Software
Improvement
Group

Finance signals 2025

A report on the hidden costs and risks of IT in the financial sector

Table of contents

Executive summary

This report delivers critical insights for CIOs, CTOs, and technology leaders in the financial services industry (FSI), helping them make informed, strategic decisions.

At Software Improvement Group (SIG), we've been tracking software trends in FSI for years. While the industry has made impressive strides in digitalization, many hidden risks and challenges remain.

The 6 key insights of 2025

So, what's where does the industry stand in 2025? Our research uncovered 6 key insights.

1. Cybersecurity remains a critical concern → FSI outperforms other industries in security, yet 44% of systems still have an average or below-average security rating, leaving them vulnerable to cyber threats.

2. Software maintainability drastically impacts costs and innovation capacity → Poor software quality can lead to an average of €2.25 million in additional maintenance costs per system, per year, reducing efficiency and slowing innovation.

3. Legacy technology is a bottleneck for agility → 37% of systems built on legacy technology have lower architecture scores, making change up to 40% slower.

4. Knowledge monopolies in software development teams contribute to the talent crisis → 66% of FSI systems fail to meet our recommended knowledge-distribution rating, creating teams where critical expertise is isolated, increasing risk and slowing progress.

5. AI adoption is booming, but most AI systems fall short on quality → AI adoption is accelerating, yet 73% of AI systems have quality issues that can threaten long-term success.

6. The need for sustainable IT goes beyond regulatory pressure → While sustainability commitments are increasing, FSI is lagging in Green IT adoption, missing opportunities to reduce emissions and costs.

Foreword

The financial sector is evolving rapidly, with AI leading the charge. From automated fraud detection to hyper-personalized customer experiences, AI is unlocking capabilities that were unthinkable just a few years ago. Yet, with these advancements come unprecedented risks. At the same time, the financial services industry must navigate rising cyber threats, aging legacy systems, a growing talent shortage, and the increasing push for sustainability.

For FSI leadership, many don't realize that the key to success lies in software quality. It determines whether institutions can:

- **Secure their systems against evolving threats,**
- **Control costs by improving maintainability,**
- **Modernize effectively without introducing unnecessary risks,**
- **Leverage AI while maintaining reliability and compliance,**
- **Reduce environmental impact through sustainable software practices**

Without structured software assurance, the financial services industry will struggle with rising costs, security vulnerabilities, and operational inefficiencies.

This report provides data-driven insights into the biggest software challenges FSI organizations face today, backed by the world's largest database containing over 300 billion lines of code across more than 20,000 systems and 300+ technologies.

Whether you're looking to reduce risk, optimize costs, or future-proof your IT landscape, this report will help you make informed, strategic decisions.

Let's shape the future of financial services–starting with better software.

Luc Brandts,

CEO of
Software Improvement Group

Chapter 1: The rising cybersecurity crisis

Key findings:

01 FSI outperforms other industries in security, yet **44% of systems still have an average or below-average security rating**, leaving them exposed to potential breaches.

02 It is estimated that **the average software system has about 19 critical security findings**, increasing operational risks and compliance concerns.

03 There is a strong correlation between the security rating and the maintainability rating of the software: **Systems that have an above market-average build quality are twice as likely to achieve a high security compliance.**

The need for a holistic cybersecurity approach

Cyber threats are growing more sophisticated, and financial institutions remain prime targets. In an industry built on trust, software security is non-negotiable—yet our data shows that nearly half of FSI systems still fall short of recommended security standards.

We tend to see that security is often treated as a final checkpoint rather than a fundamental part of the software development process. This reactive approach leaves organizations vulnerable to breaches, compliance risks, and costly remediation efforts.

A common misconception is: *"We have penetration tests, so we're secure."*

While penetration testing (pentesting) is an essential security measure, it's not enough. It typically occurs late in the development cycle, meaning vulnerabilities are only discovered when they're costly and time-consuming to fix.

Instead, FSI organizations should adopt Security by Design—a proactive approach that integrates security at every stage of the software development lifecycle (SDLC). This shift from reactive to proactive security measures is critical to reducing risk and ensuring long-term resilience.

The multi-layered approach to cybersecurity

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

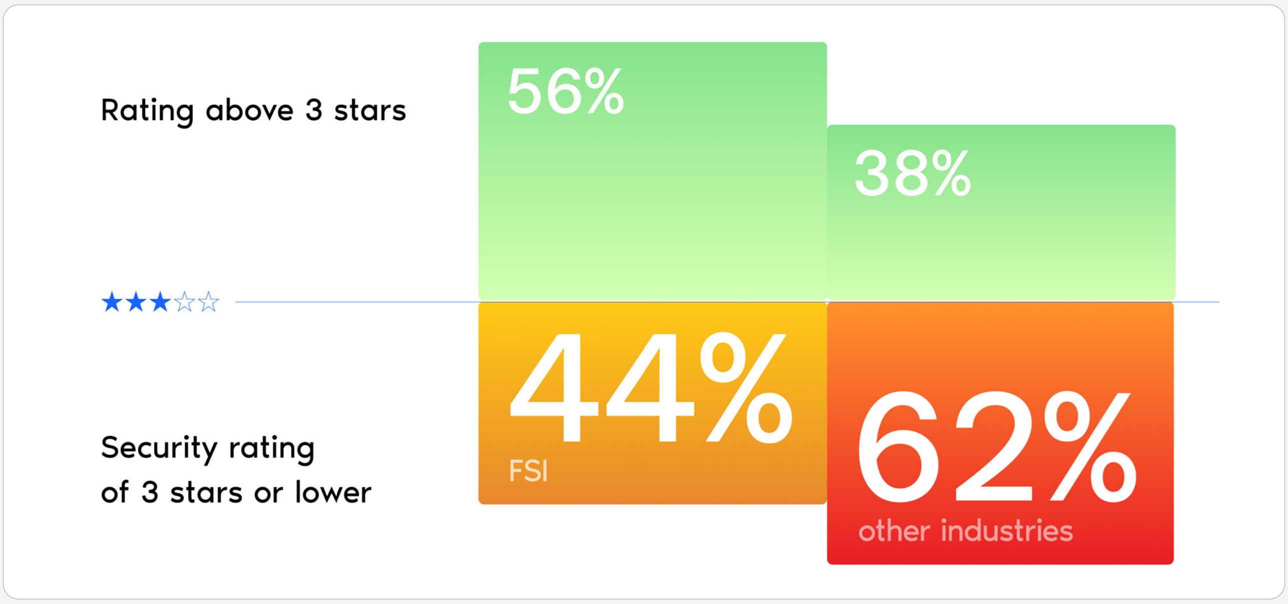
The three key methodologies in software security testing are:

- **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. Software Improvement Group's security assessment covers SAST and SCA and is complementary to penetration testing. Either can find security weaknesses that the other is fundamentally unable to find. Together, they provide a proactive security strategy that reduces risk, strengthens compliance, and ensures secure software development from the start.

