Software Improvement Group

Why cybersecurity isn't just a final checkpoint

How software quality is your first line of defense in cybersecurity

Foreword

Why cybersecurity starts in your code

Many business leaders still treat cybersecurity as a separate concern, something to check off after development is complete. But with software at the heart of business operations, this approach carries inherent risks. Security gaps in code can lead to financial losses, compliance failures, and reputational damage–costs that go far beyond the IT department.

Relying on late-stage measures like penetration testing isn't enough. While useful, these tests often come too late in the development cycle. On average, systems contain 19 critical security findings, and 60% of systems have a low degree of security controls. Fixing these issues after deployment is not only more expensive but also more disruptive.

To reduce risk, organizations need to build security into every stage of the software lifecycle. That means combining code-level testing, managing third-party components, and improving overall build quality. It also requires a shift in mindset: treating secure, maintainable software as a business asset–not just a technical goal.

Why software security isn't just a final checkpoint

Key findings:

- 60% of systems are classified as having a low degree of security controls.
- The average system contains an estimated 19 critical security findings.
- Systems with above-average build quality are twice as likely to have high security-compliance.
- Industries with the best average security ratings: Financial Services, Energy, and the Public Sector.
- Smaller systems tend to be more secure than larger systems.
- Low-code and no-code still come with security risks.
- Quantum computing poses a long-term threat to encryption standards, requiring early awareness and preparation.

The need for a holistic cybersecurity approach

As software becomes more embedded in business operations, so do the risks – from financial losses and regulatory penalties to reputational damage and operational disruption.

Cyber threats are evolving fast, mirroring the pace of technology itself. According to Forrester, global cybercrime costs are projected to hit $12 trillion this year, while IBM reported that the average cost of a data breach stands at $4.88 million.

Yet many organizations still take a reactive approach. Security is treated as a final checkpoint, not a continuous priority. This mindset leaves systems exposed – and expensive to fix.

A common misconception persists: "We do penetration tests, so we're secure." While penetration testing (pentesting) is important, it typically happens late in the development lifecycle. By the time issues are discovered, the damage may already be done or require costly rework to resolve.

Organizations must adopt a proactive, Security by Design approach–embedding security measures throughout the software lifecycle rather than bolting them on at the end.

This shift is essential to reduce risk, minimize exposure, and build 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.

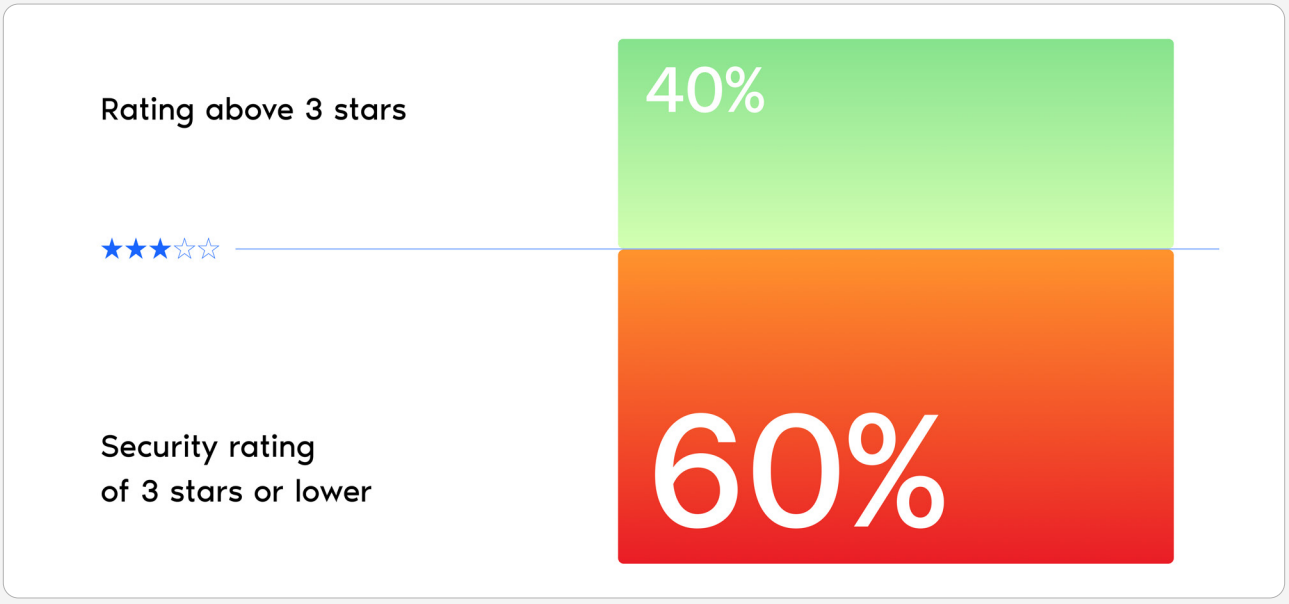
Three key methodologies in software security testing include:

• **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 enough on its own. Both SAST and SCA are complemented by penetration testing to form a complete security assessment. Together, these techniques enable earlier detection, stronger compliance, and more secure software from the start.

