SECURITY BY DESIGN

THE KLARRIO SECURITY FRAMEWORK: MOVING BEYOND COMPLIANCE

Klarrio
STREAMING AHEAD

TABLE OF CONTENTS

01

OUR CONTEXT

At Klarrio, we design custom, cloud-native, and cloud-agnostic software solutions that empower our customers to take control of their data, optimize performance, and manage cloud costs. We firmly believe that every organization should control its own destiny by maintaining custody of its data, software, and core intellectual property.

This paper is part of a series exploring our foundational beliefs and capabilities. Here, we outline our approach to security by design, detailing what you can expect when you partner with us. It complements our Manifesto and History documents. In a future installment of the series, we will present a technical architecture vision that further highlights our core beliefs on cloud-native software development.

"Regulatory compliance should be the result of robust security practices, not the reason for them."

02

INTRODUCTION

In today's digital economy, technology-driven companies are building increasingly complex platforms to meet customer expectations. To accelerate innovation and keep pace with business demands, these platforms often rely heavily on third-party and open-source components, from Kubernetes to the vast CNCF[1] ecosystems. In fact, roughly 70-90% of all company codebases today now include open-source[2].

While the open nature of these ecosystems offers significant benefits—primarily through transparency and collaborative security—their inherent openness also increases the potential for unforeseen attacks. This is because, while providing great value to the platform, they also have the potential to introduce additional vulnerabilities.
At the same time, the rise of "as-a-service" cybercrime platforms and AI-powered tools, like deepfakes for phishing and automated hacking tools, are lowering the bar for attackers. As a result, cybersecurity is no longer merely a technical issue; it's a core business threat. The economic stakes are immense. Global annual cybercrime costs are projected to exceed **$1.2 trillion by the end of 2025**[3], a significant threat to the world economy. Add to this the growing geopolitical risks from nation-state actors and the urgency is even more dire.
In response, global legislators are taking action. The EU's NIS2 Directive, Cyber Resilience Act, and similar regulations worldwide are mandating that companies take proactive measures to ensure their products are secure by design and remain protected throughout their intended lifespan. The sheer volume of these rules, however, has left many companies confused about where to even begin.

While these regulations aim to improve resilience, however, **treating compliance as the end goal in and of itself can be dangerously misleading**. In fact, checkbox compliance often creates a false sense of security, leaving critical risks unaddressed.

At Klarrio, we believe **regulatory compliance should be the result of robust security practices, not the primary reason for them**. Our approach focuses on risk-based security, where priorities are driven by threats that matter most to your business, not just by the items on a predetermined checklist.

What follows is an overview of how we embed security into the core of our solutions.

1 Cloud Native Computing Foundation

2 Census III of Free and Open Source Software, Blackduck 2025 Open Source Security and Risk Analysis Report

3 Source: Cyber Defense Magazine

03

SIX PILLARS OF SECURE SOFTWARE SOLUTIONS

Our approach is built on six foundational principles to turn security into a business enabler.

01. First, we start with Proactive Risk Identification, using threat modeling to prioritize threats that matter to your business.

02. We then focus on Securing Your Software Supply Chain by meticulously vetting open-source components and hardening the build process itself.

03. Since software is never truly finished, we embrace Continuous Life Cycle Management to protect against emerging threats.

