Software Improvement Group

Telecom signals 2025

How software quality will define cost, resilience, and innovation in telecom

Table of contents

Executive summary

The 6 software signals shaping telecom in 2025

As telecom operators accelerate the shift to 5G, AI, and cloud-native services, software quality is becoming a hidden–but critical–factor in their success.

This report draws on Software Improvement Group (SIG)'s analysis of telecom systems to highlight key risks and opportunities buried in the code. From software-driven outages to AI fragility and emissions tied to bloated systems, each chapter reveals how software can accelerate or delay transformation.

1. Build quality gaps drive higher costs and slower innovation	**67.2%** of telecom systems fall below SIG's recommended build quality threshold–the lowest of any industry. Poor build quality reduces innovation capacity by up to 40% and increases outage risk.
2. Telecom lags on software security readiness	**74.1%** of telecom systems have an at or below market-average level of security controls, compared to **55%** in other industries. Software vulnerabilities make threats harder to avoid, detect and mitigate, compounding risk across critical infrastructure.
3. Modern architecture gives telecom an edge	With an average architecture rating of **4.1 stars**, telecom is well-positioned to accelerate modernization. SIG data shows 4-star architectures enable change **30% faster**–a key advantage in scaling new services.
4. Telecom leads on knowledge sharing–but gaps remain	**50%** of telecom systems meet SIG's recommended knowledge distribution threshold. Telecom's average score of **3.9 stars** far outpaces the 2.8 cross-industry norm, helping teams reduce bottlenecks and recover faster.

5. AI adoption outpaces software readiness	**73%** of AI and big data systems show structural risks. 89% of industry executives in telecom are piloting or already implementing AI–but in general these systems underperform on build quality, making them potentially fragile and costly.
6. Software quality is key to sustainable IT	Refactoring telecom's most common languages (Java, C#) can cut energy use by up to **17%.** Cleaner code structures reduce compute load and energy waste, offering a fast track to emissions targets and regulatory readiness.

Software quality is a multiplier–not a nice-to-have

It's the foundation for reliability, speed, cost-efficiency, and sustainability. Telecom companies that invest in code quality will be best positioned to reduce risk, accelerate innovation, and deliver the scalable, always-on services modern networks demand.

Foreword

Telecom networks are under pressure like never before. As the industry races to deliver 5G, cloud-native services, and AI-powered experiences, the expectations placed on telecom providers are growing – faster speeds, stronger security, lower latency, sustainability requirements and near-zero downtime.

Behind it all lies software.

From OSS/BSS platforms to AI-driven automation, software increasingly defines how modern networks operate. But as complexity rises, so do the risks. Build quality gaps, legacy drag, and hidden security flaws can slow progress, inflate costs, and undermine reliability. At the same time, smarter software design opens the door to faster releases, lower operational expenditure (OPEX), and more resilient infrastructure.

Our data shows that software quality is not a technical detail – it's a core driver of cost, innovation, and resilience.

This report highlights the six key signals shaping telecom's software future. It's designed to help leaders in the industry:

- Identify hidden risks buried in complex systems
- Strengthen security and resilience at the software level
- Prioritize software improvements that deliver measurable ROI
- Modernize confidently without escalating cost or complexity
- Harness knowledge distribution to mitigate risk
- Unlock innovation capacity by improving code quality

If your mission is to lead in a world of always-on connectivity, this report will help ensure your software is a source of strength – not friction.

Luc Brandts

CEO
Software Improvement Group

Chapter 1: Build quality is a hidden driver of cost, resilience, and innovation

Key findings:

- **67.2% of telecom systems fall below our recommended build quality rating,** making it the worst-performing industry in this category.
- Large systems, which are negatively correlated with build quality, **are over twice as common in Telecom (22%) as in other industries (10%).**
- 4-star systems offer **30% more capacity for innovation** and improvement.

Build quality is non-negotiable in telecommunications

As telecom networks expand with 5G, cloud, and AI workloads, one factor quietly determines whether this complexity becomes a competitive advantage or a liability: the quality of the software underneath.

Poor build quality isn't just a technical issue. It's showing up in the customer experience. EY's latest risk radar reveals that over one in four households regularly face broadband or mobile connectivity issues. Behind the scenes, weak software is often a key culprit.

These risks are not just theoretical. Uptime Institute's 2024 outage analysis reports that telecom, cloud, and digital service providers now account for 67% of all publicly disclosed IT outages–up from previous years. Software-related issues alone now trigger nearly one in four (23%) major incidents. In other words, build quality is critical to network uptime.

The business impact is mounting. Recent headline incidents underline how fragile the software telecom networks are built on can be. AT&T's 12-hour nationwide outage in the US in 2024–caused by a single software issue–blocked 92 million voice calls and more than 25,000 emergency-service attempts, prompting an FCC enforcement probe. According to Cisco, 77% of large organizations suffered at least one major outage in the past two years; often due to software errors, misconfigurations, or cascading complexity. The cost? an estimated US $160 billion in annual losses.

These incidents underscore a simple truth: fragile code creates fragile networks. As systems grow more complex, even routine changes can take millions of customers offline. Build quality is a board-level imperative, not an engineering nice-to-have.

Telecom is falling behind on build quality

With board-level pressure to "do more with less," cost optimization has officially overtaken growth as the top CIO priority for 2025. According to Capgemini, 56% of organizations now rank cost reduction above revenue expansion. In telecom, where margins are under pressure and infrastructure complexity is surging, that makes every cent count.

One overlooked cost lever is software build quality. Build quality refers to how easily a system can be understood, modified, tested, and improved. The lower the build quality, the more time and resources are needed to make even minor changes, draining IT budgets. When code is clean, modular, and well-documented, maintenance effort drops and innovation headroom grows.

SIG's research makes the urgency of action on build quality in this industry abundantly clear. 67.2% of telecom systems fall below the recommended build quality threshold, the worst score of any industry we analyzed.

10 worst-performing industries

Percentage of systems per industry that fall below our recommended build quality rating

1. **Telecommunications** – 67.2%
2. **Services (Business)** – 66.9%
3. **Manufacturing** – 62.4%
4. **ICT / Software** – 59.3%
5. **Start-ups / Scale-ups** – 57.1%
6. **FSI** – 46.8%
7. **Non-Profit** – 45.4%
8. **Energy** – 45.0%
9. **Publishing** – 37.5%
10. **Public** - 31.9%

Why does that matter? Because poor build quality directly drains IT budgets. McKinsey estimates that technical debt now consumes 40% of the average IT balance sheet. Technical debt refers to quality issues in software systems that can make future changes more costly or difficult. Left unmanaged, it slows development and increases risk over time. That's development effort spent not on innovation, but on wrestling with brittle systems–refactoring messy code, navigating undocumented components, and fixing preventable defects.

The data reinforces this further. Telecom systems average just 3.2 stars for build quality, falling below the cross-industry average of 3.5*. That gap translates into higher costs, slower changes, and a heavier maintenance burden. Many organizations still devote up to 70% of their IT spend just to keep systems running.

Build quality isn't just about cleaner code. It's also a path to controlling OPEX, reducing outages, and unlocking innovation capacity that's currently trapped under legacy complexity.

