The AI boardroom gap

Global insights to close the gap and unlock a clear path to enterprise AI success in 2026

Software Improvement Group

Table of contents

Executive summary

There's a widening gap between bold AI ambition and reality. Most organizations aren't failing at AI because of the technology, but because their foundations can't support it.

1. The gap is real

- Today, 88% of organizations report using AI technology in at least one business function, and 64% say that AI is enabling their innovation.
- However, at the enterprise level, the majority are still in the experimenting or piloting stages, and just 39% report EBIT impact– often single-digit percentages.

2. Boards need a shared view

- As companies push to innovate and embrace the opportunities of AI, it's more critical than ever for IT and business to speak the same language.
- With AI evolving at breakneck speed, the gap between AI ambition and operational readiness only widens further without governance.

3. AI legislation is divergent and complex

- Regulatory pressure is rising while rules are fragmented. As a result, boards need strategies that are proactive, flexible, and geopolitically aware.
- Because the rulebooks differ, international standards are emerging as a shared language.

4. AI coding needs human oversight

- At enterprise scale, AI coding adoption is uneven, impact varies by team, and actual usage doesn't always match leadership's storyline.
- Reported outcomes on productivity boost related to AI-assisted code development vary significantly: between a 19% slowdown and a 26% speed-up.
- New experiments show that:
  - AI can generate large and structurally maintainable software systems. However, only a small fraction of generated systems compile or run without modification, limiting practical significance and end-to-end usability.
  - AI struggles more with writing secure code than humans. On average, AI showed double the amount of security risk violations compared to the human projects.

5. AI systems are present but not widely adopted in enterprise

- AI is present in enterprise portfolios but not yet dominant: From all the systems (in production) SIG has analyzed in 2025, roughly 1.5% qualify as an AI system.
- 72% of AI systems score below our recommended build-quality threshold.

6. AI systems introduce new security risks

- Boards should recognize that AI introduces different exposures and prepare accordingly.
- Organizations are advised to build upon existing security management processes instead of treating AI security risks in isolation.

Foreword:
The AI boardroom gap

Three years. That's all it took for artificial intelligence (AI) to move from curiosity to cadence; from "have you tried this?" to "what's our plan?". Looking back, the introduction to AI is reminiscent of the rise of the internet in the 90s or smartphones in the 2010s. We didn't fully understand it–but we knew it would change everything.

Fast forward to today, AI adoption is arguably the fastest technological shift in history. However, now that the initial thrill of generative AI's possibilities is beginning to fade, organizations start asking a tougher question: where's the value?

A recent MIT report revealed that despite $30–40 billion in enterprise investments in generative AI, 95% initiatives show zero return, and according to McKinsey, only 1% of company executives described their gen-AI rollouts as "mature."

Meanwhile, the massive wave of AI (and challenges that come with it) stretches far beyond Generative AI. Machine learning and deep learning capabilities enabling predictive maintenance, fraud detection, or customer behavior prediction now sit in the same conversation about value.

Today, 88% of organizations report using AI technology in at least one business function, and 64% say that AI is enabling their innovation. However, at the enterprise level, the majority are still in the experimenting or piloting stages, and just 39% report EBIT impact– often single-digit percentages.

The ambition is there; the foundations lag.

At the same time, regulatory pressure is rising while rules fragment. As a result, boards need strategies that are proactive, flexible, and geopolitically aware.

Seemingly in a blink, AI moved from a technical topic to board responsibility. It is changing what software is, how software is built, and increasingly, who thrives.

This report aims to bridge the gap between AI ambition and reality and turns technical complexity into business clarity – so you can make better decisions, fund the right investments, and ignite your AI journey with strategic control.

Chapter 1: The need for AI Governance

As companies push to innovate and embrace the opportunities of AI, it's more critical than ever for IT and business to speak the same language.

Even before AI, many organizations lacked clear insight into their technology, couldn't understand their true IT investment needs, and struggled to control rising risks.

In fact, according to Gartner, 67% of organizations say they talk with stakeholders about mapping IT spend to outcomes, yet just 22 % have a formal process to translate those costs into business KPIs the board can understand.

While system outages, high costs, and challenging modernization attempts were already prevalent, escalating cyber threats, evolving compliance needs, and AI has significantly raised the stakes.

Now more than ever, organizations need to have a shared understanding of their technology. At Software Improvement Group, we call this 'Shifting Up': creating a shared understanding of your software estate so you can reduce risk, control cost, and unlock value.

In the age of AI, everything moves faster, making the shift-up approach even more important. In 2026, active oversight is essential. EY's global survey found only 12% of C-suite respondents could correctly identify the right controls for five common AI risks.

The board's job is to make sure the organization can benefit from AI and do so responsibly. Most of what goes wrong with AI in enterprise today has nothing to do with the technology. The instinct many organizations tend to follow is to go faster; the reality is they need designed speed–guardrails to ensure rapid progress without causing problems.