The majority of software systems are classified as having a low degree of security controls

Our data reveals that 60% of systems are classified as having a low degree of security controls, 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.

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 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.

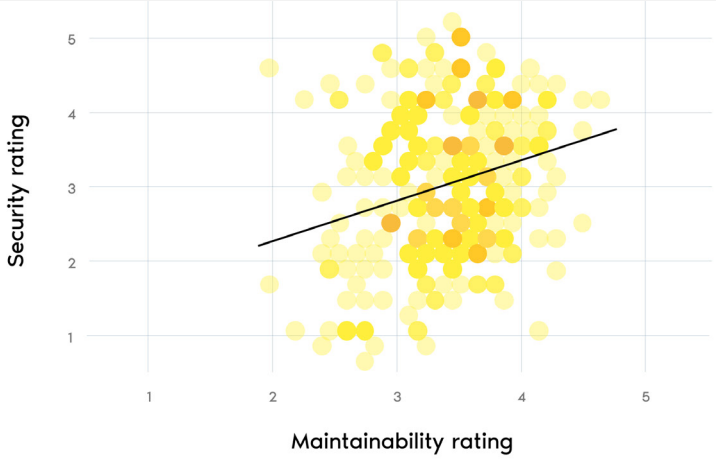
This number reflects an average per system, based on a typical-sized system in our benchmark. However, it's important to note that financial services institution (FSI) systems can be up to ten times larger than the average system in our benchmark. Generally, larger systems tend to have lower security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

Build quality and security go hand in hand

Our benchmark data shows that poor software quality strongly correlates with a higher number of security vulnerabilities. Systems that have an above-market-average build quality are twice as likely to have strong security compliance.



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 medio 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

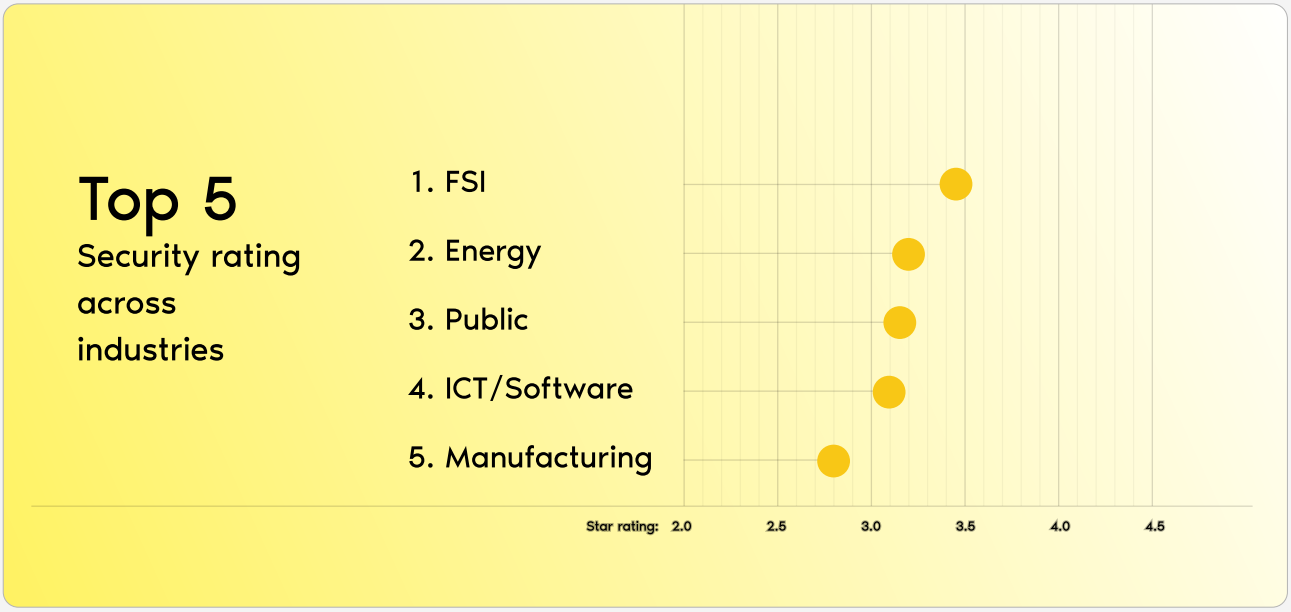
Founder & CEO at code4thought,

Avoiding a False Sense of Cybersecurity webinar

Security ratings vary widely by industry

Industries with the best average security ratings: Financial Services, Energy, and the Public Sector.