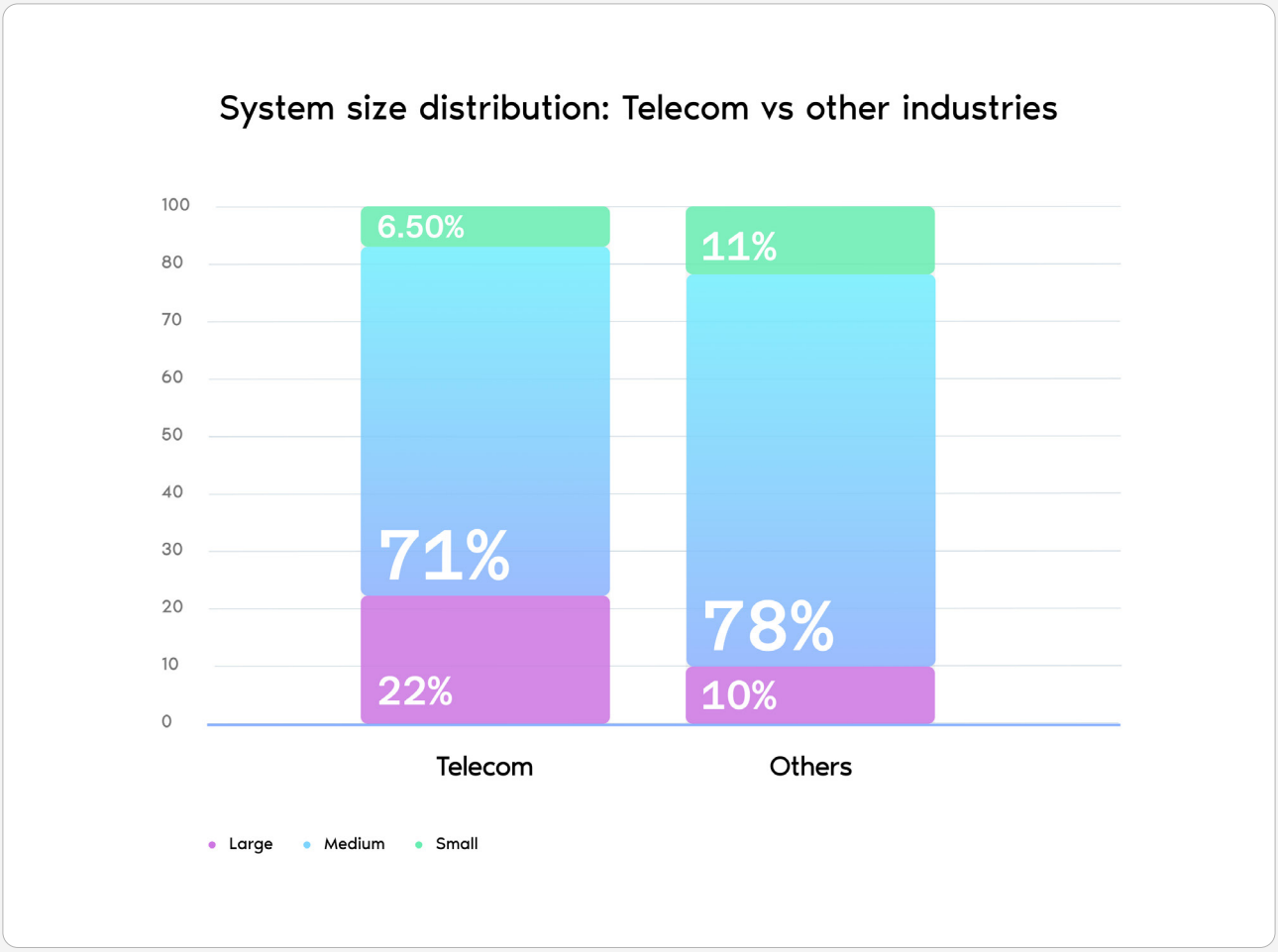
A note on SIG's star ratings:

SIG's star ratings are a way to evaluate and compare software quality.

The ratings range from 1 to 5 stars, with half-star increments (so technically 0.5 to 5.5). A 3-star rating represents the market average. The ratings are based on comparing a system's properties to SIG's benchmark, which includes thousands of systems and is recalibrated yearly.

Why size drags telecom build quality down

One possible explanation for this underperformance on build quality is the average system size within telecom companies. On average telecom companies in our database work with larger systems than in other industries, and the median system size is also larger.



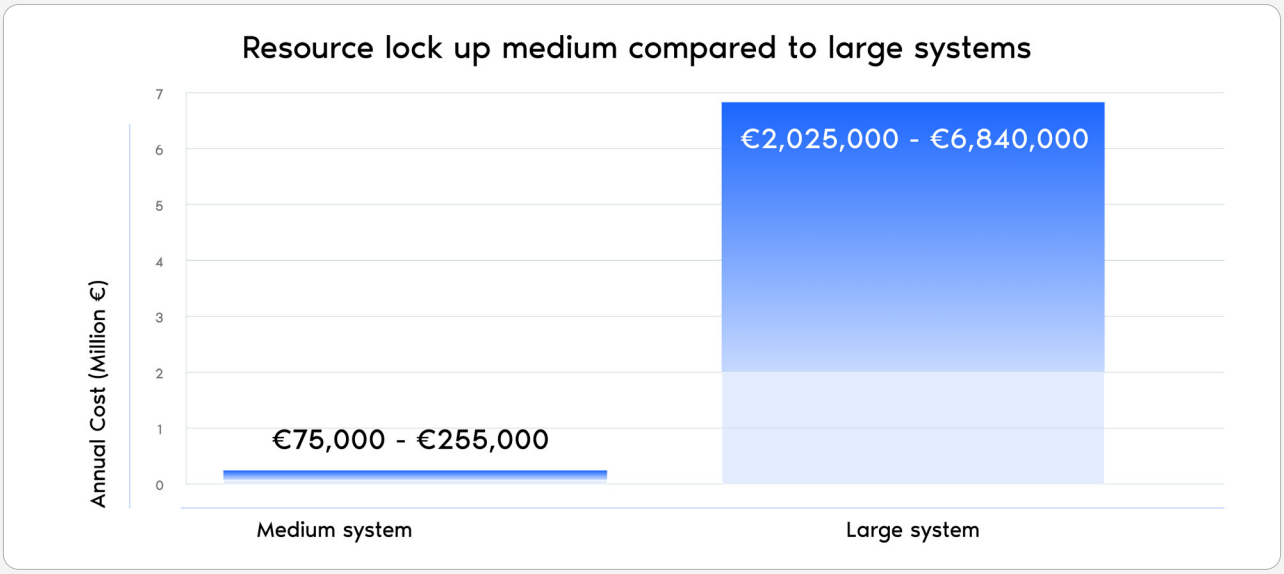
Compared to other industries, large systems are **roughly twice as common in telecom**, while genuinely small, nimble codebases are scarce. Size matters because larger systems are generally harder to maintain. As systems grow in size, a few key things happen:

- The project requires larger teams and longer development times, which introduces more complexity and overhead.
- The design becomes more complex to manage.
- Defect density (bugs per 1000 lines of code) increases substantially.
- It becomes harder to search through, analyze, and understand the codebase.
- Making changes becomes riskier, as it's more difficult to predict ripple effects across the system.

The net effect: oversized systems siphon engineering capacity into firefighting, erode star ratings, and keep telecom operators stuck in execution mode instead of innovation.

Bigger systems mean more budget burn

Not all systems carry the same weight when it comes to maintenance costs, and the impact of poor build quality scales dramatically depending on how big a system is.



Medium systems represent 80% of systems in the database, while large systems represent the top 10% of the largest systems in the database.
Amounts are calculated by multiplying number of FTEs by an average yearly developer salary of €150,000.

In a medium-sized system, improving build quality from:

- **2 to 4 stars frees up 0.5 FTE** → saving about €75,000 per year
- **1 to 4 stars frees up 1.7 FTE** → saving about €255,000 per year

Now zoom out to large systems, and the numbers skyrocket:

- **2 to 4 stars frees up 13.5 FTE** → saving about €2,025,000 per year
- **1 to 4 stars frees up 46.6 FTE** → saving about €6,840,000 per year

That's per system.

And it adds up fast. Large enterprises typically run hundreds of systems. Even a portfolio of 10 large systems rated at 2 stars could cost an organization over **€20 million a year in unnecessary maintenance overhead.**

Building better build quality

While the data paints a concerning picture, telecom operators can take decisive steps to reverse these trends. It's not impossible for large systems to have good build quality. Improving build quality is entirely possible and can give telecom companies the upper hand in both cost reduction and innovation.

Better code unlocks capacity and cuts costs

Build quality isn't just about stability. It directly impacts a company's ability to evolve and innovate.

- 4-star systems offer 30% more capacity for innovation and improvement.
- 2-star systems experience a 40% shortage, as teams are forced to firefight instead of moving forward.

The cost impact is real. Our most recent State of Software Report estimates that poor build quality can increase system-level maintenance costs by up to €250,000–a hidden tax on every new feature or integration.

Earlier research has proven that systems with a 4-star maintainability score gain 30% extra capacity for innovation and improvement compared to 3-star systems. While 2-star systems lead to a 40% capacity shortage due to regular maintenance.

Cost optimization through better build quality

Telecom operators face relentless pressure to lower operational expenditure (OPEX) while expanding 5G, cloud, and AI services. Strengthening build quality is the most immediate, controllable lever for keeping costs down without slowing innovation.

- **Hard-to-maintain systems inflate costs** → Large, low-quality codebases lock teams into firefighting and can consume millions in avoidable FTE hours.

- **Software-driven outages hit revenue and trust** → Mis-configured releases and fragile dependencies are now among the top causes of major telco outages, costing the industry billions.

- **Clean, modular code unlocks growth capacity** → Elevating a system's build quality frees up more engineering time for new features and faster time-to-market.

By upgrading build quality, telecoms can release budget, cut outage risk, and enable telecom leaders to pass those savings on to their customers.