In addition, with AI evolving at breakneck speed, the gap between AI ambition and operational readiness only widens further without governance.

Which is why the first test of readiness isn't more pilots, it's clarity.

So, the quickest way to see where your organization stand is not to ask, ''Are we investing in or piloting AI?'' It's to ask a simpler, repeatable question:

''Can we show–on one page–what we have, where it runs, who owns it, how it's controlled, and that it's safe and compliant?''

If you can't answer that today, it's time to change—fast. AI's capability curve is steepening while organizational change sluggishly moves at human speed. If you're not on top of today's implementation, you won't be ready for tomorrow's.

Luc Brandts
CEO of Software
Improvement Group

"Everyone agrees technology runs the business, yet too many organizations still don't have a clear, end-to-end view needed to steer it. That's certainly not a new problem, but AI is turning up the speed, the stakes, and the consequences.

Even more reason that we need to 'shift up' and have a shared language for IT. This means keeping the technical truth but losing the jargon. Boards tend to tune out when they hear terms like 'source code' and 'refactoring,' but they lean in when the same ideas are framed as security, innovation, costs, resilience, and time-to-market impact.

What the enterprise needs in 2026 is a clear and unified view and understanding of the IT landscape–covering both AI-assisted development and AI systems in operation–with measurable KPIs that leaders can see, question, and act on. With the clarity that comes with IT Portfolio Governance, organizations don't just keep up with AI's pace; they can steer it with strategic control."

Chapter 2: Compliance snapshot

According to EY, the most common AI risk is non-compliance with AI regulations (57%). And understandably so, as the ground seems to be pulling in different directions.

Europe is building risk-based regulations aimed at safe, fair use of AI, while the United States is leaning into a hands-off posture focused on maximum innovation. Meanwhile, the UK and APAC regions follow their own principle-led or hybrid paths.

For organizations, the result is a disjointed map where rules both overlap and collide.

This is where global operations get tangled. For example, an organization that markets, deploys, or has AI outputs used in the EU will meet EU AI Act obligations, even if it's headquartered elsewhere. The same AI system might face federal questions in the US.

Because the rulebooks differ, international standards are emerging as a shared language. ISO, NIST, and similar frameworks help organizations demonstrate evidence of control – how systems are built, how they behave, and how issues are corrected.

Such as, but not limited to, the ISO/IEC 5338, co-developed by Software Improvement Group, the new global standard for AI lifecycle management.

We've created a quick (and non-exhaustive) overview of current legislation and standards to pay attention to, and we've included links to the original sources where we think you should keep an eye on, depending on where your organization operates.

A global snapshot of current AI legislation and developments

United States

The United States has introduced several key legislative measures to regulate AI. However, the complexity of federalism has made it challenging to implement a unified AI policy. In addition, since January 2025, US federal policy has emphasized an innovation-first posture, implemented through agency guidance and enforcement, plus new state laws.

- Executive Order: Removing Barriers to American Leadership in Artificial Intelligence
- Winning the AI Race: America's AI Action Plan
- National Conference of State Legislatures

United Kingdom

Similar to the US, the UK currently doesn't yet have a single, comprehensive AI-specific law. It continues to take a lighter, more flexible approach to regulations based on the five principles of safety, transparency, fairness, accountability, and contestability, set out in 2023.

- Policy Paper: A pro-innovation approach to AI regulation
- Independent report: AI Opportunities Action Plan
- Regulatory Innovation Office

European Union

The EU AI Act aims to make AI safer and more secure for public and commercial use, mitigate its risks, ensure it remains under human control, reduce any negative impacts of AI on the environment and society, keep data safe and private, and ensure transparency in almost all forms of AI use.

- EU AI Act

APAC

The Asia-Pacific AI regulatory environment spans 16+ jurisdictions with dramatically different approaches, from Japan's voluntary compliance frameworks to South Korea's Basic AI Act, designed to establish a national governance framework for AI, systematically foster the AI industry, and prevent potential risks associated with AI, to China's labelling requirements for AI-generated content.

Relevant global standards

To help navigate the complexity, global standards are becoming a shared language. While adopting these standards doesn't automatically equal legal compliance, they do give you a credible, cross-border, evidence-based grammar that regulators understand–and, in the EU, harmonized standards will carry legal weight once published for the AI Act.