44% of FSI systems have an average or below-average security rating

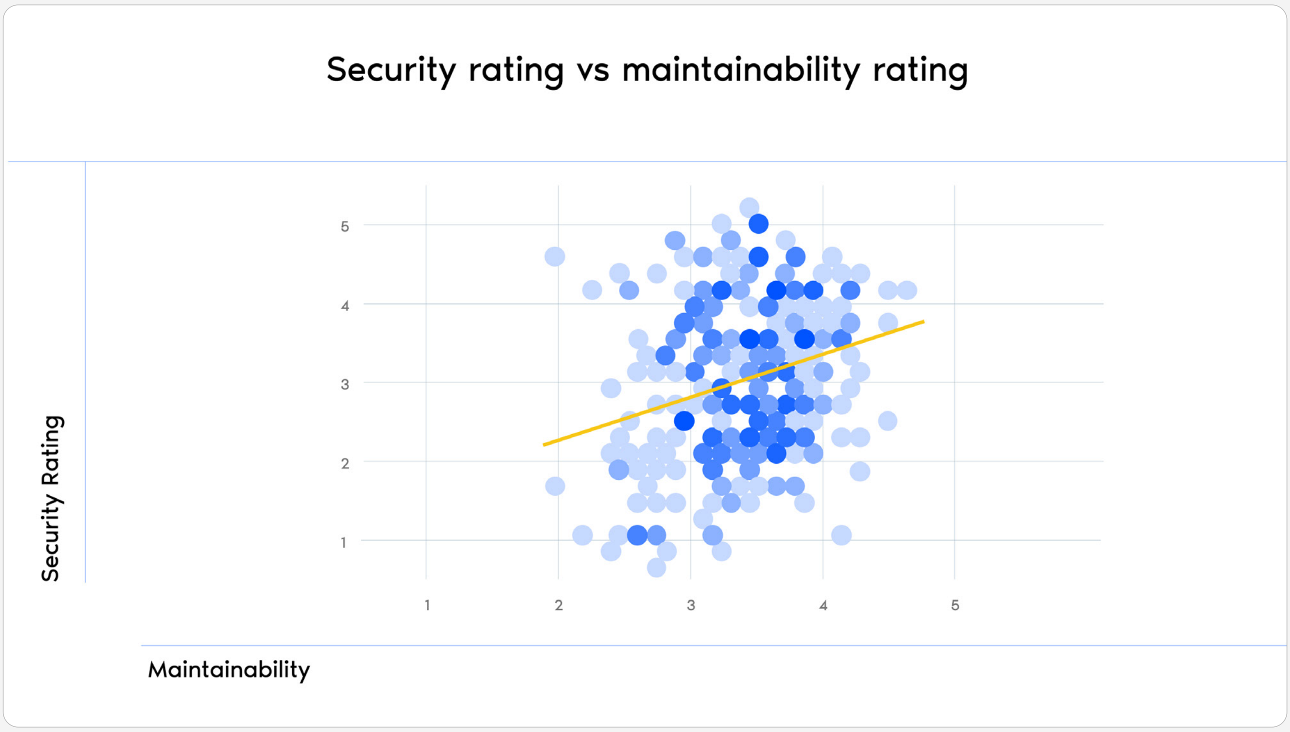
While it's comforting to see that FSI organizations are performing better than the average across industries, 44% of FSI systems have an average or below-average security rating, exposing them to compliance risks, fraud, and reputational damage.



Based on a snapshot of active security findings in all systems in our data warehouse on a random day in June 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.

Systems that have an above-market-average build quality are twice as likely to achieve strong security compliance

Our benchmark data proves that ***poor software quality strongly correlates with a higher number of security vulnerabilities.***



This visual shows an estimate based on a snapshot of active security findings in all systems in our data warehouse on a random day in June 2023. A darker color blue indicates there are more systems in that area. We can see those systems with a maintainability score of 3 stars, have a 54% higher security rating than systems with 2* maintainability and systems with 4 stars have a 108% higher security rating.

The reason? 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, FSI organizations can proactively reduce risk, detect vulnerabilities early, and prevent costly breaches.

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

Yiannis Kanellopoulos

Founder & CEO at code4thought,

Avoiding a False Sense of Cybersecurity webinar

The scale of security findings

Based on our data, we could calculate an estimation of security findings in an average system. We found that it's not uncommon for an average-sized software system to have 19 critical security findings.

19

Critical security findings per system

*This estimation is based on a snapshot of active security findings in all systems on a day in June 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, the average breach globally costing $4.88 million, why take the risk? Catching vulnerabilities early in the development process can help FSI organizations avoid things like costly breaches, business disruption, and reputational harm.

The open-source dilemma

Open-source software (OSS) usage is on the rise, playing a big part in FSI organization's digital transformation strategies. According to the 2024 State of Open-Source Report, ***nearly 60% of FSI organizations are increasing their use of OSS***. Certainly, OSS helps cut costs, develop and deploy new applications faster, and modify and tailor software, but it also introduces hidden risks.

Our earlier findings showed that 50-60% of enterprise software systems contain at least one vulnerable open-source dependency each month, and ***30% have a critically vulnerable dependency.***

To mitigate these risks, FSI organizations need a **Software Composition Analysis (SCA)**, which scans dependencies for vulnerabilities, licensing issues, and legal risks.

Building a resilient cybersecurity framework

As we've learned, cybersecurity is a lot more than just firewalls and monitoring. It starts with the code itself. FSI organizations must adopt a secure-by-design approach, integrating security into every stage of software development.

By improving software maintainability, addressing vulnerabilities early, and managing open-source dependencies effectively, FSI organizations can build more resilient software and maintain customer trust despite inevitable cyber threats.