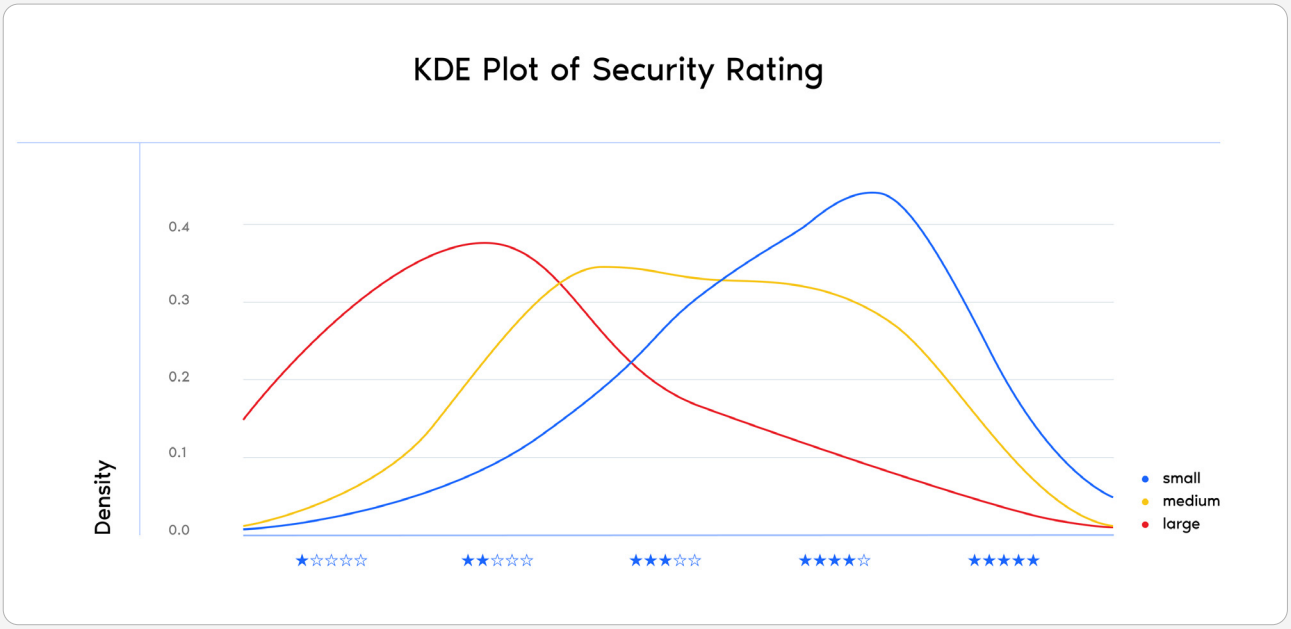
Good to note that there is still room for improvement as the best-performing scores typically fall between having a low and moderate degree of security controls. In addition, even the highest ratings won't guarantee complete security; it simply indicates that security considerations have been factored into the design and implementation, making vulnerabilities less likely.



This overview is based on our medio 2023 data snapshot, using SIG's 1-5 star SAST security model. The star ratings indicate compliance with OWASP Top 10 security controls, from 1 (severely low) to 5 (high). Note that industries with insufficient data were excluded, and even high ratings don't guarantee complete security; it simply indicates that security considerations have been factored into the design and implementation, making vulnerabilities less likely.

Larger systems tend to have weaker security

When we break down security ratings 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.

This reflects the complexity and fragmentation common in larger codebases, often the result of years of growth, legacy layers, and inconsistent security practices.

The open-source dilemma

Open-source software (OSS) usage is on the rise. According to the 2025 State of Open-Source Report, 58% of organizations increased their use of OSS over the past year. While OSS, no doubt, enables faster development, lower costs, and greater flexibility, it also introduces hidden risks if not properly managed.

Our earlier findings showed:

- **Each month, we see that 50% of enterprise software systems are vulnerable due to security issues in open-source libraries.**
- **30% of systems contain at least one critical vulnerable dependency.**

To manage this, organizations need regular Software Composition Analysis (SCA) which scans dependencies for vulnerabilities, licensing issues, and legal risks.

The low-code / no-code blind spot

Low-code and no-code platforms are reshaping how organizations build and ship software. Gartner estimates that 70% of applications will be built using low-code or no-code tools in 2025, up from less than 25% in 2020. These platforms promise faster development cycles, greater business agility, and improved collaboration between IT and business teams.

But while the benefits are clear, the security risks are still often overlooked.