- ISO/IEC 27001
- ISO/IEC 31700
- ISO/IEC 5338
- ISO/IEC 42001
- ISO/IEC 27091
- NIST AI Risk Management Framework

Joris Willems
Head of the Technology Group at NautaDutilh and the Chair of the Dutch Association of AI and Robotics Law (NVAIR)

"The rules will keep looking different, but our responsibility shouldn't. I don't think of regulation as a brake—I think of it as guardrails. If organizations build on a few non-negotiables—ethics, safety, security—and we can show our work with clear data lineage, honest disclosures, and real accountability, they can move quickly in the US, the EU, the UK—wherever—without tripping over ourselves. Any organization using AI should have proper AI governance. At board level and leadership level, there needs to be real involvement with the use of AI throughout the organization. There should be a governance committee from different tribes, so not just legal, not just compliance, but also business (also technical depending on wherever you are). A diverse group of people and that group should look at the deployment of AI in the organization (both internally and externally)."

Chapter 3: AI-assisted software development

Three years ago, a professional developer using AI felt novel; today, it's normal. 90% of technology professionals now use AI at work, and assistants draft code, suggest fixes, and speed up routine tasks. The upside is real: 52% of developers agree that AI tools and/or AI agents have had a positive effect on their productivity. But at enterprise scale, we often see that the reality at our clients is more modest: adoption is uneven, impact varies by team, and at times the level of use doesn't match the narrative from the top.

The ambition

AI coding assistants promise throughput: automate the repetitive, generate scaffolding, and provide context-aware suggestions. Time savings show up quickly—studies report hours saved per developer per week, and one experiment has found that developer output can be increased by 26%.

The reality

Research indicates 22% of merged code is AI-authored, signaling that use is present but not yet scaled. Many organizations have rolled out tools, but haven't productized use cases, redesigned workflows around them, or put the guardrails in place to run them safely at scale. Governance lags: only 29% report having formal oversight or processes to assess AI-generated code.

Why this matters: AI-authored changes raise questions the board cares about–quality, security, coherence across systems, and legal provenance.

Common risks related to AI code

Accuracy and rework

Generative models learn from market-average code and pattern matching. They usually produce convincing results. However, many professional developers say they distrust AI answers more than they trust them, and the most experienced developers are the most cautious. In practice, a lot of AI output is *almost right*, and "almost right" still costs time to verify and correct. Another experiment has shown that debugging faulty AI code can make the entire process 19% slower.

AI coding assistants can write high-quality code, but it doesn't run without modifications

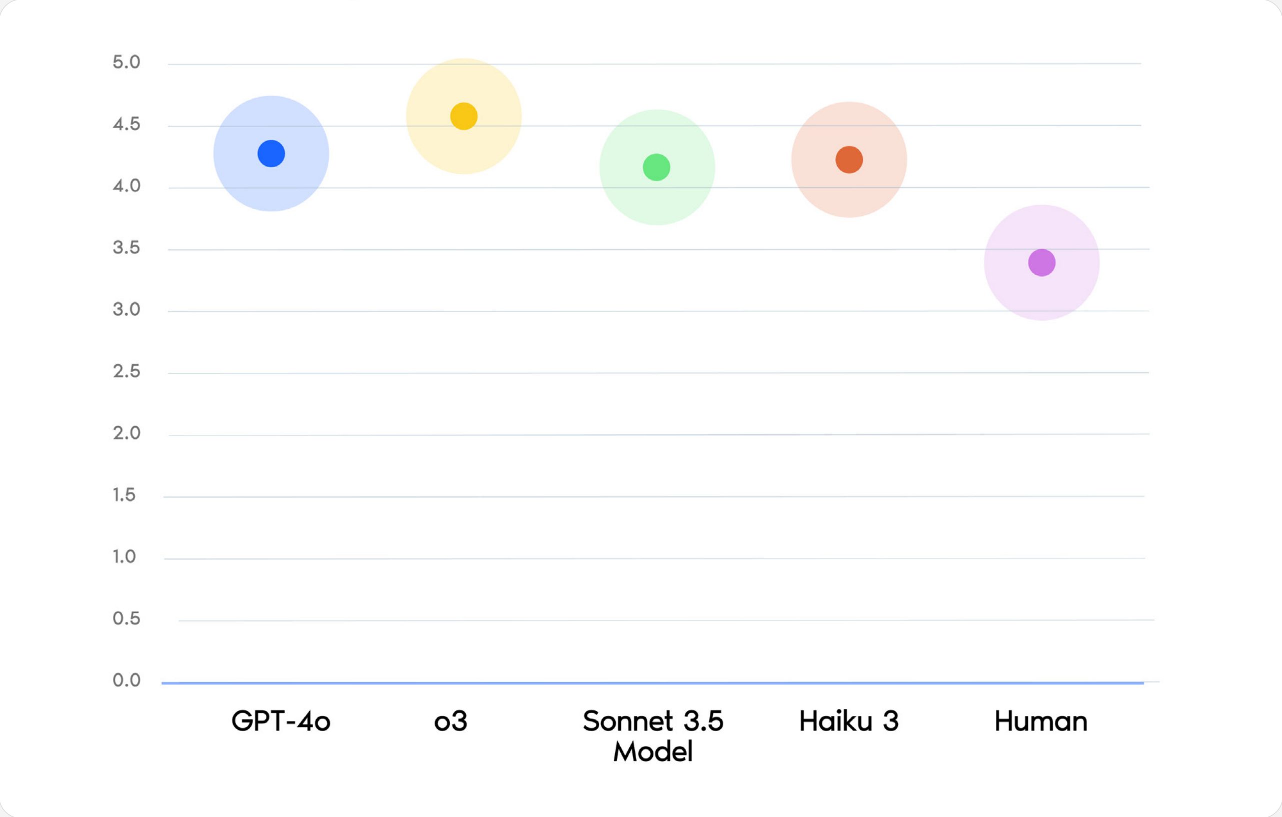
Recently, we've conducted an experiment in which complete applications were generated using AI, and various aspects of code quality were assessed and compared with human-made implementations.