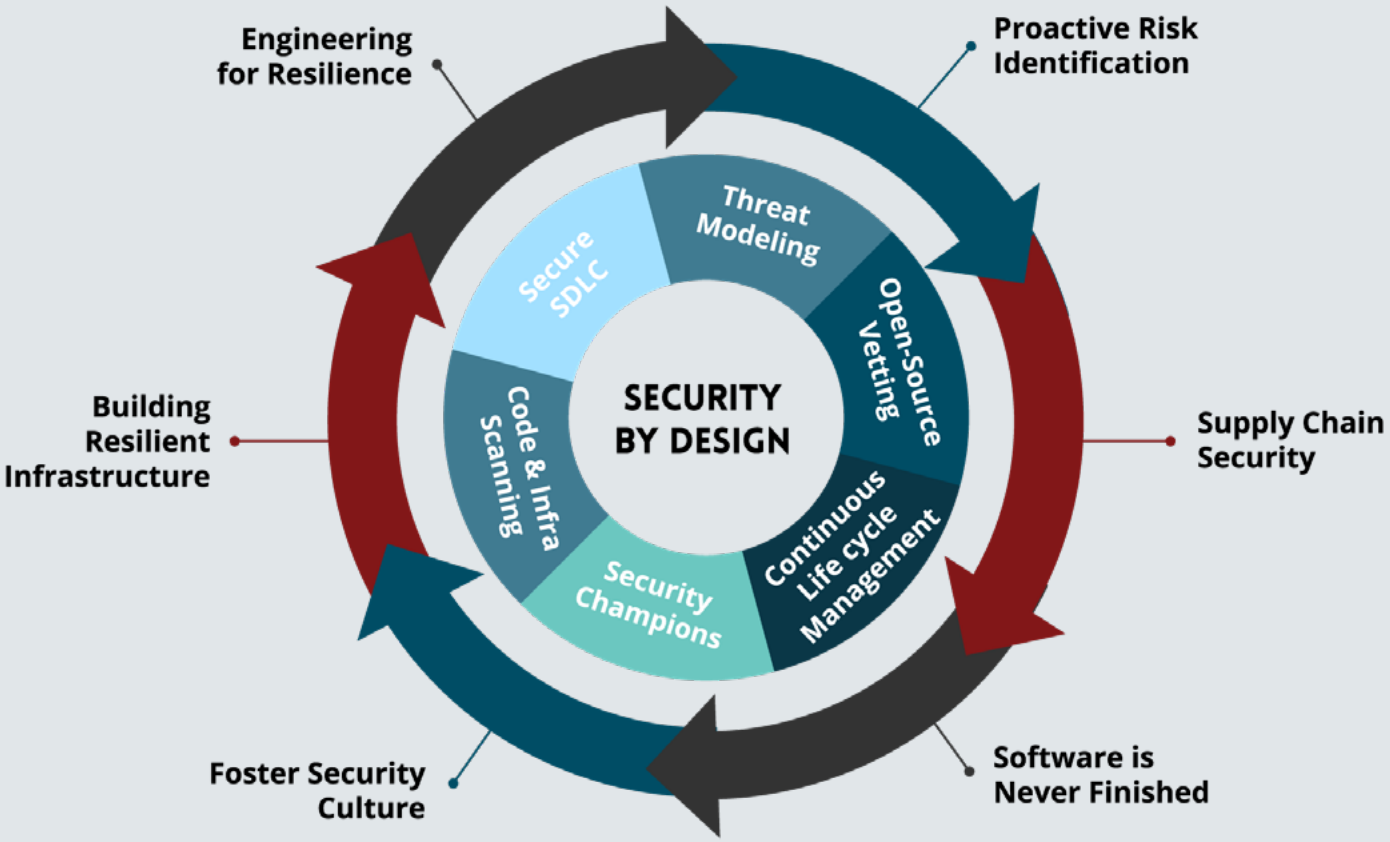
04. We also recognize that people are our greatest asset, so we actively foster a strong Security Culture through training and our Security Champions program.

05. In addition, our approach focuses on Building a Resilient Infrastructure by implementing Zero Trust architecture[4] and advocating for strategic independence from hyperscalers.

06. Finally, we establish a Secure Software Development Life Cycle (SSDLC) to measure, improve, and adapt our security posture over time.

---

4 A Zero Trust model is a strategic approach that eliminates implicit trust in a network, protecting against both external threats and insider risks by requiring strict verification at every access point.



The Klarrio Security by Design Framework.
Read on to learn how these principles can build long-term business resilience.

04

TANGIBLE BENEFITS, TANGIBLE RESULTS

We advocate a **Security by Design** approach. **Security by Design** isn't just a slogan. It describes a clear framework for embedding security considerations from the very beginning of the software development process, rather than retrofitting them after deployment. In practice, this shift-left[5] philosophy ensures:

- **Early risk mitigation** to address vulnerabilities before they become costly incidents.
- **Regulatory alignment** whereby compliance is a byproduct, not a goal.
- **Operational resilience**, which reduces downtime and stronger business continuity.
- **Cost efficiency,** because preventing issues is far cheaper than fixing them post-release.
- **Continuous improvement**— measuring, identifying, and improving our security posture.