Chapter 2: Cybersecurity is a growing risk in telecom

Key findings:

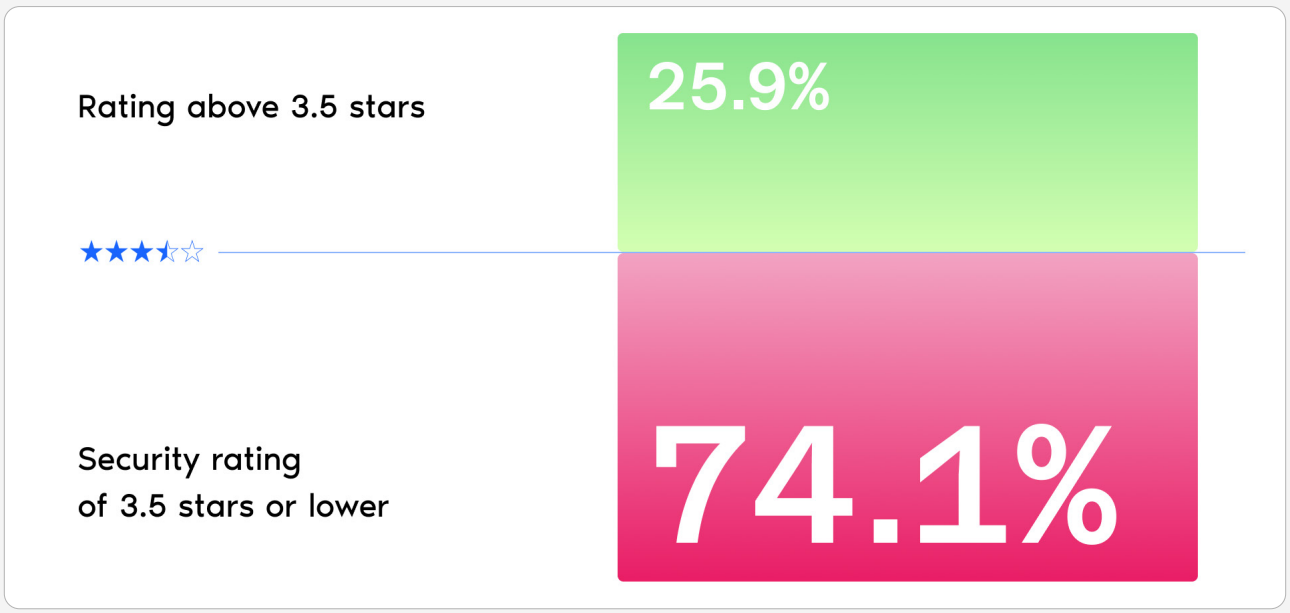
- **74%** of telecom systems have an at or below market-average level of security controls, versus **55%** across other industries.
- The average telecom security rating is **2.6 stars**–well under the cross-industry mean of **3.1 stars.**
- Systems with above-average build quality are **2x more likely** to achieve strong security compliance.

The threat landscape around telecom networks has intensified sharply. *Microsoft's Digital Defense Report* shows a **40% year-on-year increase in cyber-attacks targeting critical telecom infrastructure**, the steepest rise of any critical-infrastructure sector. The timing couldn't be worse: 5G roll-outs, hybrid-cloud adoption and always-on digital channels are multiplying entry points faster than most teams can secure them.

The potential business impact cannot be overstated. BAE systems found that 69% of telecom leaders admit a successful cyber-attack would have a **"severe or catastrophic"** effect on their organization. One study from the U.S. reports security breach-related complaints against telecom providers **surged 190% between 2021 and 2023**. In 2024, IBM reported that the average cost of a data breach stands at $4.88 million. In short, escalating attack volume and growing financial risk make first-class cyber-resilience more important than ever in telecom.

Below-average security ratings are leaving the telecom sector exposed

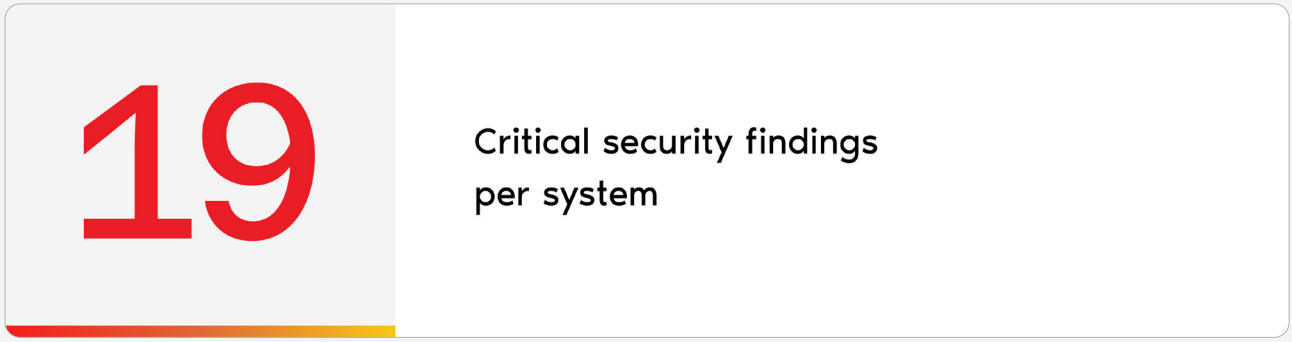
Our data reveals that 74.1% of telecom systems are classified as having an at or below market-average level of security controls, compared with 55% in other industries putting them at risk of regulatory penalties, data breaches, and reputational damage. It is important to note that an above-average rating does not guarantee full security; it simply indicates that security considerations have been factored into the design and implementation, making vulnerabilities less likely.



Based on a snapshot of active security findings in all systems in our data warehouse on a random day medio 2023.
Our SAST (Static Application Security Testing) security model that ranks software systems from 1 to 5 stars.
We evaluate system properties through a thorough analysis of the source code and infrastructure. This includes reviewing the codebase and other artifacts (such as documentation) to derive scores for various system characteristics. These characteristic scores are then mapped to the OWASP Top 10, which identifies the ten most critical risks in web application security. This report is compiled by a group of security professionals from around the globe and serves as an "awareness document." It is recommended that all organizations integrate its findings into their processes to effectively reduce and manage security risks.
The star rating reflects your compliance benchmark against the OWASP Top 10: 1. Severely low degree of security controls, 2. Very low degree of security controls, 3. Low degree of security controls, 4. Moderate degree of security controls. 5. High degree of security controls.
It is important to note that a 4- or 5-star rating does not guarantee full security; it simply indicates that security considerations have been factored into the design and implementation, making vulnerabilities less likely.

This is reflected in the average security rating in telecom, which lags at 2.6 stars compared to a 3.1 star average overall.

Across all industries–including telecom–the average system carries 19 critical findings, many of which can expose systems to operational and regulatory risk.



*This estimation is based on a snapshot of active security findings in all systems on a random day medio 2023. The number of findings were then translated into an average of security findings (1.16) per person year (size of system), which was then used to calculate an estimation of critical security findings per system.
A software system refers to a collection of interrelated programs, data, and documentation that work together to perform specific tasks or functions and have their own team. For example, a single application can consist of multiple interconnected systems. The size of the system we took as an average equals 16.3 person years which indicates how many years it would take a single person to rebuild the same system from scratch.

This number reflects an average per system, based on a typical-sized system in our benchmark. However, it's important to note that financial services institution (FSI) systems can be up to ten times larger than the average system in our benchmark. Generally, larger systems tend to have lower security ratings, which correspond to a relatively higher number of security findings, while smaller systems often achieve higher security ratings.

We evaluate system properties through a thorough analysis of the source code and infrastructure. This includes reviewing the codebase and other artifacts (such as documentation) to derive scores for various system characteristics. These characteristic scores are then mapped to the OWASP Top 10, which identifies the ten most critical risks in web application security. This report is compiled by a group of security professionals from around the globe and serves as an "awareness document." It is recommended that all organizations integrate its findings into their processes to effectively reduce and manage security risks.

Not every security flaw turns into a breach, but with attack surfaces expanding and critical infrastructure at risk, companies can't afford to treat software security as an afterthought.

Identifying and remediating vulnerabilities should be a priority for every telecom provider aiming to maintain operational resilience and regulatory compliance.