We used four popular and advanced Large Language Models to generate large amounts of code needed. Next, we evaluated this AI-generated code based on functionality, security, and overall quality.

The findings showed that when given the right architectural context, these models can produce high-quality code, sometimes even surpassing human efforts.

However, despite the high scores of the AI-generated code, only a small fraction of these systems work correctly without modification, limiting their practical use and overall reliability.

Maintainability score of AI-generated code compared to human-written code

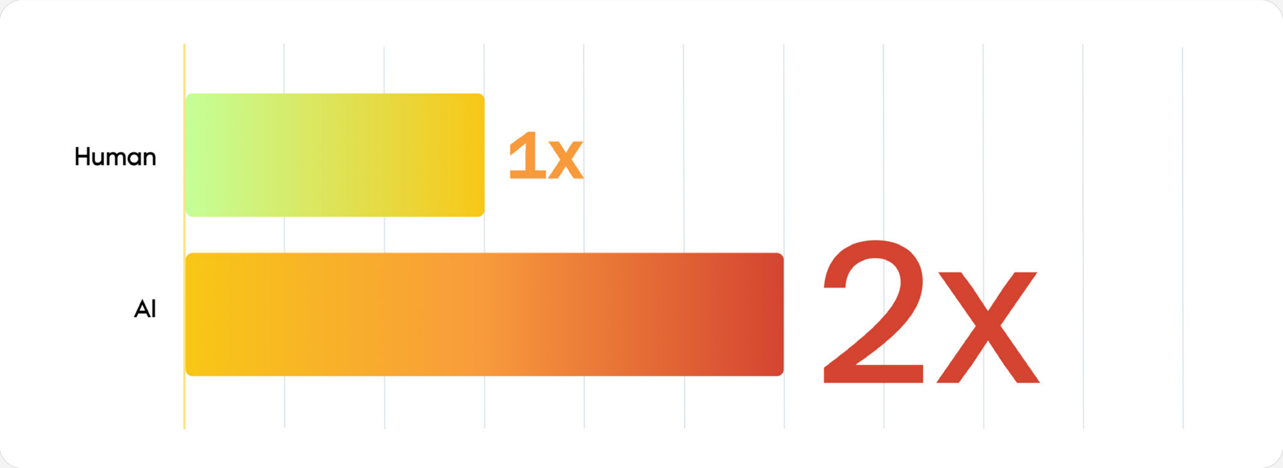


* This experiment was based on 16 projects that were generated from enterprise architecture descriptions expressed in ArchiMate. The results were used for comparative analysis between human output and four popular LLMs: GPT-4o, 03, Sonnet 3.5, and Haiku 3. The 16 projects used in this experiment are limited and may not represent diverse architectural patterns. At Software Improvement Group, we compare analysis results for systems against a benchmark of 30,000+ industry systems. This benchmark set is selected and calibrated (rebalanced) yearly to keep up with the current state of software development. Our code quality measurement score is TÜViT certified and expressed in a star rating on a scale from 1 to 5 stars. It follows a 5%-30%-30%-30%-5% distribution.

Security vulnerabilities are common in AI output

AI can repeat weak patterns from public code or invent dependencies. Without explicit safeguards, key protections are missed. A Springer Nature publication has shown that more than 50% of AI-generated code contains security vulnerabilities.

Our experiment results echo this, as they show that AI struggles more with writing secure code than humans. On average, AI showed double the amount of security risk violations compared to the human projects.



This experiment was based on 16 projects that were generated from enterprise architecture descriptions expressed in ArchiMate. The results were used for comparative analysis between human output and four popular LLMs. The 16 projects used in this experiment are limited and may not represent diverse architectural patterns. At Software Improvement Group, we evaluate security findings through a thorough analysis of the source code. These findings are then mapped to the OWASP Top 10, which identifies the ten most critical risks in web application security.

In addition, because AI lacks awareness of your architecture and policies, it can accidentally bypass security protocols or introduce unsafe dependencies.