By shifting our focus from remediation to prevention, we turn security into a core business strength, rather than an isolated technical function. As such, **Security by Design** is a foundation for sustainable business growth, and our approach focuses on prioritizing investments where they matter most.

For Klarrio, **Security by Design** isn't static. It evolves along with the threat landscape, adapting to new threats as they emerge, and we've made this ongoing improvement process a core part of how we build our technology.

5 Shifting left moves security testing and practices earlier into the software development life cycle, reducing the risk of expensive delays and potential breaches by finding and resolving issues earlier.

05

THE KLARRIO SECURITY BY DESIGN FRAMEWORK

Our framework is built on a simple, yet powerful principle: you cannot secure what you do not understand. Therefore, the first and most critical step is to assess and know your risks. We have encapsulated the process into six clearly defined principles, all which can either stand alone or build upon each other.

"You cannot secure what you do not understand."

THE FIRST PRINCIPLE: PROACTIVE RISK IDENTIFICATION

In today's complex threat landscape, a one-size-fits-all approach to security is a recipe for wasted resources and unmitigated risk. To make sound business decisions, you must be able to identify and prioritize the threats that matter most to your organization.

We achieve this through **threat modeling**, a structured process that takes place early in the design phase of every new feature or solution. For every significant feature or integration, we bring the development team together, guided by our security experts to model how data flows through the system and where vulnerabilities could emerge. We use established frameworks like STRIDE[6] to identify threats and the OWASP Risk Rating to quantify their potential impact. This process isn't just about finding vulnerabilities; it's about building a shared understanding of the system's design and creating a framework for informed decision-making.

6 STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Escalation of Privilege (a threat modeling framework)

Threats are then quantified into risks, allowing us to decide for each of them whether to mitigate, transfer, or accept them accordingly, which gives rise to a number of critical questions and considerations.

- **Which risks do we mitigate** through fixing or elimination?
- **Which risks can we transfer**, such as through cybersecurity insurance against financial losses?
- **Which risks are safe to accept?**

The answers to these questions (and oftentimes more) are not universal. Instead, they are guided by two key business factors:

1. your organization's **risk tolerance** (the amount of risk you're willing to accept to pursue added business value) and

2. the **risk profile** of the specific application. By aligning our security work with these factors, we ensure that every investment and mitigation directly supports your strategic business goals.

The insights gained from this process aren't one-off solutions. We capture them as secure-by-default architectural requirements and best practices, embedding them into all future solutions we build. This continuous feedback loop ensures that our security posture improves with every project.

THE SECOND PRINCIPLE: SECURING YOUR SOFTWARE SUPPLY CHAIN

One of the most significant threats we and our customers face is a compromised software supply chain, particularly from the open-source components used to build our platforms. Attackers are increasingly targeting these open-source components, knowing that a single vulnerability can provide a backdoor into countless applications and entire cloud environments.

This has led to high-profile incidents in open-source software like the xz package backdoor. Attacks like the xz backdoor show just how far attackers will go: spending three years posing as a legitimate open-source contributor, patiently taking tasks, gaining trust, and then using that position to plant malicious code at the heart of the software supply chain. These supply chain compromises also occur in proprietary software, as seen with the SolarWinds incident, making it clear that supply chain security is a global, mission-critical challenge for everyone.

At Klarrio, we believe open-source offers unparalleled flexibility and innovation. However, safely leveraging it requires a rigorous, continuous process. Two core pillars in particular, **meticulous open-source vetting** and **securing the build process**, merit additional explanation.

METICULOUS OPEN-SOURCE VETTING

We are committed to building custom, cloud-agnostic solutions that help our customers reclaim full control of their systems. This means we are highly selective about every open-source component we recommend and integrate.