Build quality and security go hand in hand

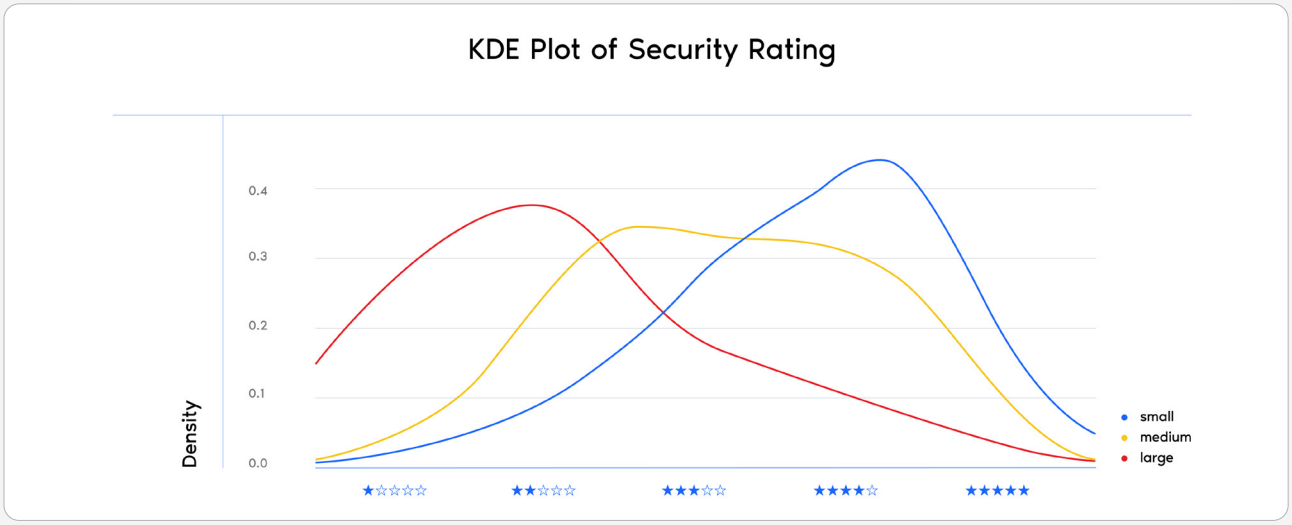
Our State of Software 2025 report confirms that **build quality and security move in lockstep**. Across the full data set, systems that score above the market-average for build quality (≥ 3.5 stars) are **roughly twice as likely to earn a strong security rating** as those that fall below.

Telecom generally sits on the wrong side of this divide. Because the majority of its systems do not clear the recommended build quality bar as shown in chapter 1, they have a greater risk of ending up with sub-par security scores.

Larger systems tend to have weaker security

The size factor amplifies the gap: telco applications skew large, as discussed in chapter 1 and sprawling code bases make it harder to trace data flows, lock down dependencies, and apply patches consistently.

When we break down security ratings across industries by system size, a clear trend emerges: the larger the system, the lower the average security rating.



Small systems typically score higher, with most clustering around the 4-star mark. Medium systems show more variation. But large systems consistently have lower ratings, with many falling below the 3-star security rating, indicating a very low degree of security controls.

The mechanism is straightforward. When software is poorly structured, it's difficult to understand, modify, and test, making it more difficult to identify weaknesses, add preventive measures in all relevant locations, and maintain those preventive measures.

Things like outdated dependencies, weak encryption, and coding errors all create exploitable gaps for attackers. Sure, firewalls, intrusion detection, and threat monitoring all have a role to play, but they don't mean much if the software is built on a shaky foundation.

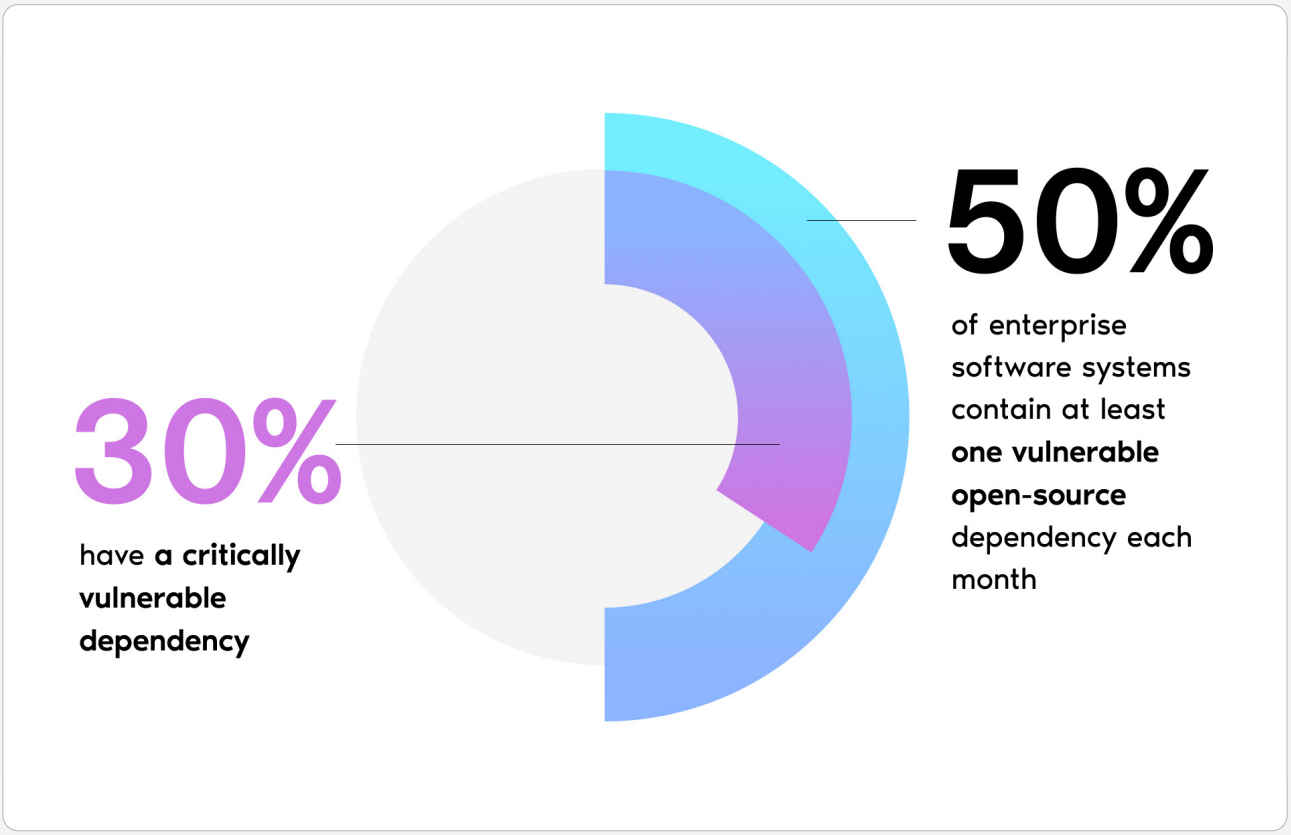
By embedding secure coding practices and software quality management in the core of the software development lifecycle, organizations can proactively reduce risk, detect vulnerabilities early, and prevent costly breaches.

As Yiannis Kanellopoulos, CEO of Code4Thought, puts it:

> **"Addressing security issues early in the development lifecycle not only reduces costs but also fortifies your system's security."**

The open-source dilemma for telecom

Weak core code is only half the story; vulnerable dependencies complete the picture. Open-source software (OSS) adoption keeps accelerating: **96% of organisations worldwide are increasing or maintaining their use of OSS**. For telcos, open-source speeds up network-function virtualization, trims licensing costs, and lets teams customize code for 5G and edge services. But it also introduces hidden risks. SIG's analysis shows **50% of enterprise systems contain at least one vulnerable open-source dependency each month, and 30% include a critically vulnerable component.**



The multi-layered approach to cybersecurity

To establish a strong cybersecurity posture, organizations need a layered approach that combines multiple security measures.

Three key methodologies in software security testing include:

- **Penetration Testing (Pentest)** → Simulates external attacks to uncover vulnerabilities.

- **Static Application Security Testing (SAST)** → Analyzes the source code to detect weaknesses before deployment.

- **Software Composition Analysis (SCA)** → Scans third-party open-source libraries and dependencies for known vulnerabilities.

No single method is sufficient on its own. SAST and SCA catch issues early in the pipeline, while pentesting validates defenses in production. Together they provide fuller coverage, earlier detection, and stronger compliance.

Telecom operators need to get ahead of open-source risk by baking this layered approach into their ways of working, patching flagged components quickly, and treating OSS governance–not just perimeter defense–as a core plank of their cybersecurity strategy.

Chapter 3: Legacy modernization unlocks speed, savings, and security

Key findings:

- **Only 2% of telecom systems still rely on legacy tech,** versus 7% in other industries.
- **4-star architecture delivers changes 30% faster** than market-average systems; 2-star architectures slow change by 40%
- **Up to 60% OPEX reduction** reported by telecoms replacing legacy platforms.