System scale and architectural context

AI coding assistants don't "see" your whole landscape and don't comprehend your architecture. As systems span more components and business rules, AI suggestions lose context.

Recently, Stanford University conducted a large-scale analysis that shows a clear pattern: AI productivity gains shrink as codebases grow. At ~10,000 lines of code, development teams saw ~60% lift in productivity; by ~100,000 lines, those gains collapsed.

The reason isn't that AI coding assistants 'stop working'; it's that scale amplifies the parts AI doesn't see: your architecture.

The larger the code base that's generated, the more issues. Therefore, more time is required by human developers to fix these issues. In addition, trying to let the AI coding assistant fix some issues may lead to cross-contamination.

Legal provenance

AI coding assistants can generate code that's subject to restrictive open-source licenses, potentially exposing your organization to legal disputes or even forced open-sourcing of proprietary software. Where a company must release its proprietary source code under an open-source license, often as a result of failing to comply with the terms of an open-source license it used in its own product.

Visibility

It's surprisingly hard to tell which code was AI-generated. Even experienced developers find it hard to distinguish AI generated code from human-written code and "achieve only about 47% accuracy" —slightly worse than flipping a coin.

You can't control what you can't see. How do you evaluate the effectiveness of AI assisted coding?

All the above risk doesn't make AI coding a bad idea; it emphasizes why trust–earned through evidence–matters more than raw speed.

You can't control what you can't see. So, how do you evaluate the effectiveness of AI-assisted coding?

A realistic picture of the near term

McKinsey reports that nearly two-thirds of respondents said their organizations have not yet begun scaling AI across the enterprise. A report from GetDX states that structured enablement drives measurable ROI. Organizations that pair rollout with training, governance, and measurement outperform those treating AI as a plug-and-play tool.

The real question isn't whether your teams use these tools–they do.

It's whether the organization understands what's being produced, where it came from, and how it behaves once it's live.

Werner Heijstek
Senior Director at Software Improvement Group

"AI is a programming buddy from another planet: brilliant at drafting boilerplate, tests, and docs, but it doesn't know your business or your architecture. 'Vibe coding'—prompt, ship, hope—is fine for prototypes; it isn't enterprise engineering, where change has to be safe. Go all-in without controls, and you'll move faster—straight into familiar traps: quality slips, security gaps, architecture drift. The answer isn't a bigger model reviewing everything. Put AI inside the process, not instead of it: deterministic checks, provenance on dependencies, and human review that enforces your standards across the whole portfolio. Then measure consistently. Right-size expectations, too: You can't 100× what's mostly understanding, specifying, collaborating—and later, changing. Aim for speed with control."

Chapter 4: AI system engineering

While AI-assisted coding changes how we build software, AI systems change what software is.

AI systems vs. traditional software

Unlike conventional software, which follows fixed, pre-programmed rules, AI learns, evolves, and makes autonomous decisions.

According to ISO/IEC 5338, co-developed by Software Improvement Group (SIG), AI is classified as a software system with unique characteristics. These include the ability to think autonomously, learn from data, make decisions based on that data, and even potentially talk, see, listen, and move.

In addition, AI needs regular retraining to stay accurate.

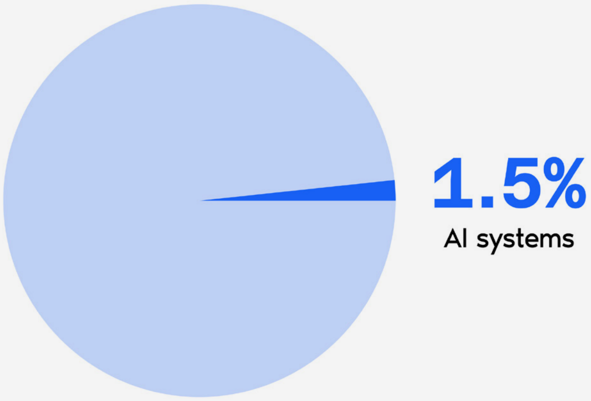
What sets AI software apart from traditional software is that it doesn't just follow fixed rules. Instead, it learns by analyzing large sets of data, finding patterns, and using that knowledge to make educated guesses when making decisions, solving problems, or answering questions.

Because of its unique features, AI is often misunderstood and can carry risks, including security issues, mistrust, and potential harm. To manage these risks, AI systems need strong engineering practices and proper regulation within the organization.