Our due diligence goes far beyond a routine license check. It includes a comprehensive security audit to verify authenticity, dependencies, and community security practices. By rigorously evaluating components before they ever enter your platform, we proactively guard against malicious code and reduce your exposure to risk.

SECURING THE BUILD PROCESS

To protect against sophisticated supply chain attacks, it's essential to **secure the entire software build process**. An attacker who compromises your automated CI/CD pipeline can inject malicious code, creating a significant backdoor into your applications before they are even deployed.

A key defense is to cryptographically sign the artifacts produced by the build, such as container images, to ensure their integrity and origin. Frameworks like the Supply-chain Levels for Software Artifacts (SLSA) provide a structured approach to systematically strengthen these processes, giving Klarrio and our customers confidence in the software we deliver.

ADDRESSING THE RISKS OF AI

The rise of artificial intelligence presents new challenges to software supply chain security. Developers using AI-assisted coding tools risk inadvertently introducing security vulnerabilities into their projects by not fully understanding the AI-generated code. They also risk unintentionally leaking sensitive intellectual property by allowing AI companies to use their inputs for model training. These risks are compounded by AI-assisted attackers who leverage Large Language Models (LLMs) to generate and distribute thousands of malicious modules, as we documented in our own research[7] on a large-scale malware network on GitHub.

At Klarrio, we approach AI-assisted coding with caution. We thoroughly evaluate its potential benefits and pitfalls before adopting it on any customer projects, ensuring we maintain the highest standards of security and integrity in our solutions.

7 https://klarrio.com/klarrio-discovers-large-scale-malware-network-on-github/

THE THIRD PRINCIPLE: SOFTWARE IS NEVER FINISHED

Modern software is never truly 'finished'. The moment an application is deployed, it enters a dynamic and challenging environment where new threats and vulnerabilities constantly emerge. This reality makes continuous maintenance not just an option, but a fundamental requirement for security. A platform that is secure today may be vulnerable tomorrow, requiring an ongoing, proactive approach to monitoring and management throughout its entire life cycle.

"Modern software is never truly finished."

CONTINUOUS LIFE CYCLE MANAGEMENT

Vulnerabilities are discovered every day, and a secure platform requires a timely, proactive response. To defend against this, we create a detailed **Software Bill of Materials (SBOM)** for every application. This is more than just a list; it's an inventory that provides a record of every component in your software.

With a clear SBOM, we can:

- Quickly identify which applications are affected when a new vulnerability is discovered.
- Automate the process of continuously monitoring new security risks.
- Ensure that patched versions are deployed swiftly and with a clear process, protecting your business from emerging threats.

Our goal is not just to build a secure platform, but to ensure its resilience. By carefully selecting our building blocks and continuously monitoring them, we protect your applications, infrastructure, and your customers from a rapidly evolving threat landscape.

THE FOURTH PRINCIPLE: FOSTERING A SECURITY CULTURE

While processes and tools are essential, the most significant security challenge is a human one. The reality is that most developers and architects are not security experts; yet, they are responsible for building increasingly complex systems. A lack of security awareness can lead to critical misconfigurations, oversights and logic error—each a potential entry point for attackers that could lead to data exposure, privilege escalation, or full-system compromise.

The solution is not simply to hire more security experts, but to scale the expertise across the entire organization. **Security culture is built through both top-down leadership and bottom-up empowerment.** One without the other fails. Executive mandates without developer buy-in stall at the policy level, while grassroots enthusiasm without leadership support runs out of resources.

KLARRIO'S SECURITY CHAMPIONS PROGRAM

At Klarrio, our security culture is anchored by our Security Champions Program. These champions are passionate, embedded security representatives within each development team. They act as a vital bridge between their teams and our core security function, serving as the first point of contact for security questions, in addition to promoting best practices. This program ensures that security is not a separate discipline, but an integral part of day-to-day development, empowering teams to take ownership of their own security responsibilities.

TRAINING AND AWARENESS

An effective culture is built on knowledge. That's why we invest heavily in continuous training and awareness for all personnel involved in the software life cycle. This training is not generic; it's technology- and role-specific, ensuring our teams have the precise knowledge they need to build secure solutions. For example, in 2025 our developers received in-depth training on OAuth2 and OpenID, key technologies used widely across the internet and enterprise applications, while our champions and senior engineers participated in intensive threat-modeling workshops. This investment gives our teams the skills to proactively identify and mitigate risks, turning a potential weakness into a core strength.