Modernization in telecom is making strides

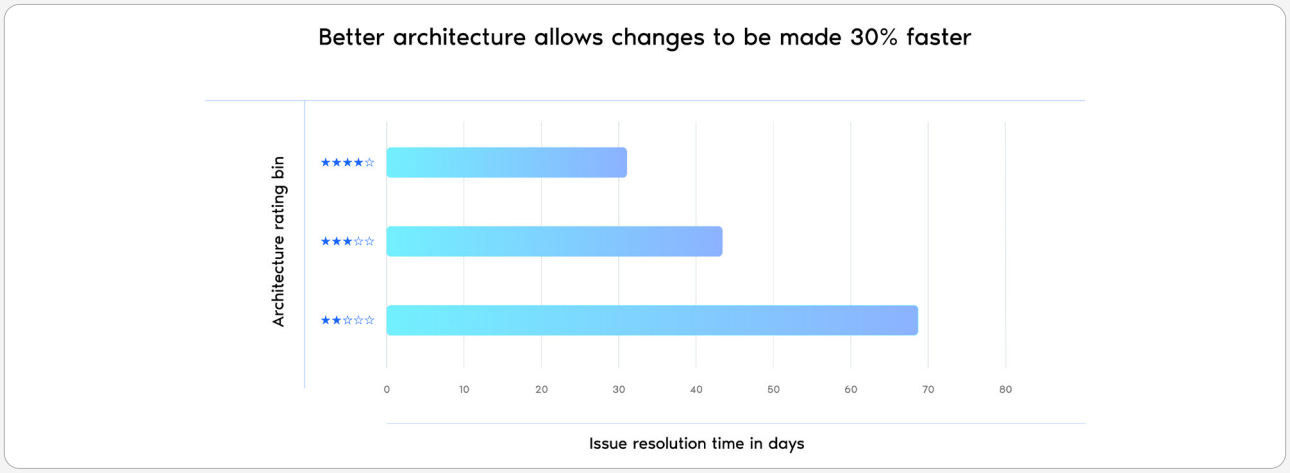
Telecom has made remarkable progress on legacy modernization. Just 2% of systems in the sector still rely on outdated technology, compared to 7% in other industries, according to SIG data. That puts telecom ahead of the curve–but the last stretch of modernization may be the most critical.

Why? Because even a small slice of legacy tech can cause outsized damage. These older systems often power revenue-critical functions like billing and provisioning. They're harder to maintain, slower to update, and more vulnerable to outage and attack.

Small footprint, big consequences

Legacy architecture drags down change velocity and reliability. Our research shows:

- 37% of legacy-based systems across industries fall below the recommended architecture-quality threshold–versus just 11% of modern systems.
- 2-star systems are 40% slower to change than average; 4-star systems are 30% faster.



Modern platforms aren't just more agile. They're more secure and cost-effective too. Research shows operators that replaced mainframe components reported up to 60% lower OPEX, fewer outages, and stronger cybersecurity postures. In fact organizations that rely heavily on legacy systems see a 300% increase in expected risk-related costs and are twice as likely to experience a major security incident, underscoring the security arguments made in Chapter 2.

Even where legacy tech is minimal, its consequences are not.

Telecom's next win: architecture quality at scale

As a consequence of this modernization, telecom architecture quality stands at 4.1 stars–matching the cross-industry average. Whilst this provides a good foundation, it doesn't guarantee consistency or resilience across the entire software landscape. With AI, 5G, and network automation accelerating demand, architecture quality must be applied deliberately and at scale to prevent it from becoming a hidden constraint.

Modernization isn't a clean-up task. It should be a strategy for business advantage. Systems that can't scale or adapt quickly enough will bottleneck innovation and increase risk exposure.

Keep modernizing or watch competitors sprint past

Telecom's small legacy footprint is promising, but it mustn't breed complacency. Even a small slice of outdated code can stall releases, inflate costs, and increase security risk. Forward-thinking IT leaders must make sure modernization is an ongoing priority. By keeping modernization on the agenda, leaders can avoid giving competitors the runway they need to win the next round of the innovation game.

Chapter 4:
Turning knowledge into competitive advantage

Key findings:

- **50% of telecom systems meet the recommended threshold** for knowledge distribution. However, the other half still falls short, meaning siloed knowledge remains a significant barrier.
- Telecom systems score an average of **3.9 stars on knowledge distribution**–well above the 2.8-star cross-industry average but attracting and retaining talent is emerging as a key constraint putting this score at risk.

As telecom operators pursue digital transformation at speed, talent is emerging as a key constraint–and a critical differentiator. McKinsey finds that over 80% of telecom C-suite leaders now see talent as the top enabler of ''tech-co'' transformation. Yet across the sector, some teams are struggling to keep up with the pace of change.

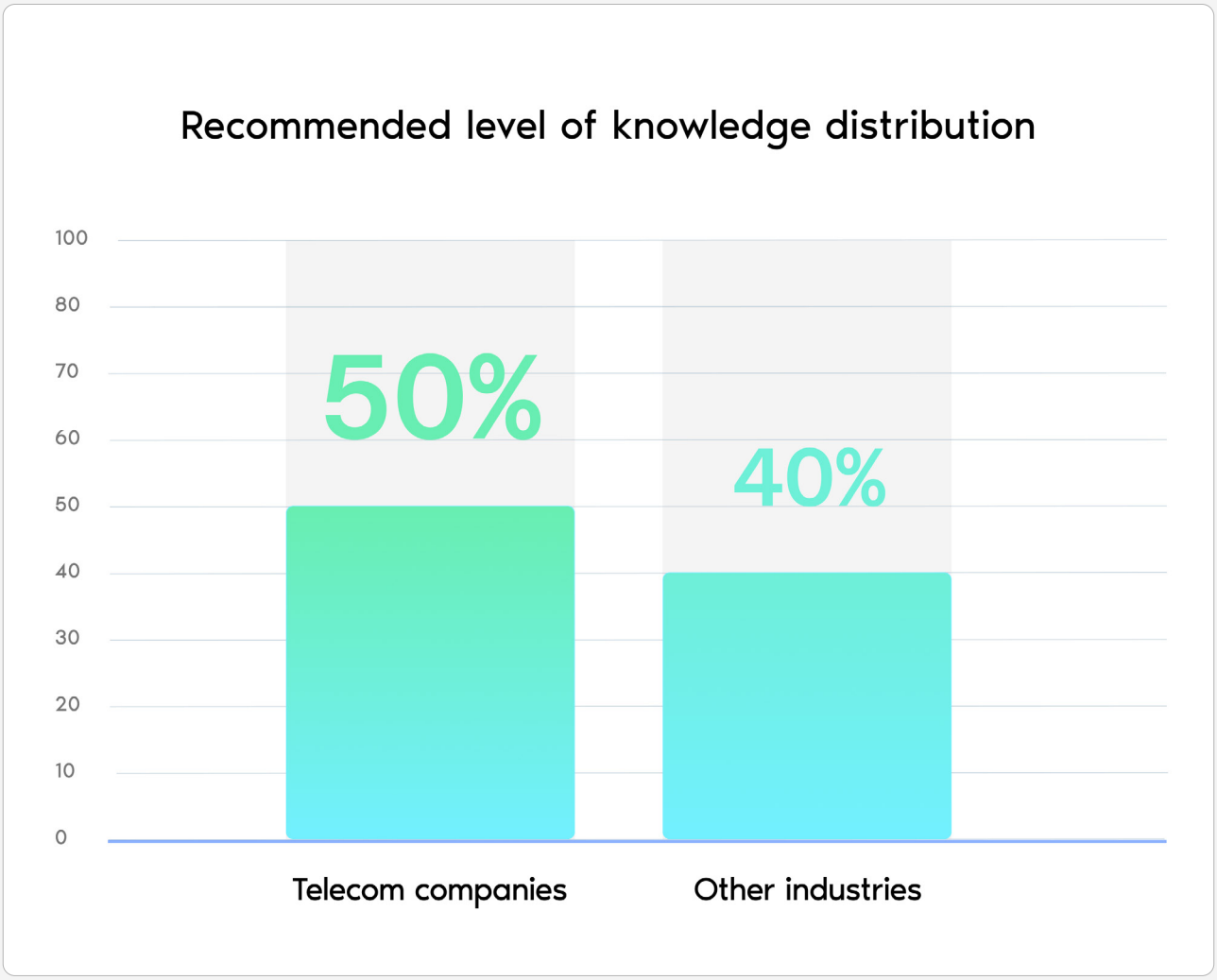
The challenge isn't just hiring. IBM estimates that the half-life of tech skills has dropped to just 2.5 years, meaning that even current employees need continuous learning to stay productive. Meanwhile, 74% of employers say they are struggling to find the skilled talent they need, and in another study, 42% say the specialist skills they need simply don't exist in the external market.

In this environment, how knowledge is shared across the organization–not just who holds it–matters more than ever.

Telecom leads on knowledge distribution, but gaps remain

Our data shows that telecom outperforms other industries when it comes to knowledge distribution. The average telecom system scores 3.9 stars–well above the 2.8-star cross-industry average. And 50% of telecom companies meet or exceed our recommended threshold for effective knowledge sharing.