Chapter 2: How poor maintainability drains budgets

Key findings:

01 **36% of FSI systems fall below our recommended maintainability rating**, leading to higher costs and operational inefficiencies.

02 Poor system quality can drive **€2.25 million in additional maintenance costs** per system, per year.

03 4-star maintainability systems unlock **30% increase in innovation capacity**, allowing FSI organizations to focus on value-driven initiatives instead of just keeping systems running.

For financial institutions, cost optimization is a top strategic priority. Yet one major factor often goes overlooked: software maintainability.

What is maintainability? It's the ease with which you can repair, improve, and understand the source code of your software –all essential for reducing costs, accelerating innovation, and staying compliant.

It may be somewhat shocking to learn that according to Garner, on average 70% of IT budgets go toward maintenance, not innovation.

Over a third of FSI systems fall below our recommended maintainability rating

Our benchmark data shows that *36% of FSI systems fall below our recommended maintainability rating*, leading to higher maintenance costs and lower operational efficiency.

★★★★☆

Maintainability rating

36%

of FSI systems fall below our recommended maintainability rating of 4 stars

Maintainability is determined through automated source code analysis. Maintainability according to the ISO 25010 standard has five sub-characteristics: Analyzability, Modifiability, Testability, Modularity, and Reusability. These sub-characteristics can be seen as a representation of the phases that are passed when performing maintenance work. Software Improvement Group measures a set of properties of source code, as defined by the SIG/TÜViT Evaluation Criteria for Trusted Product Maintainability. The outcomes are compared to the SIG Benchmark, which is recalibrated yearly from thousands of systems in the SIG dataset. This results in a star rating. The ISO 25010 standard refers to maintainability as: "The degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements."

Lower maintainability leads to higher costs and lower innovation capacity

Poorly maintained systems can lead to up to

€2.25 million

in excess maintenance costs per system, per year.

* In FSI, a 3-star system needs 1 FTE (0.7) per system per year more than what you would need if your system was 4 stars, and a 2-star system would need 14 FTE more per system, per year compared to 4 stars. Based on a yearly estimated wage of €150,000 per FTE.

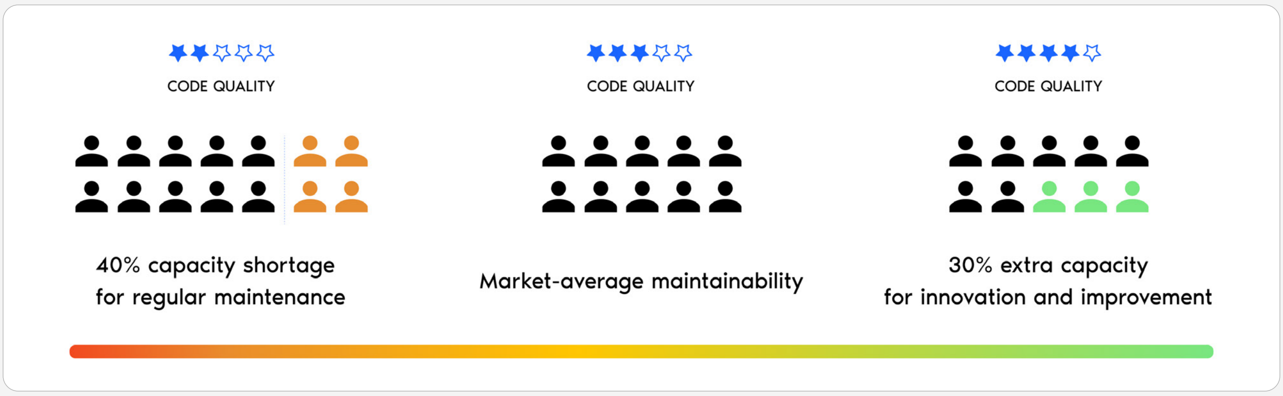
This can add up quickly as it is not uncommon for FSI organizations to have hundreds of systems.

Systems with a higher code quality score gain 30% extra capacity for innovation and improvement

FSI organizations with higher-maintainability software gain a 30% boost in innovation capacity. Why? Because when less time is spent on fixing existing systems, more effort can be invested in developing new products, enhancing customer experiences, and driving digital transformation.

Our data shows that:

- **4-star maintainability systems unlock 30% more capacity for innovation and improvement.**
- **2-star systems experience a 40% capacity shortage, as teams are constantly firefighting instead of innovating**



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.

Industry pressures on cost reduction

The financial industry is under mounting pressure to reduce costs while maintaining innovation and compliance. KPMG research indicates that ***banks aim to achieve 10% cost efficiencies within 12 months, with targets increasing to 20-30% over the next three years***.

But meeting these ambitions is easier said than done.

A survey by Infosys found that only ***one in four banks achieve the expected returns from their IT cost optimization programs***. Many banks struggle due to the complexity of their IT environments, which often include a patchwork of legacy systems that have grown over decades without sufficient consolidation or modernization.

Barriers to cost optimization

- **Outdated systems create inefficiencies** → Many banks rely on layered legacy systems that were never streamlined. Instead of replacing outdated technology, new systems are often added on top, increasing complexity and making cost-saving efforts harder to implement.
- **Short-term growth vs. long-term efficiency** → Cost optimization is often deprioritized during periods of growth. With shifting economic conditions, financial institutions struggle to balance immediate expansion with the need for sustainable cost reductions.
- **Resistance to change** → Many cost-cutting initiatives focus solely on reducing expenses rather than improving efficiency. But success requires a mindset shift. This means understanding that modernization leads to long-term savings and a stronger return on investment.

Understanding the total cost of ownership (TCO) of software

Despite IT budgets being under scrutiny, quantifying the true Total Cost of Ownership (TCO) of software remains a challenge. Many organizations fail to consider the ongoing costs of maintaining and operating software after development.

A path toward sustainable cost optimization

By improving software maintainability, FSI organizations can:

- **Reduce long-term IT costs** while increasing flexibility.
- **Speed up time-to-market** for new features and services.
- **Improve developer efficiency and retention** by reducing frustration with outdated systems.

The takeaway?

High-quality, maintainable software isn't just an IT best practice–it's a financial imperative.

Chapter 3: The true cost of legacy technology

Key findings:

01 **37% of FSI systems with legacy technologies** have a below-average architecture rating (compared to 11% of modern technologies).