This commitment to knowledge transfer extends directly to our customers. By embedding their own developers and architects within our teams we ensure a continuous, hands-on transfer of knowledge throughout the project life cycle. Through co-creating with our engineers, your teams will gain a deeper understanding of the product, from its core technology and design to its crucial security aspects. Additionally, we offer customized training through our academy, tutorrio.

"Security culture is built through both top-down leadership and bottom-up empowerment."

THE FIFTH PRINCIPLE: BUILDING A RESILIENT INFRASTRUCTURE

Attackers can exploit vulnerabilities not only in applications but also in the cloud infrastructure itself. Misconfigured access rights or unpatched infrastructure code are example issues that can grant attackers control of entire clusters. To defend against these attacks, we secure both applications and Infrastructure as Code[8] (IaC).

VULNERABILITY MANAGEMENT: FROM CODE TO INFRASTRUCTURE

In the age of Infrastructure as Code, vulnerabilities aren't limited to application logic; they are embedded in the very definition of your cloud environment. We implement a holistic vulnerability management program that "shifts left" to detect misconfigurations before deployment, saving time and reducing exposure:

- **Proactive Scanning:** We continuously scan for vulnerabilities in both applications and the IaC that define our platforms. This automated process ensures that risks are identified and addressed before they ever reach a production environment.
- **Shared Responsibility:** We extend the standard shared responsibility model to forge a true partnership with our customers. By working together to manage and patch vulnerabilities, we ensure our mutual success in a dynamic threat landscape.

8 Infrastructure as Code (IaC) is a modern approach that uses code, scripts, and configuration files to automatically build and manage IT infrastructure, moving away from manual and error-prone processes.

ZERO TRUST ARCHITECTURE

A cornerstone of our security philosophy is the **Zero Trust model**. We operate on the principle of "never trust, always verify," which assumes no user, device, or network is inherently trustworthy, regardless of its location. By implementing granular controls and strict verification, we contain a potential breach and significantly limit the "blast radius" of any compromised system. This approach provides a powerful defense against both external threats and internal misuse, safeguarding your data and operations.

STRATEGIC INDEPENDENCE AND DATA SOVEREIGNTY

An often-overlooked aspect of infrastructure security is the ability to trust your cloud provider. We actively advocate for **owning your data and remaining cloud agnostic**. This is a strategic choice that protects you from geopolitical risks, regulatory changes, and vendor lock-in.

As two of our core beliefs, cloud agnosticism and data sovereignty merit a dedicated document. The Klarrio Manifesto[9] clarifies our core beliefs, our history, our points of difference, and how we help clients take back—and keep—control of their data.

Several European providers like Exoscale, Hetzner, and OVH already offer strong foundational cloud services such as networking, server capacity, and storage. With significant compute power and a deep pool of technical talent across Europe, it's entirely possible to build comprehensive products without depending on US hyperscalers.

By leveraging these resources and focusing on open-source, cloud-agnostic architectures, we can move beyond the current US-centric dominance of essential cloud services and, at the same time, also grow the European cloud-provider alternatives.

9 Access the Klarrio Manifesto

THE SIXTH PRINCIPLE: ENGINEERING FOR RESILIENCE

In a shifting threat environment, resilience isn't a product feature: it's a capability built into the way you work.

Our **Secure Software Development Life Cycle (SSDLC)** embeds security at every stage, from concept to deployment, and is designed for continuous improvement. This process forms the very backbone of a successful application security program.

MEASURE, IMPROVE, AND ADAPT

Any effective program of continuous improvement is built on a cycle of measuring, identifying, and improving. We use the OWASP SAMM maturity model to provide clear, actionable metrics on our SSDLC process. These metrics give us strategic insights into the effectiveness of our security program, allowing us to:

- **Identify areas for enhancement** and build a security improvement roadmap.
- **Align security investments** directly with your organization's growth goals.
- **Measure adherence to policies** and regulatory requirements, such as ISO 27001 and RVIT[10] to ensure you meet your compliance needs while fostering genuine security.