This is encouraging. Strong knowledge dis-tribution means fewer single points of failure, faster onboarding, and smoother handovers. It also equips teams to adapt as technology evolves.



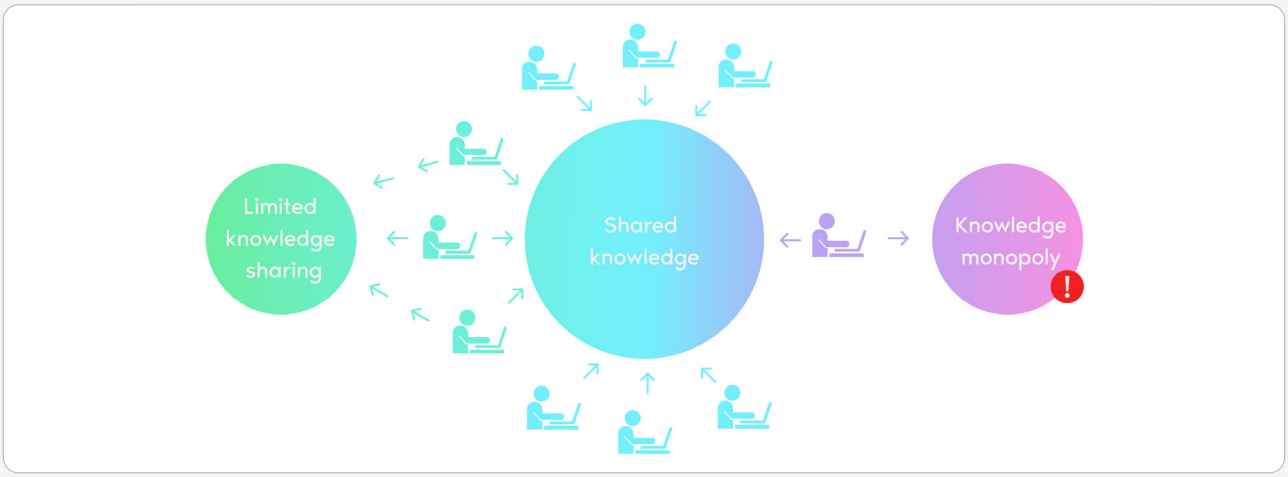
But there's still work to do. Half of all telecom systems still fall short of the recommended threshold, meaning siloed knowledge remains a significant barrier in many organizations. In high-pressure environments where the only person who knows how a system works is unavailable, even routine changes can turn into costly delays. Leaders who actively dismantle knowledge monopolies–and embed sharing into how teams operate–are better positioned to scale, pivot, and recover fast.

The risks of knowledge monopolies

• **Higher operational costs** →	New engineers struggle to navigate undocumented or complex legacy systems.
• **Longer recovery times** →	When key experts leave, it takes longer to resolve issues and restore service.
• **Slower system evolution** →	Poorly distributed knowledge limits agility, delaying critical innovations like AI-enabled services or real-time analytics.

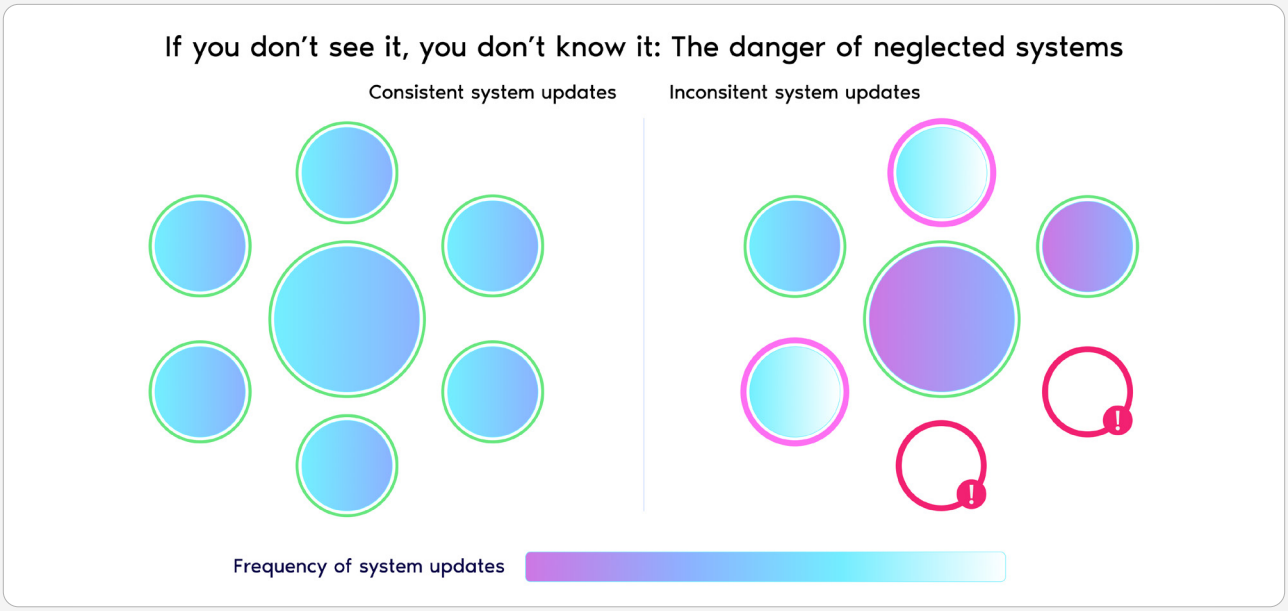
For telecom companies managing increasingly complex digital systems, these risks scale quickly–draining resources and threatening both reliability and innovation.

How knowledge monopolies form: The risk of uneven knowledge distribution



If you don't see it, you don't know it: The danger of neglected systems

When components aren't consistently updated or maintained, systems become harder to evolve, introducing security, cost, and compliance risks. In an industry where uptime is non-negotiable, these blind spots create unnecessary exposure.



To stay competitive, make knowledge visible–and shared

Even the best systems degrade without visibility and upkeep. Our data shows that when teams don't regularly touch or update code, those systems become harder to evolve, which creates blind spots that compound over time.

To stay resilient and agile, telecom leaders should treat documentation, mentoring, and regular code walkthroughs as strategic priorities. The more evenly knowledge is spread, the faster teams can recover, pivot, and build for what's next.

Chapter 5: Telecom's AI future depends on software discipline

Key findings:

- AI and big data systems score an average of just 2.7 stars on build quality–below the benchmark average.
- 89% of industry executives in telecom are piloting or already implementing AI.
- AI systems contain just 1.5% test code vs. 43% in traditional systems, increasing fragility.

Telecom is betting big on AI. Research by Nvidia shows that 97% of industry executives are piloting or already implementing AI to improve customer experiences, enhance security, automate processes, increase productivity, and refine network operations. In addition, an IBM study shows that in the last few years, commercial deployment of AI – particularly in generative AI use cases – increased fourfold, underscoring the industry's full commitment to the AI age.

These stats combined? A clear signal that telecom sees AI as a must-have.

And the optimism is well-founded, both from an operational and a security point of view. Machine learning AI can be used to analyze real-time network data to make intelligent predictions and automatically adjust operations to enhance overall performance. In addition, IBM reports that leading adopters of AI systems (not limited to generative AI) have already reduced security breaches by nearly half. This highlights one of AI's many benefits in telecom–and a potentially powerful tool for addressing the cybersecurity risks discussed in Chapter 2.