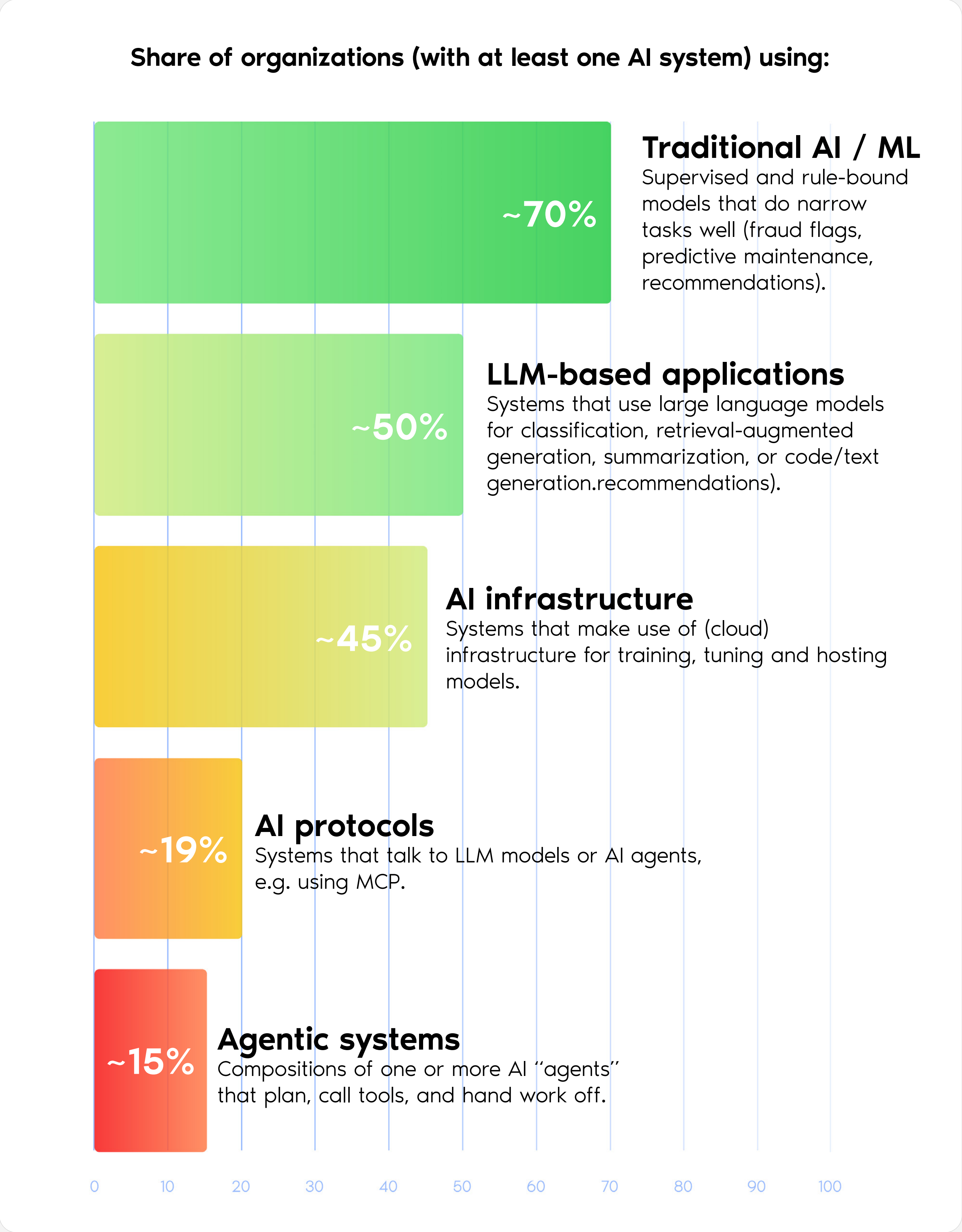
AI system adoption and popular technology categories

In our database, we see that AI is present but not yet dominant: From all the systems (in production) we analyzed last year, **roughly 1.5% qualify as an AI system.**

This aligns with realistic adoption trends discussed earlier in this report. Many organizations are piloting; fewer have crossed into scaled, business-critical AI in production.