02 Poor architecture slows down change-making updates **40% slower in 2-star systems versus 4-star systems.**

03 By 2028, failing to modernize could cost banks over **$57 billion, with missed revenue opportunities in payments alone reaching 42%.**

Financial institutions are built on legacy systems—many dating back to the 1980s and 1990s. While these systems still power critical operations, they are also one of the biggest barriers to agility, innovation, and cost efficiency.

By 2028, failing to modernize is projected to cost banks over $57 billion, one IDC study found, *with missed revenue opportunities in payments alone reaching 42% and potential cost savings of 21% annually.*

Despite rapid growth in the banking sector, expected to hit $1 trillion by 2028 according to Gartner, many financial institutions are struggling to modernize. The problem? **Legacy technology consumes the majority of IT budgets**, leaving little room for innovation.

Why legacy systems are holding FSI organizations back

Legacy systems may still "work", but they weren't built for today's digital economy. Most FSI organizations are still running older technology like COBOL. For example, Forrester research found that around *95% of ATM transactions still rely on COBOL, and an estimated 220 billion lines of COBOL code remain in use globally.*

But with most COBOL programmers retiring or clocking out for good soon, maintaining these systems is becoming increasingly difficult.

The urgency to modernize

So, it's clear that legacy modernization is needed to stay competitive, improve efficiency, and meet evolving customer expectations. But integrating modern technologies like AI, blockchain, and IoT also presents some tricky challenges.

Unlike FinTechs, which tend to be more agile and tech-driven, traditional banks are heavily regulated, more risk-averse, and slower to adapt. Their IT environments are complex, combining on-premises infrastructure, cloud services, and hybrid solutions, making modernization a slow and expensive process.

Instead of full-scale replacements, many banks opt to maintain existing systems while modernizing gradually, reducing risk and managing costs more effectively.

The reality of legacy modernization

While the financial services industry recognizes the need for modernization, but the risks and challenges are significant. According to a report by Advanced, ***74% of organizations fail to complete legacy modernization projects***. And modernization doesn't just mean outdated technology. It also relates to fragile architecture, poor design, and lost institutional knowledge.

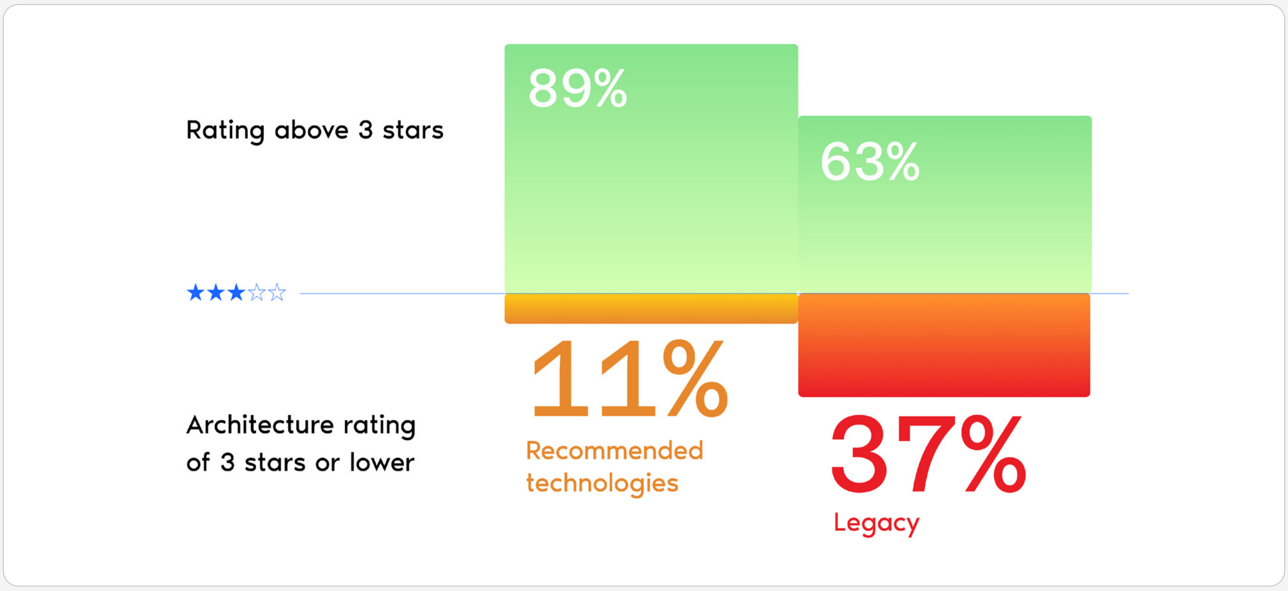
At Software Improvement Group (SIG), we used our Architecture Quality Model to quantify how well financial institutions manage modernization. The model captures six architecture aspects, covering both technical and social aspects, and evaluates the results against other systems in SIG's benchmark.

★★★★☆

Architecture rating

37%

of FSI systems with legacy technologies have a below-average architecture rating (compared to 11% of modern technologies)