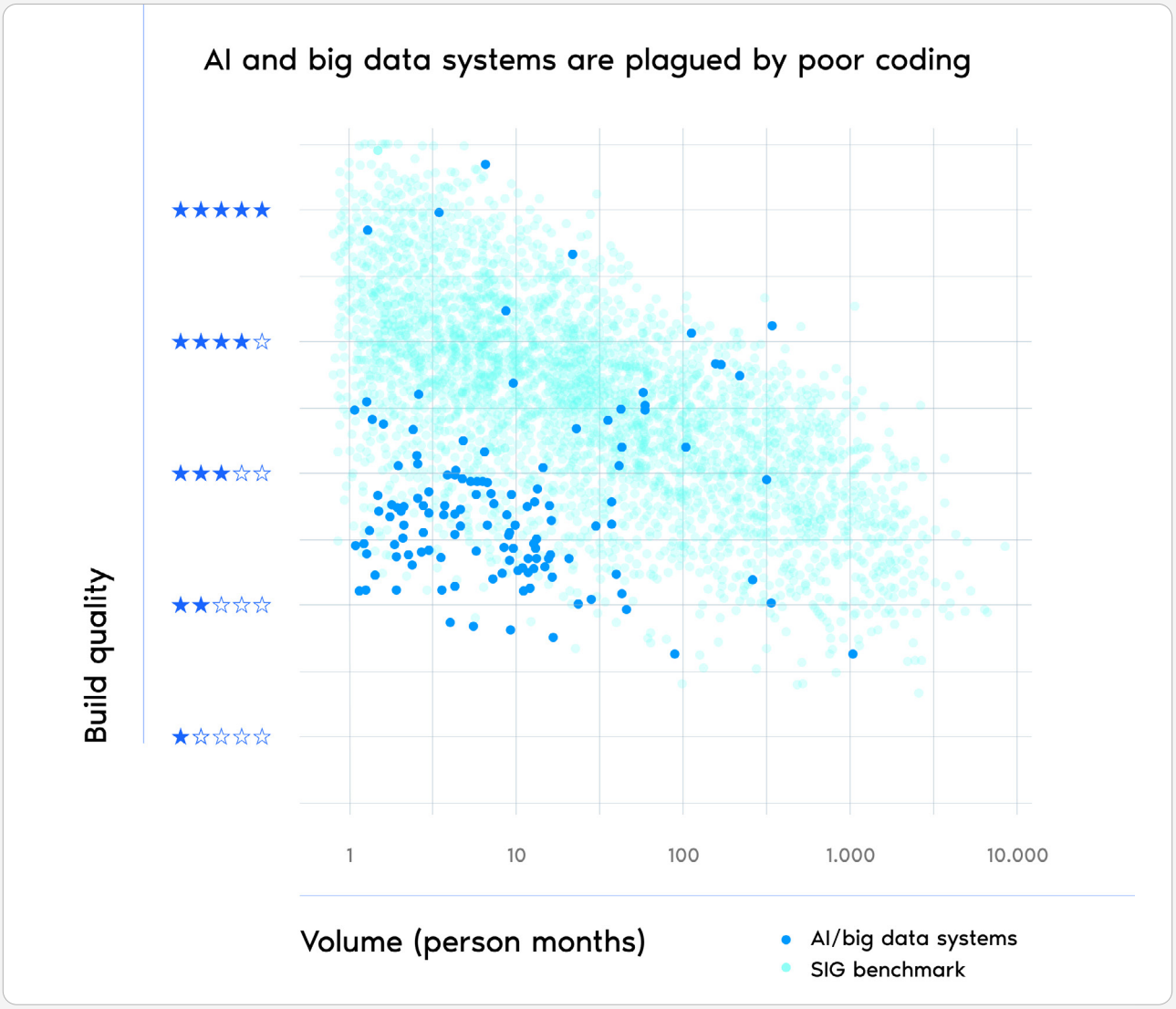
AI vs. traditional software

Despite its potential in telecom, AI can introduce new risks that many teams aren't used to managing. To understand these risks, we must first define what we mean by 'AI', beyond the buzzwords.

Unlike traditional software, which follows fixed rules, AI systems learn from data, adapt over time, and make autonomous decisions–often without predictable outputs. ISO/IEC 5338, co-developed by SIG, classifies AI systems as distinct due to these characteristics. AI software often needs to interpret language, images, or patterns, make probabilistic judgments, and evolve through retraining. That makes them harder to test, govern, and maintain–especially when engineering discipline is lacking.

Many AI systems aren't built to last

AI systems are only as good as the software they run on. But many AI systems aren't engineered with longevity in mind. 73% of AI and big data systems show structural quality issues–scoring below the SIG benchmark average in build quality, with an average rating of just 2.7 stars, significantly lower than traditional software systems.



Our dataset of AI/big data systems was compiled by selecting systems that revolve around statistical analysis or machine learning, based on the technologies used (e.g. R and Tensorflow) and documentation.

The logical next step is to ask why this is happening. SIG's cross-industry research highlights two major issues:

- **Complex, bloated code** → AI systems often have long, unfocused code blocks handling multiple responsibilities, making them difficult to modify, analyze, and reuse.
- **Lack of testability** → AI and big data systems contain just 1.5% test code, compared to 43% in traditional systems, making errors harder to detect and AI models riskier to update.

In telecom, where build quality is already a prevalent issue, leaders must be careful not to compound the issue with AI built on shaky foundations, but rather to improve the quality of their software.

The path forward: Build AI like critical infrastructure

To realize long-term value from AI, telecom companies must treat it as serious software rather than as an experiment. That means applying the same disciplined engineering practices used in core systems, from architecture and documentation to testing and governance.

SIG's data and client work suggest four essential steps:

1. Apply software engineering best practices	→ Modular, maintainable, and well-documented code is essential for building AI that can evolve over time.
2. Bridge AI and software engineering teams	→ Many AI systems are still developed in silos. Integrating software engineers into AI projects improves long-term stability and avoids creating legacy from day one.
3. Strengthen AI governance	→ Organizations should define clear accountability and align AI development with policies for risk, compliance, and transparency.
4. Implement continuous validation	→ AI systems degrade over time. Regular testing and retraining are critical to ensure safe, scalable performance.

Treating AI as a core capability–built to scale and governed with intent–is the only way to unlock its full potential in the telecom sector.

Chapter 6: Green IT is the hidden lever in telecom's net-zero push

Key findings:

- 87% of telecom emissions come from indirect sources, including software and digital infrastructure.
- European telecoms cut emissions by ~50% between 2019 and 2022–despite a doubling in data traffic.
- Refactoring common telecom languages like Java can cut energy use by up to 17%.

Telcos are decarbonizing at pace. Between 2019 and 2023, global telecom emissions dropped by 8%, and European operators led with a 56% reduction. This progress came despite a fourfold increase in data traffic–driven largely by smarter, software-based efficiencies like network automation and virtualization. Still, 87% of telecom's carbon footprint stems from indirect sources, including cloud infrastructure, devices, and the software itself. Despite encouraging momentum, the same report from GSMA warns the pace must double to remain on track for net-zero by 2050.

Sustainable software is a cost and compliance issue

Green IT isn't just about optics or Environmental, Social, and Governance (ESG) reporting. To truly decarbonize IT, organizations must turn their attention to software, which is the unseen layer driving emissions through compute load, storage use, and inefficiencies in code.

Historically, Green IT initiatives have focused on replacing legacy hardware with more energy-efficient alternatives and ensuring responsible recycling. However, to 'green' IT as a whole, means of making software and its development more sustainable are now being more seriously considered. With this in mind, it's clear that sustainable software engineering must be part of the solution.

Optimizing software for energy efficiency has a direct impact on both **cost** and **compliance**. As more telecom companies commit to net-zero or emissions reduction targets, software becomes part of the measurable equation–and the business's bottom line.

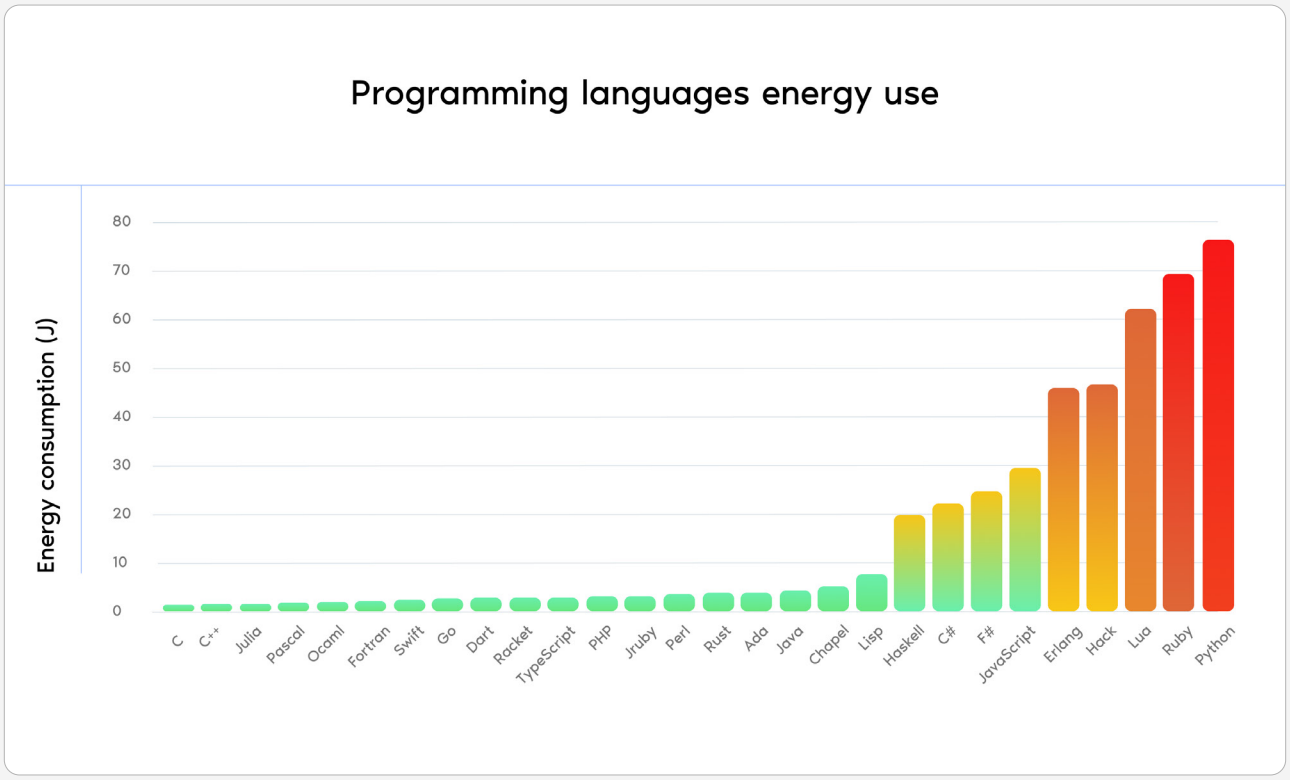
Sustainable software delivers measurable business value:

• **Reduced emissions**	→	Cut unnecessary compute, storage, and load to shrink IT's carbon footprint.
• **Faster software**	→	Lean systems improve performance and reduce latency.

