agencies, and departments.

Surveys were conducted from April to August 2026. Questionnaires were sent to respondents from the private and public sectors and distributed to two different groups – CEOs and CIOs. During the preparation of the survey, an Advisory Board of select CEOs and CIOs contributed with input and constructive feedback to the process of developing and prioritising the content and topics questionnaire. To provide a full picture of current opinions, trends, and challenges, we distinguish between the private and the public sector.

Private Sector

IT in Practice is based on a survey conducted among the largest 1,000 companies in Denmark, as ranked by the Danish newspaper, Børsen. In total, 130 top executives participated in the survey. The results for the private sector are presented in the English version of the report, Digital Transformation in Denmark 2026-2027, IT in Practice.

Public Sector

The survey was also conducted in the Danish public sector. The sector is divided into four levels: government, higher educational institutions, municipalities, and regions. In total, 130 top executives participated in the survey. The results for the public sector are presented in the Danish version, Digital Transformation i Danmark 2026-2027, IT i praksis®. The Danish version also contains the results of an online survey of a representative sample of 1,032 Danish citizens, whose responses were submitted through a web panel.





About Ramboll Management Consulting & Dansk IT

Ramboll Management Consulting is one of the largest management consultancies in the Nordic region and an integrated part of the Ramboll Group, which employs 18,000 people in 35 countries.

Ramboll Management Consulting is a trusted partner for private companies and works collaboratively with the public sector to help develop core welfare services. Our consultants engage in strategic and analytical groundwork, provide data-driven insight, and assist with determining the need for sustainability and change-related processes. To ensure our clients receive the best solutions, we also draw on the expertise of relevant staff and experts across the entire Ramboll Group.

IT in Practice is compiled by Ramboll Management Consulting's Digital Transformation service practice, which assists our clients in using technology to underpin strategic, analytical, and implementation processes, thereby creating business value. We help our clients in public and private sector enterprises to develop strategies, processes, products, and services.

Dansk IT (the Danish IT Society) is an independent nonprofit organisation and a community for IT professionals. Members can focus on their careers through continued competency development and participation in Denmark's largest network for IT professionals. Dansk IT works to promote and support IT in areas where it creates value for society and the individual.

Dansk IT gathers, strengthens, and develops the skills and professionalism of IT users and professionals, while providing an independent focus on the IT interests of society and its members. You can read more about Dansk IT on www.dit.dk.

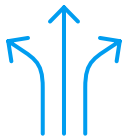
Throughout the year, Dansk IT offers conferences, courses, professional member meetings, and certifications. The association also facilitates a number of political committees, professional councils, and network groups.

At https://akademi.dit.dk members of Dansk IT have access to webinars, e-learning, podcasts, and articles that strengthen their knowledge and competences in the digital field.

Ramboll Management Consulting supports your digital journey

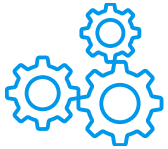
Ramboll Management Consulting is an independent advisor for digital transformation. We deliver technology agnostic consultancy helping clients to succeed through strategy, analysis, and execution.

Digital & AI Strategy



We help our clients develop strategies for digitalisation and AI to build the organisation and digital architecture needed to realise the potentials provided by the digital world.

Digital Operating Model



We help our clients develop digital Operating Models and IT organisations, ensuring digital capabilities and balancing interfaces between internal and external partners and processes.

Digital Services Procurement



We help our clients acquire digital services based on preliminary analyses by means of negotiation and tender procedures, thus establishing efficient vendor collaboration.

Digitalisation Projects & Programmes



We help our clients implement and realise the business benefits of changes to processes, digital services, and products.

Contact & Information

Digital Transformation in Denmark 2026-2027, IT in Practice

Editorial Team

Steen Christensen, Lorenzo Courir, Asger Højen Danielsen, Jacob Fink, Thomas Fjeldberg, Maja Levin, Nikolaj Vad Schou, Cathrine Lind, Thomas Trier Larsen, Nils Roien, and Morten Damgaard

Published by

Ramboll Management Consulting A/S
Hannemanns Allé 53
2300 Copenhagen S
Denmark

Phone +45 5161 1000
www.ramboll.com/management-consulting
31st year, Version 1.0
ISSN: 2596-3821

Rendering of the analysis is permitted so long as Ramboll Management Consulting is credited as source.



Steen Christensen
Director
STEC@ramboll.com

Responsible for
Digital Transformation in
Denmark, IT in Practice



Lorenzo Courir
Consultant
LZCR@ramboll.com

Project Manager and contact
person for Digital Transformation
in Denmark, IT in Practice

Follow Ramboll to learn more about how we create sustainable change
www.ramboll.com/management-consulting

Bright
ideas.
Sustainable
change.

RAMBØLL