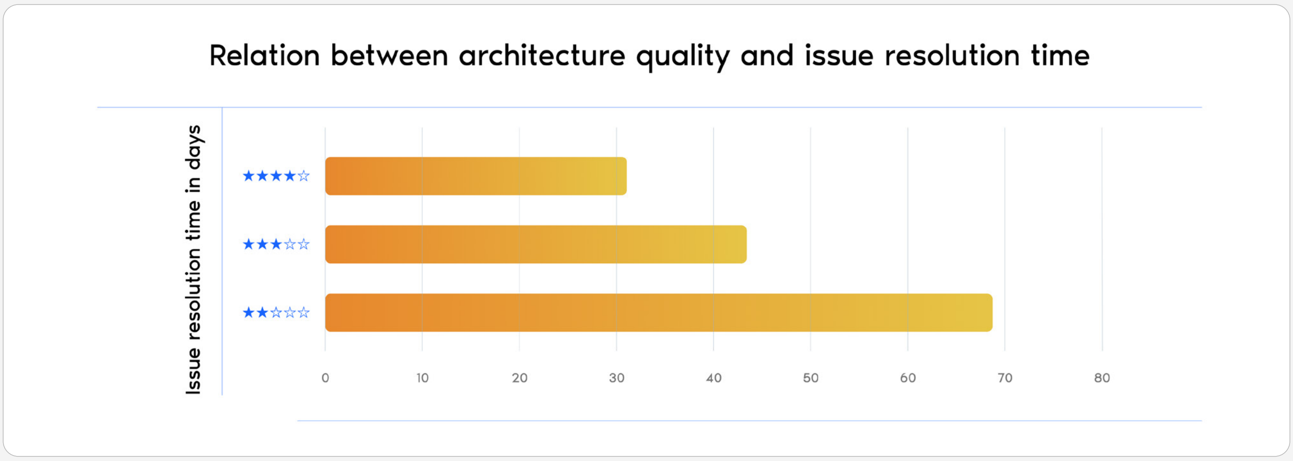


The SIG Architecture Quality model provides insight into the ability for an application to evolve as business needs change. SIG's Architecture Model maps architectural characteristics to 9 system properties: Code breakdown, component cohesion, communication centralization, component coupling, data coupling, bounded evolution, code reuse, component freshness, and knowledge distribution and maps them according to the 5 sub-characteristics represent properties of software architecture that affect the velocity in which foundational changes can be made to a software system: Structure, Communication, Data access, Evolution, Knowledge. It then comes up with a star-rating of 1 to 5 stars.

4-star architecture systems allow for changes to be made 30% faster

Our earlier research highlighted the efficiency gap between legacy and modern systems in financial services. Poor architecture slows down innovation, while well-structured systems enable faster, more agile technological advancements.

4-star architecture systems allow for changes to be made 30% faster than market-average systems, while 2-star systems experience a 40% slowdown when implementing changes.


Relation between architecture quality and issue resolution time

This diagram shows a correlation between architecture quality and issue resolution time. When it comes to architecture quality, it is, on average, 30% faster to make changes in a 4-star system than in a market-average system. Reversely, making changes to a 2-star system will be about 40% slower.

The path forward

So, what does this mean for you? Legacy systems aren't disappearing overnight, but FSI organizations that prioritize architectural improvements can outpace competitors in speed, efficiency, and innovation

Chapter 4: The skills shortage putting the industry at risk

Key findings:

01 **66% of FSI systems fail to meet SIG's recommended knowledge distribution rating,** creating "knowledge monopolies" that slow progress.

02 **70% of financial services CEOs see the lack of skilled professionals as a bigger threat** than competition or shifting customer demands.

03 Poor knowledge sharing increases risks—systems that rely on a small group of developers become harder to maintain, slower to improve, and riskier to scale.

As financial institutions accelerate digital transformation, talent shortages are becoming a major roadblock. The blazing pace of innovation calls for skilled professionals, yet many struggle to attract and retain the necessary talent.

According to PwC, 70% of financial services CEOs say ***the talent gap is a greater threat to growth than increased competition or changing consumer behavior.*** Despite this, only 28% are prioritizing upskilling their workforce.

The shifting talent landscape

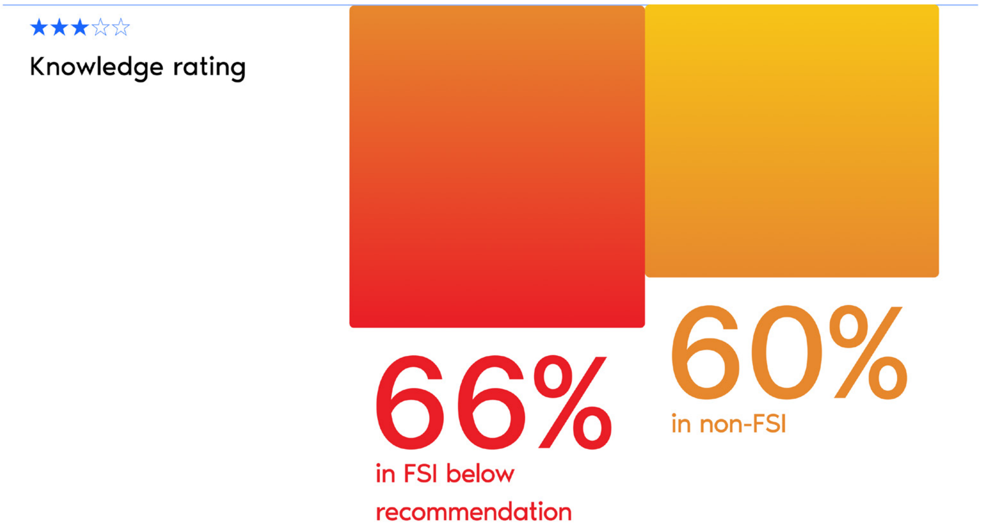
According to the World Economic Forum, Technology, digitalization, and sustainability are shaping the fastest-growing roles, particularly in the financial services industry. In the next five years, ***44% of current skills will need to evolve, and six out of ten employees will require retraining.*** Yet only half of them will have access to the necessary opportunities, leaving many unprepared for the industry's future demands.

Without a structured approach to knowledge retention and workforce development, FSI organizations risk falling behind in an increasingly competitive landscape.

The hidden knowledge crisis in FSI software development

Talent shortages are a challenge, but poor knowledge distribution within development teams makes the problem even worse. Our benchmark data reveals:

66% of FSI systems fail to meet SIG's recommended knowledge distribution rating, meaning critical expertise is concentrated in a small group of developers. This creates "knowledge monopolies"– where only a handful of people truly understand how a system works.