• **Scalable by design**	→	Right-sized code adapts to real demand, preventing overprovisioning.
• **Ready for regulation**	→	Sustainable software supports ESG, CSRD, and IFRS compliance.

Programming languages impact energy use

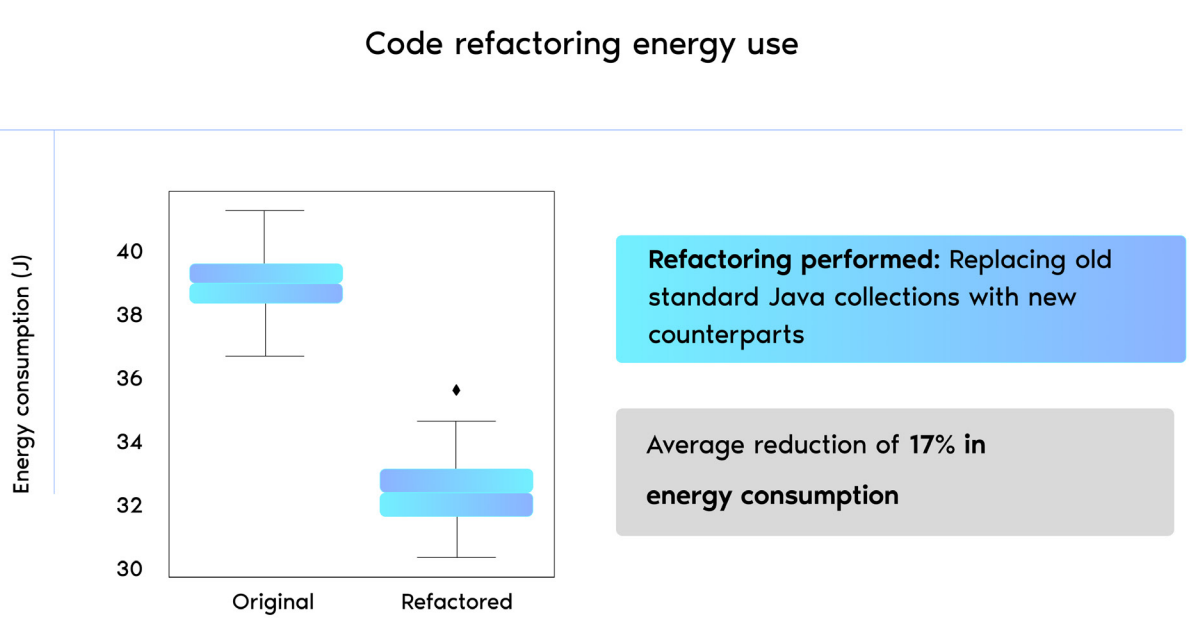
The choice of programming language directly affects a system's energy consumption. IT leaders in telecom need to consider sustainability alongside performance, scalability, and long-term build quality when selecting technologies. While rebuilding a system in a new language isn't always feasible, the trade-offs are worth evaluating–especially as digital workloads continue to grow.



Telecom must act on software efficiency

Telecom's software stack matters–not just for performance, but for sustainability. SIG data shows that Java and C# are the most commonly used technologies in the telecom sector. These languages aren't the most energy-intensive overall, but they still present untapped opportunities for efficiency gains.

Java, in particular, dominates many telco systems. While it's definitely not the most energy intensive, there are still opportunities to improve. SIG's analysis reveals that targeted refactoring of Java code –such as replacing legacy collections or improving data handling–can reduce energy consumption by up to 17% on average. With Java so widespread in telecom, even modest improvements at scale could significantly reduce resource usage.



Poorly structured code doesn't just cost more to maintain–it consumes more compute, inflates cloud bills, and drives up emissions. The good news: these are solvable problems. Clean architecture and disciplined engineering can help telcos cut energy usage without necessarily switching languages or sacrificing stability.

As sustainability pressures mount, software modernization and quality improvements offer a practical lever telecom leaders can pull today.

Key takeaways & conclusion

• **Build quality can be a huge hidden cost in telecom.**	67.2% of systems fall below SIG's recommended build quality. This can drive up costs, outage risk, and technical debt.
• **Security must be built into the code.**	74.1% of telecom systems have an at or below market average degree of security controls, closely linked to vulnerabilities in the codebase.
• **Modern architecture accelerates transformation in telecom.**	Only 2% of telco systems still rely on legacy tech. Modern architectures support change up to 30% faster, making this a promising signal.
• **Knowledge sharing builds resilience.**	50% of systems meet SIG's threshold for knowledge distribution–reducing risk and improving agility, but 50% still fall behind.
• **Successful AI adoption depends on solid software engineering.**	73% of AI systems show structural flaws. AI without quality is fragile, costly, and hard to scale.
• **Green IT cannot be overlooked.**	Refactoring Java in telco systems can cut energy use by up to 17%. Efficient code supports climate goals and reduces cost.

Telecom's next leap depends on software quality

Telcos racing to deliver high-speed, AI-powered, and always-on services can't afford fragile software foundations. From resilience to sustainability, software quality is a strategic multiplier.

Want to see how your systems compare?
Contact us today to benchmark and future-proof your software landscape.

Written by Software Improvement Group

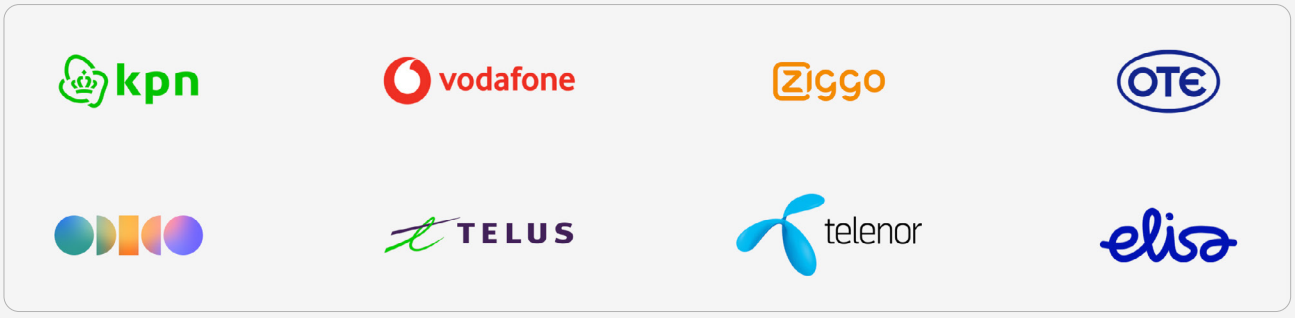
Software Improvement Group (SIG) leads in traditional and AI software quality assurance. Empowering organizations to become more resilient and agile by guiding them to enhance their software quality and security through deep source code analysis and tailored, strategic advice.

Sigrid® - its software assurance platform - leverages the world's largest database containing over 300 billion lines of code across more than 20,000 systems and 300+ technologies and intelligently recommends the most crucial initiatives for organizations. SIG complies with multiple ISO/IEC standards, including ISO/IEC 27001 and 17025, and has co-developed ISO/IEC 5338, the new global standard for AI lifecycle management.

SIG was founded in 2000 and has offices in New York, Copenhagen, Brussels, and Frankfurt, and is headquartered in Amsterdam.

Sigrid®, together with expert software engineering consultants, and over 25 years of industry-leading research, position SIG as the foremost authority on software excellence.

Trusted by



Ensure your software is always two steps ahead

Modernize your stack, secure your network, and stay in control.

Discover SIG for Telecom

Telecom signals 2025

Software Improvement Group