For example, low-code environments can introduce:

- **Shadow IT from business users deploying apps without IT oversight.**
- **Unvetted integrations that bypass enterprise security controls.**
- **Inconsistent quality that's harder to secure using traditional methods.**
- **Over-permissioned apps that expose sensitive data to unauthorized users.**
- **Lack of auditing or monitoring, making incident detection and response harder.**
- **Identity flaws, like account impersonation, due to weak or missing role enforcement**

In short: Adopting low-code platforms may increase speed, but without proper guardrails, it may also come with increased risks.

To scale low-code/no-code adoption safely, organizations should:

- **Establish clear governance and approval frameworks to manage development across business units.**
- **Assess platform vendors for robust, built-in security features like role-based access, encryption, and secure defaults.**
- **Apply the same security principles to low-code platforms as to traditional software – focusing on authentication, authorization, monitoring, and configuration.**

Watch this space: Quantum computing and the future of security

Quantum computing may seem like a far-off risk, but it's closer than many think. Industry analysts and security leaders are increasingly concerned about what happens when quantum machines become powerful enough to break current encryption standards.

As Ted Shorter, CTO at Keyfactor, told CIO.com ***"CIOs should prepare their systems and data for the upcoming quantum computing threat"*** as early as 2025. Why? Attackers may already be harvesting encrypted data now to decrypt later, once quantum capabilities arrive.

The shift toward post-quantum encryption is already underway. The U.S. National Institute of Standards and Technology (NIST) is finalizing new quantum-resilient algorithms to replace those vulnerable to quantum attacks.

While most organizations aren't ready to make changes yet, now is the time to:

- **Take inventory of sensitive systems and data.**
- **Follow emerging encryption standards from NIST and other global bodies.**
- **Monitor quantum advancements as part of long-term tech strategy.**

Cybersecurity is a core part of business resilience

Cybersecurity is a core part of business resilience. It's not just about technical defenses but about integrating security into the fabric of the organization. A robust cybersecurity strategy should align with and support broader business objectives, ensuring that security measures enable, rather than hinder, growth and innovation. This involves fostering a security-aware culture throughout the organization, from the C-suite to entry-level employees.

Implementing a comprehensive cybersecurity framework like NIST or ISO 27001 can provide a structured approach to identifying and managing risks. Regular risk assessments, incident response planning, and business continuity exercises are crucial components of building cyber resilience. Additionally, organizations should consider cyber insurance as part of their risk management strategy to mitigate potential financial impacts of security incidents.

Cybersecurity is about a lot more than just firewalls and monitoring. It starts with writing secure, maintainable code. Organizations that take a Security-by-Design approach are better equipped to reduce risk, ensure compliance, and drive long-term business success.

Being better equipped means implementing layered testing strategies using SAST, SCA, and pentesting, improving build quality and maintainability to reduce vulnerability, and monitoring and updating open-source dependencies continuously.

Written by Software Improvement Group

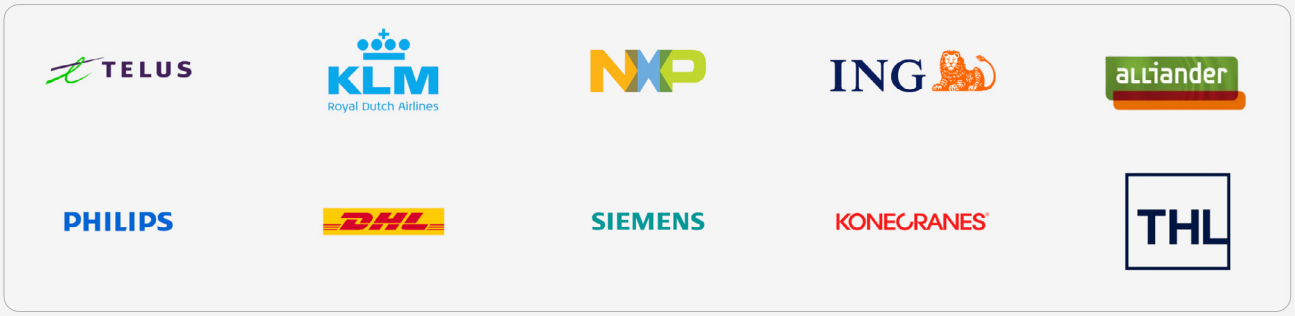
Software Improvement Group (SIG) leads in traditional and AI software quality assurance. Empowering organizations to become more resilient and agile by guiding them to enhance their software quality and security through deep source code analysis and tailored, strategic advice.

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



This is an excerpt of our State of Software 2025 report. This report delivers critical insights on the state of software quality in 2025 so that CIOs, CTOs, and technology leaders can make informed and strategic decisions. For more insights, download the full report.

Read the full report