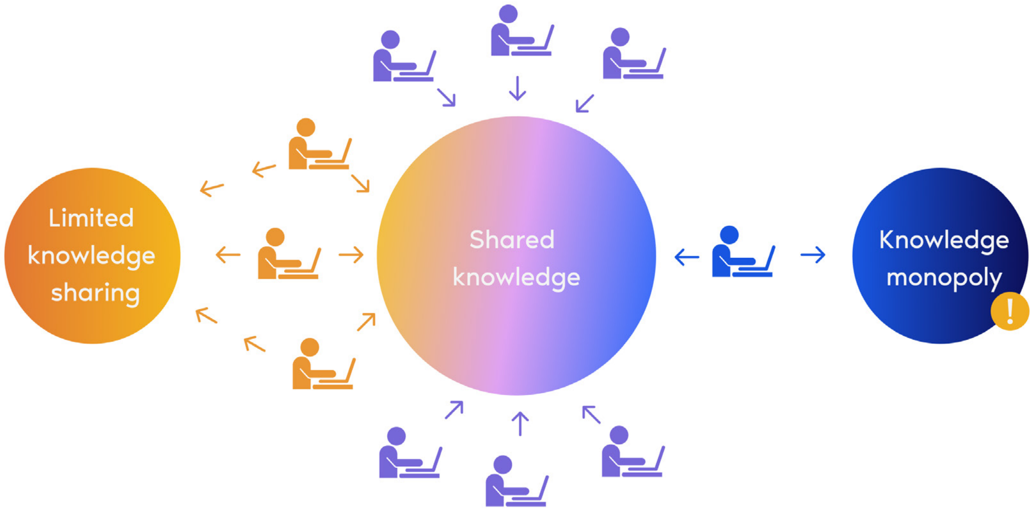
Architecture characteristics are defined by SIG's architecture quality framework. The SIG Architecture Quality model provides insight into the ability for an application to evolve as businessneeds change. The knowledge rating is one of the 5 aspects of Software Improvement Groups' Architecture model and consists out of 2 properties: "Component freshness" (measures the distribution of recent code churn across the system components as regular maintenance is being made) , and "Knowledge distribution" (measured as the number of authors with significant contributions to a component per KLOC (thousands of lines of code)).

The risks of knowledge monopolies?

- **Higher operational costs–new developers struggle to navigate undocumented or complex code.**
- **Longer recovery times–when key developers leave, it takes longer to fix issues.**
- **Slower software evolution–poorly distributed knowledge limits agility and adaptability.**

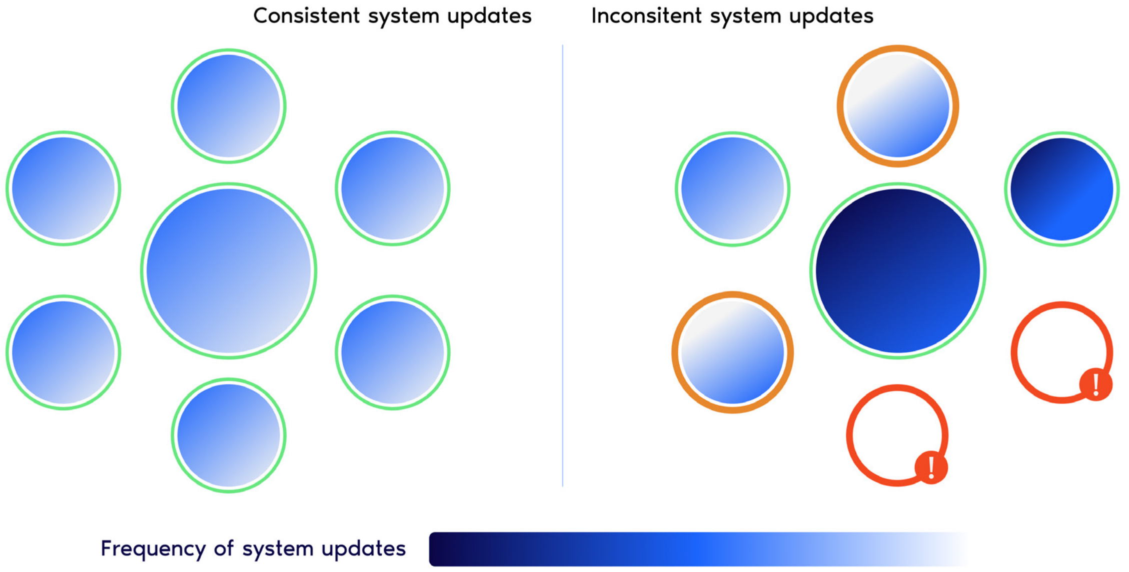
For FSI organizations managing hundreds of software systems, these inefficiencies scale exponentially, draining resources and increasing risks.

How knowledge monopolies form: The risk of uneven knowledge distribution



Next to this, FSI should aim to keep system components up to date. When system components aren't regularly maintained, they become harder to modify, increasing security and operational risks. Regular system updates are critical to ensuring long-term efficiency.

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


Consistent system updates
Inconsitent system updates
Frequency of system updates

Prioritizing skills and knowledge distribution

To remain competitive, financial institutions must prioritize knowledge-sharing, and upskilling strategies. Regular training programs, documentation practices, and component maintenance are key to reducing risk and ensuring a resilient, future-proof workforce.

Chapter 5: The challenge of AI adoption

Key findings:

01 AI adoption in financial services is accelerating, but **73% of AI and big data systems have quality issues,** making long-term success uncertain.

02 **AI is fundamentally different from traditional software,** requiring new approaches to security, maintainability, and compliance.

03 **Poor AI maintainability leads to higher costs and increased risks**—AI models degrade over time and require continuous validation and retraining.

In the past decade, FSI organizations have rapidly transitioned from manual, paper-based processes to digital-first operations. As more services move online, these institutions are generating unprecedented amounts of financial data, from customer behavior insights to spending patterns and transaction trends.

To leverage all this data and enhance their services, these same organizations are investing heavily in Artificial Intelligence (AI).

According to EY, AI is transforming financial services. From automated fraud detection to hyper-personalized customer experiences, AI is unlocking new capabilities that were unthinkable just a decade ago.

AI vs. traditional software

Despite its potential, AI also introduces risks many haven't faced before. Unlike conventional financial 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. AI also needs regular retraining to stay accurate.