This ensures our security posture isn't static but dynamically adapts to new threats and business needs, empowering long-term protection and stability.

10 RVIT: Regeling veiligheid en integriteit telecommunicatie (Dutch cyber security legislation)

07

CONCLUSION

Ultimately, true security isn't just about the technology you build. It's about the mindset and processes that guide your business. By adopting the Klarrio Security Framework, you're not just addressing a technical problem—you're transforming security from a compliance burden into a competitive advantage and a foundation for sustainable growth.

We are ready to partner with you to embed these principles, not only building secure software, but a resilient business model fully prepared for the threats of tomorrow.

ANNEX

ACRONYMS

- **CNCF:** Cloud Native Computing Foundation
- **CI/CD:** Continuous Integration / Continuous Delivery
- **IaC:** Infrastructure as Code
- **NIS2:** Network and Information Systems Directive 2
- **CRA:** Cyber Resilience Act
- **OWASP:** Open Worldwide Application Security Project
- **SBOM:** Software Bill of Materials
- **SSDLC:** Secure Software Development Life Cycle
- **SLSA:** Supply-Chain Levels for Software Artifacts
- **STRIDE:** Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Escalation of Privilege (a threat-modeling framework)
- **LLM:** Large Language Model, e.g. ChatGPT
- **ISO/IEC 27001:** Information security standard
- **RVIT:** Regeling veiligheid en integriteit telecommunicatie (Dutch cyber security legislation)

HYPERLINKS

To ensure all referenced resources are accessible in both digital and print formats, the following is a list of hyperlinks mentioned in this document.

- **Klarrio Manifesto:** https://klarrio.com/manifesto
- **tutorrio:** https://tutorrio.com
- **Klarrio Discovers Large-Scale Malware Network on GitHub:** https://klarrio.com/klarrio-discovers-large-scale-malware-network-on-github
- **Cloud Native Computing Foundation:** https://www.cncf.io
- **Blackduck 2025 Open Source Security and Risk Analysis Report:** https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf
- **Cost of cybercrime: Cyber Defense Magazine:** https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/
- **XZ Package Backdoor:** https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2024/xz.md
- **SolarWinds Incident:** https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2020/solarwinds.md
- **OAuth2:** https://en.wikipedia.org/wiki/OAuth
- **OpenID:** https://en.wikipedia.org/wiki/OpenID
- **STRIDE Framework:** https://en.wikipedia.org/wiki/STRIDE_model
- **OWASP Risk Rating:** https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
- **SLSA Framework:** https://slsa.dev
- **OWASP SAMM:** https://owaspsamm.org
- **ISO/IEC 27001:** https://klarrio.com/iso-certification
- **RVIT:** https://wetten.overheid.nl/BWBR0045665/2021-10-06

ABOUT THE AUTHOR

Joris Gorinsek - Staff Security Architect at Klarrio

Joris is an expert in developing secure software and platforms. At Klarrio, he runs the security champions program and coaches our development teams while building secure and resilient systems. In his previous job, as AppSec Security Lead, he guided the company in navigating the complexity of cybersecurity legislation for IoT device manufacturers.

Method of contact: info@klarrio.com

This document is edited by Klarrio.

For any questions or suggestions, please contact: info@klarrio.com

CONTACT US

- BELGIUM
- NETHERLANDS
- GERMANY
- SPAIN
- UNITED STATES

info@klarrio.com

www.klarrio.com

Klarrio specializes in large-scale and real-time data processing implementations. We offer deep expertise in cloud-native and hybrid solutions. But more importantly, we have the experience you need to understand where you've been, where you are today, and how best to achieve your goals going forward.

We're much more than a software solutions provider. Klarrio offers proactive and sustainable open source innovations with no vendor lock-in, all while working as a trusted partner who ensures you always remain in complete control of your own data.

Control your destiny. Contact us today.

linkedin.com/company/klarrio

klarrio.medium.com

Klarrio
STREAMING AHEAD