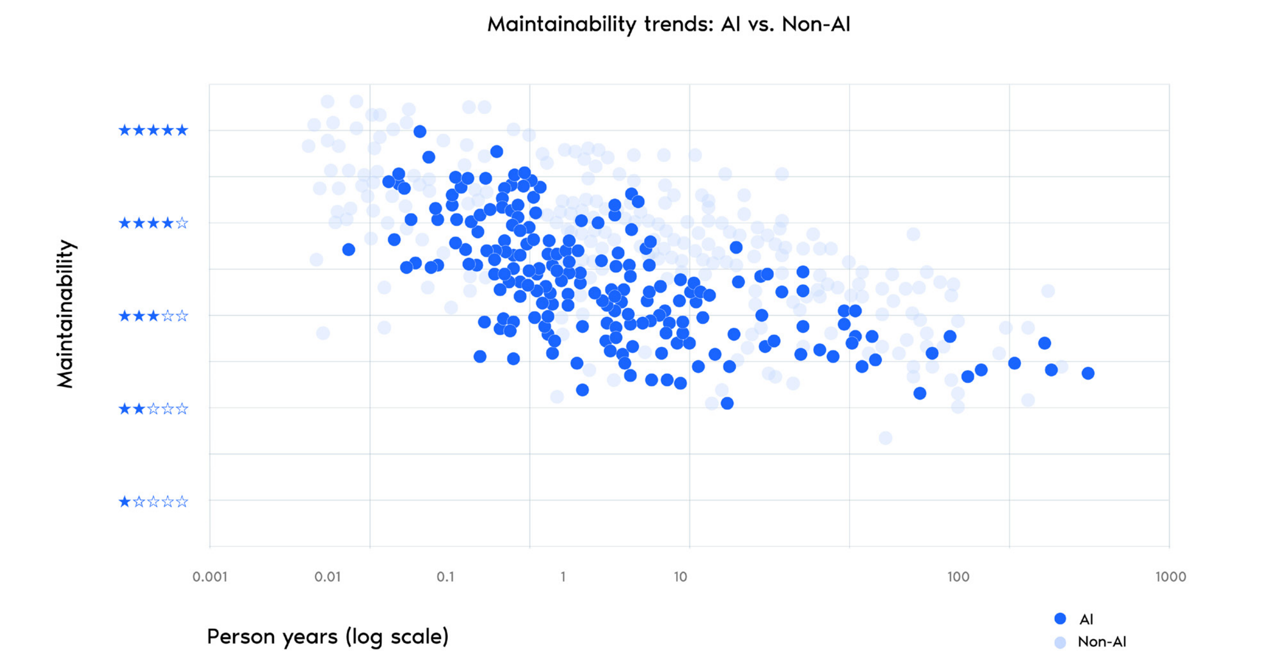


These figures show, per AI category, the share of the organizations we analyzed that operate at least one system in that category. Because organizations can operate multiple system types, categories may overlap.



The AI system quality issue

Our benchmark data shows a clear pattern: 72% of AI systems score below our recommended build-quality threshold.



Based on a subset of 300+ AI systems compared to traditional software systems written in similar languages and of similar volume.

The good news is that it is certainly possible to develop high-quality AI systems. However, engineering robust, future-proof AI systems is still a relatively new field.

We see many organizations struggling to transition AI from experimental projects in the lab to scalable, secure, compliant, and maintainable real-world applications.

The engineering challenges stem from how AI engineers—such as data scientists—are traditionally managed and trained. Their focus is often on quickly creating insights and models, not on building systems that are secure, reliable, maintainable, reusable, easy to transfer, and testable.

AI systems are software systems and should be treated as such. That said, AI systems are unlike any software we've worked with before. They learn, adapt, and operate with a level of autonomy that traditional systems don't. That creates opportunity, but also complexity, and with it, real risks.

Yiannis Kanellopoulos
CEO and founder of
code4thought

"AI is changing what software can do: it learns from data, adapts, and makes decisions. It is different from traditional software in many ways. Understanding how AI works, where it can go wrong, and how to govern it responsibly are now essential for almost every level in the organization. So, enterprises shouldn't treat AI as the holy grail, but as mission-critical software whose quality is of great importance: design for fairness, transparency, reliability, security, auditability compliance, and maintainability, and plan for regular retraining and continuous monitoring to keep performance strong and catch risks early."

Chapter 5: AI systems and security risks

Before AI, security felt challenging, but at least it was contained: firewalls, passwords, malware, phishing. Then AI walked in as an intern and started acting like a CEO. It can now sit in the middle of products and operations, learn from your data, and even speak on your behalf.

As soon as models can look things up, send messages, or trigger business tools, the key question becomes: **what are they allowed to do, for whom, and under what conditions?**

According to the OWASP AI exchange, AI security is a critical concern: AI technology is being connected to everything, there are many ways to attack AI systems, and most engineers don't yet know how to make AI secure. In addition, to highlight the urgency, Google's latest Cyber Security Forecast predicts a rise in targeted attacks on enterprise AI systems in 2026.

How to mitigate these risks?

We strongly recommend that organizations build upon existing security management processes instead of treating AI security risks in isolation. However, boards should recognize that AI introduces *different* exposures.

Why AI creates a new class of security exposure

AI systems are still software, but they behave differently. They learn from data, rely on large external components, accept open-ended inputs, and can be influenced in ways traditional applications cannot.

The "system" you must keep safe now includes **what teaches** the model (datasets, augmentation stores), **what talks to it** (prompts, documents, APIs), and **what it can do** (tool calls, workflow triggers).

Three AI security challenges the board can't ignore

1. Inputs can be weaponized

Inputs–training data, augmentation data, prompts–can directly influence model behavior. Robust testing cannot reliably detect these manipulations because the model behaves like a black box. In practice, this means:

- Data poisoning: altering training or augmentation data quietly changes how a model behaves. Even small changes can cause critical misclassifications, and because models learn statistically, these changes can be undetectable in testing.
- Input attacks at runtime: small, crafted changes to inputs can steer outputs (evasion), leak information (inversion, membership inference), or inject instructions (prompt injection). Modern AI systems cannot reliably distinguish "data" from "instructions", which means adversaries can place hidden commands into otherwise legitimate inputs.