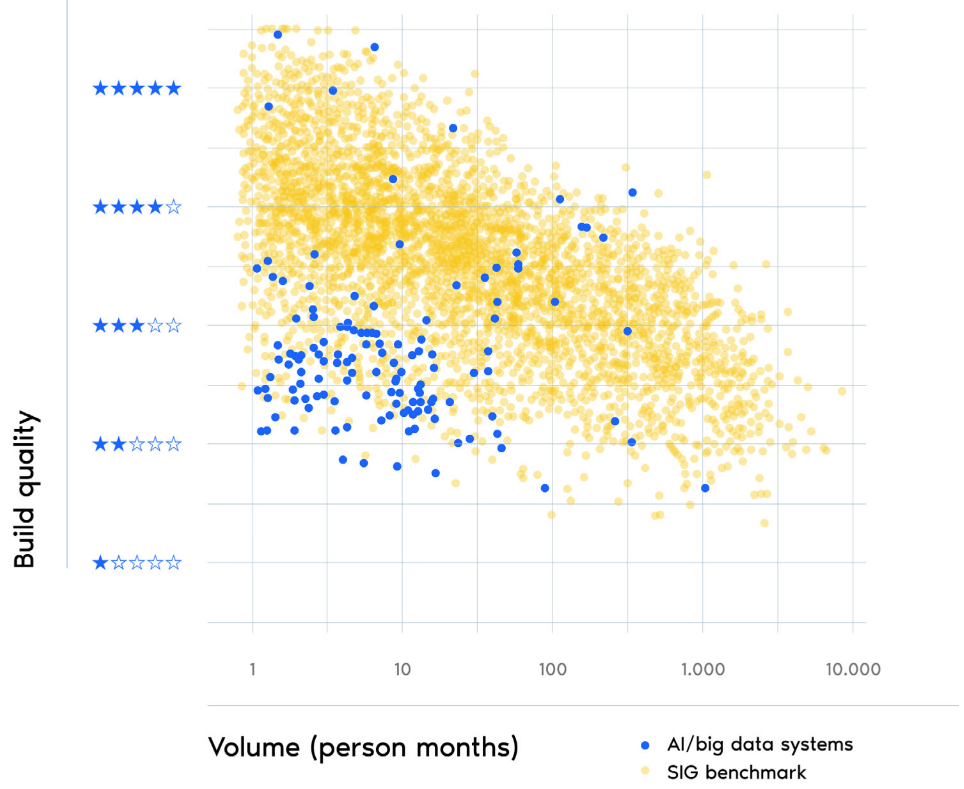
What sets AI software apart from traditional software is that it doesn't just follow fixed rules. Instead, it learns by analyzing large sets of data, finding patterns, and using that knowledge to make educated guesses when making decisions, solving problems, or answering questions.

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 needs strong engineering practices and proper regulation.

The AI maintainability crisis

Our benchmark data exposes a serious issue: most AI and big data systems suffer from poor maintainability and testability. ***In fact, 73% of AI/big data systems score below the benchmark average in maintainability,*** with an average rating of just 2.7 stars, significantly lower than traditional software systems.

AI and big data systems are plagued by poor coding



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.

But why is this happening?

SIG's 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.

Building reliable AI: Best practices

To ensure AI remains stable, secure, and scalable in the future, financial institutions must move beyond experimental AI and adopt enterprise-grade software engineering principles.

This includes:

- **Applying software engineering best practices** → AI development must prioritize modular, maintainable, and well-documented code.
- **Bridging AI and software engineering teams** → Integrating software engineers into AI projects ensures long-term stability.
- **Strengthening AI governance** → FSI organizations must define clear policies for AI transparency, ethics, and regulatory compliance.
- **Implementing continuous validation** → AI models degrade over time and require regular retraining and rigorous testing.

The path forward

As we've learned, AI is software, but it's unlike any software we've seen before. Unlike traditional systems, AI learns, evolves, and operates autonomously, requiring constant oversight and adaptation.

It can process vast amounts of data, interact through speech, vision, and even robotics, but its complexity introduces serious risks to security, reliability, and trust.

To build safe and trustworthy AI, FSI organizations must adopt strong engineering practices, continuous validation, regular retraining, and clear documentation.

For a structured approach to AI integration, download our free AI Readiness Guide today.

Chapter 6: The growing need to go green

Key findings:

01 On average, **code refactoring reduces energy consumption by 17%**—and in some cases, algorithmic optimizations cut energy use by up to 90%.

02 **35% of financial institutions are off-track to achieve net zero by 2050** and are still increasing emissions.

03 **Python**, one of the most widely used programming languages, is also among the most energy-intensive, highlighting the need for sustainable technology practices.

Just last November, the World Meteorological Organization (WMO) issued yet another Red Alert in its State of the Climate 2024 update, warning of the rapid pace of climate change within a single generation, fueled by rising greenhouse gas levels.

This has put financial institutions under growing pressure from regulators, clients, and society to be more transparent about their climate impact and sustainability efforts.

While more banks recognize the need to actively contribute to a greener economy, digital transformation is making things...well, complicated. As organizations move their systems online, IT infrastructure expands, leading to higher energy consumption and greater environmental impact.

And the outlook isn't great:

- **35% of financial institutions are off-track to achieve net zero by 2050 and are still growing emissions.**
- **80% of IT equipment emissions come from the production of new hardware.**
- **Only 50% of banks vs. 22% of insurers have adopted sustainable IT hardware practices like recycling and reusing equipment.**

But while FSI organizations focus on sustainable finance and ESG reporting, one major factor often goes unnoticed—the carbon footprint of their IT operations.

Why Green IT is needed

So, how can financial institutions reduce their environmental footprint and meet stakeholder expectations? This is where Green IT comes in.

And we don't just mean adopting greener technology. We mean changing consumption habits, embedding sustainability into every stage of IT operations, and making a conscious effort to measure, reduce, and optimize emissions. Real impact also requires strategic planning, engaged leadership, and sustainable software architecture.

But what exactly is Green IT?

Also known as green computing or sustainable IT, Green IT focuses on minimizing the environmental impact of IT operations. While a lot of attention goes to hardware and infrastructure (due to their massive carbon footprint), software also plays a huge role.

Poor coding standards, inefficient system architecture, and energy-draining coding structures (like excessive looping and conditional statements) increase energy consumption. These inefficiencies not only make software more resource-intensive to run, but they also demand more energy to maintain, fix, adapt, and scale over time.

The power of green software engineering

Green software engineering isn't just good for the environment. It can also boost performance, reduce costs, and improve compliance. Here's how:

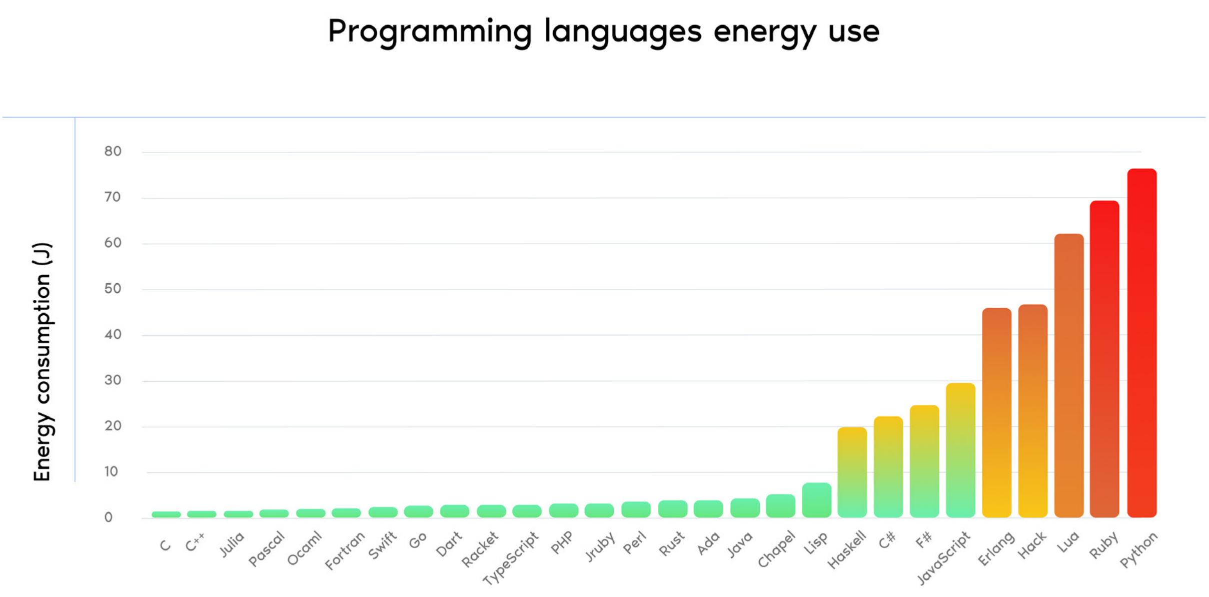
- **Reduce emissions** → The main goal is to cut greenhouse gas emissions by making software more energy efficient.
- **Lower costs** → More efficient software uses fewer computing resources, leading to lower hosting and cloud expenses.
- **Faster software** → Optimized workloads mean better performance, lower latency, and a smoother user experience.
- **Greater scalability** → Software that adjusts to actual demand performs better and is prepared for future growth.
- **Easier compliance** → Sustainable software practices help meet ESG reporting requirements (e.g., IFRS, CSRD).

Optimizing financial software for sustainability

At Software Improvement Group (SIG), we've been researching IT sustainability since 2014. Our findings highlight a direct link between software quality and energy efficiency.

Programming languages impact energy use

The choice of programming languages directly affects a system's energy consumption. FSI organizations should factor in sustainability alongside performance and scalability when selecting technologies. However, rebuilding an entire system in a new language isn't always feasible and should be carefully assessed.


Programming languages energy use

Generally speaking, and based on the last five years, we see that the technology with the highest energy consumption is still in the top 5 of most-used technologies in our database.

Top 5 technologies

1 Java

2 C#

3 Typescript

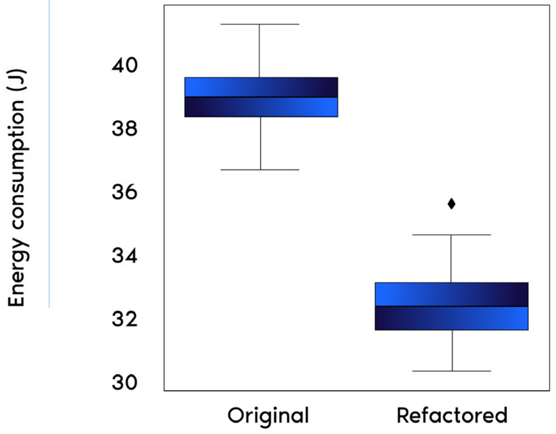
4 Javascript

5 Python

Simple code refactoring can slash energy use to up to 90%

On average, code refactoring reduces energy consumption by 17%. *In extreme cases, algorithmic optimizations have cut energy use by up to 90%.*

Code refactoring energy use



Refactoring performed: Replacing old standard Java collections with new counterparts

Average reduction of **17% in energy consumption**

The bottom line

Green IT isn't just a nice-to-have, it's a necessity. By optimizing both hardware and software, financial institutions can lower emissions, reduce costs, and build a more sustainable future.

Conclusion

Strong software is the backbone of a resilient financial services industry

The financial services industry has always adapted to change, but today's landscape presents unprecedented challenges. Cybersecurity threats, rising costs, aging infrastructure, talent shortages, AI adoption, and sustainability pressures are converging like never before.

Throughout this report, one message has been clear: *Software quality is the common denominator across all these challenges.*

A proactive approach to software excellence determines how well FSI organizations can:

- **Secure their systems and mitigate cybersecurity risks.**
- **Control costs by reducing technical debt and improving maintainability.**
- **Modernize operations without increasing risk or disrupting business continuity.**
- **Leverage AI effectively while maintaining quality, transparency, and compliance.**
- **Meet sustainability goals through energy-efficient software and Green IT practices.**

Key takeaways from Finance signals 2025

- **Cybersecurity must be proactive.** → Security isn't just about penetration testing–it must be embedded in software from the start.
- **Software maintainability is a cost and innovation driver.** → High-quality software can save millions in maintenance costs while increasing innovation capacity by 30%.
- **Legacy systems slow innovation.** → Strategic modernization is key to balancing risk and opportunity.
- **The talent crisis is growing.** → Knowledge-sharing and upskilling must be prioritized to prevent "**knowledge monopolies**" and maintain operational resilience.
- **AI is powerful but fragile.** → Without strong engineering discipline, **AI can become a liability rather than an asset**.
- **Green IT is a business necessity.** → Reducing IT-related emissions isn't just about compliance–it cuts costs and improves efficiency.

The future belongs to FSI organizations that prioritize software quality

FSI organizations that take a structured, data-driven approach to software quality, security, and maintainability will lead the industry forward.

At Software Improvement Group (SIG), we help FSI organizations assess, benchmark, and optimize their software portfolios, ensuring they are built for security, scalability, and sustainability.

Want to see how your systems compare? Contact us today to take control of 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

ING

EUROPEAN CENTRAL BANK

a.s.r.

ABN·AMRO

Allianz

bank btpn

S&P Global

bdc

Stronger IT for finance

Turn digital transformation into your competitive advantage, become secure, reliable, and future-ready. Explore our financial services solutions here

Finance signals 2025

Software
Improvement
Group