For boards, this represents a fundamental shift: attackers no longer need to breach the system; they can influence it. According to this 2025 IO report, more than one in four surveyed organizations in the UK and US (26%) have fallen victim to AI data poisoning in 2025.

2. New crown jewels: AI-specific assets

AI systems introduce categories of sensitive assets that are not part of traditional security inventories:

- training data and augmentation stores
- model parameters
- externally sourced data and pre-trained models
- logs, experiments, and evaluation artefacts
- prompts and outputs (which may contain personal or confidential information)

These assets have confidentiality and integrity risks, and many live in development environments where teams work with production data using third-party tools–an additional weak point.

3. A much larger supply chain

AI systems rarely operate in isolation. They import external models, rely on cloud-hosted infrastructure, and use tools or datasets obtained from outside the organization. If any of these components are poisoned or compromised upstream, the resulting model inherits the behavior without visible signs.

Even when models run in a "private instance" on a cloud AI platform, sensitive inputs may still traverse shared GPU infrastructure. This is not necessarily unacceptable, but it must be understood and managed–especially when prompts contain company-sensitive information or proprietary code.

What this means for assurance

Customers and regulators won't just ask whether the server was patched. They'll want the receipts: where the data came from, who could change it, which model and context were actually used, what the system could access or trigger, and how behavior drift was detected and brought back within bounds. In short: assurance now covers the lineage and behavior of your AI, not just its deployment.

How your security teams can adapt

Your security teams do not need to build a separate "AI-only" security framework. AI systems are still software systems. Existing secure development practices remain the foundation–access control, screening, network security, supply-chain checks, and least privilege all still apply.

But teams must extend them with AI-specific considerations:

- Threat modelling that includes AI behaviors, not just software components. Most risks can be ruled out quickly once the architecture is clear.

- Protection of training, augmentation, and model data with the same rigor as source code or customer records.

- Close partnership between security and AI engineers, because mitigations like noise injection, pattern detection, or federated learning sit within the AI discipline, not traditional security.

- Zero-trust for model behavior: assume the model will occasionally be wrong, unpredictable, or manipulated–and build guardrails that limit the impact of incorrect actions.

AI doesn't just run; it learns, absorbs, and sometimes improvises. That dynamism is exactly where attackers will probe–and where regulators and customers will ask for proof. The board's security question shifts from "Is the system patched?" to "Can we demonstrate—at any moment—that our AI operates within defined limits, and that any issue is detected quickly and contained before it becomes a problem."

Standards to watch

Work to harmonize AI security practices is underway globally. Software Improvement Group's Chief AI Officer, Rob van der Veer, is right in the middle of these developments. For example, he is the elected co-editor of the AI Act security standard and contributor to the upcoming ISO standard on AI security (ISO/IEC 27090). Next to founding the security standard hub OpenCRE.org, Rob founded the OWASP AI Exchange at owaspai.org, effectively open-sourcing international AI security standardization.

Rob van der Veer
Chief AI Officer at Software Improvement Group

"AI is rapidly moving from experimental pilot to the central nervous system of our organizations. Used well, it will unlock new products, sharper decisions, and more resilient operations; used carelessly, it becomes a powerful new attack surface that we barely understand. My vision is that we embrace the 'blue sky' potential of AI, while being honest about its 'burning earth' risks, and design our systems so that models are never trusted without guardrails. Innovation and security are not opposing forces here – the organizations that will win are those that can prove their AI stays within its bounds, and that they can detect and correct it quickly when it doesn't."

Written by Software Improvement Group

Software Improvement Group (SIG) empowers organizations to govern the software their business runs on. Through complete portfolio analysis and tailored strategic advice, SIG helps companies embrace AI with control, improve software quality and security by focusing strategic efforts across people, process, and technology.

Sigrid®—SIG's software governance platform—analyzes over 400 billion lines of code across more than 30,000 systems and 300+ technologies, offering evidence-based insights to help organizations prioritize and manage their most critical IT initiatives.

Founded in 2000 and headquartered in Amsterdam, SIG has offices in New York, Copenhagen, Brussels, and Frankfurt. The company complies with leading ISO/IEC standards, including 27001 and 17025, and co-developed ISO/IEC 5338—the new global standard for AI lifecycle management.

Combining expert consulting with over 25 years of industry-leading research, SIG is the global authority on software portfolio governance.

Trusted by

TELUS

KLM Royal Dutch Airlines

NXP

ING

alliander

PHILIPS

DHL

SIEMENS

KONECRANES

THL

The AI boardroom gap

Software
Improvement
Group