

# Sprita iT

**Development – Embedding Security Across SDLC to Improve Quality, Reduce Costs, and Enable Risk-Based Decisions**

## Introduction: Software as a Cross-Industry Driver

Software has become the backbone of nearly every industry, including finance, healthcare, retail, manufacturing, telecommunications, and beyond. From mission-critical enterprise applications to customer-facing platforms, code now sustains competitiveness and innovation. However, vulnerabilities introduced during early stages, reliance on third-party dependencies, accelerated delivery cycles, and rising regulatory pressures all create risks. Organizations must embed security and quality from design without slowing down innovation.

## Common Challenges in Software Development

Industries face similar issues regardless of sector:

- Pressure to deliver faster with Agile and DevOps practices.
- Heavy reliance on open-source and third-party components.
- Risks in maintaining legacy systems with limited visibility.
- Lack of clear metrics and Service Level Agreements (SLAs) for software quality and security.
- Exposure to regulatory requirements such as GDPR, HIPAA, PCI DSS, ISO 27001, or NIST.

These challenges highlight the need for integrated, proactive security embedded in the SDLC.

## Our Solutions: Integrating Security, Quality, and Governance Across the SDLC

We help organizations in all industries integrate security, quality, and risk governance into software development through a comprehensive approach:

Security by Design:

- 1) Early identification of vulnerabilities in source code.
  - Alignment with international standards such as OWASP Top 10 and CWE.
  - Transparent reporting that enables developers to remediate issues before they reach production.
- 2) Dependency and Third-Party Component Management:
  - Continuous evaluation of libraries and frameworks.
  - Detection of known vulnerabilities (CVEs) and licensing risks.
  - Real-time alerts to keep applications updated and secure.
- 3) Software Supply Chain Protection:
  - Continuous monitoring of CI/CD pipelines.
  - Integrity validation for every release.
  - Traceable evidence to support audits and certifications.
- 4) SLA Definition and Metrics:
  - Support in defining security-focused SLAs.
  - Dashboards and KPIs for continuous compliance monitoring.
  - Prioritization of risks for efficient resource allocation.
- 5) Risk Evaluation for New and Legacy Systems:
  - Structured methodology to assess risks before adopting new systems.
  - Identification of vulnerabilities in legacy applications.
  - Secure modernization without disrupting operations.

## Strategic Advantages for CISOs, CIOs, and CTOs

By adopting our solutions, organizations gain clear advantages:

- **Quality Improvement:** More resilient and reliable software.
- **Cost Reduction:** Early remediation reduces support and maintenance costs.
- **Simplified Compliance:** Evidence and reports aligned with major regulatory frameworks.
- **Faster Delivery:** Secure DevOps practices that do not slow innovation.
- **Customer and User Trust:** Applications that reinforce corporate reputation.

## Cross-Industry Use Cases

- **Finance & Insurance:** Securing banking platforms and fraud prevention.
- **Healthcare:** Protecting EHRs and telemedicine platforms under HIPAA/GDPR.
- **Retail & eCommerce:** Reducing breaches in web portals and mobile apps.
- **Telecommunications:** Protecting infrastructure and digital services from supply chain risks.
- **Manufacturing & Industry 4.0:** Securing IoT platforms and industrial applications.

## Looking Ahead: Security as an Innovation Accelerator

Security and quality are not obstacles but enablers of digital transformation. Our solutions allow organizations not only to comply with regulations but also to innovate with confidence—launching products faster, modernizing systems securely, and strengthening customer experience with reliable and secure applications.

## Benefits Overview

Benefit	Description
Quality Improvement	Secure design and early vulnerability detection improve overall software quality.
Cost Reduction	Reduced remediation costs through early fixes and proactive monitoring.
SLA Definition	Support in defining and enforcing security-driven SLAs across teams.
Risk Evaluation	Assessment of risks when adopting new systems or maintaining legacy applications.
Innovation Enablement	Security as a driver for safe and faster digital transformation.

## Sprita iT: Security by Design, Innovation with Confidence.

At Sprita iT, we help organizations across all industries turn software security and quality into a strategic advantage. By embedding protection, governance, and risk management throughout the entire software development lifecycle, we enable CISOs, CIOs, and CTOs to improve resilience, reduce costs, and accelerate digital transformation without compromising compliance or innovation.

Our solutions transform security from a regulatory obligation into a catalyst for growth—strengthening trust, ensuring operational continuity, and empowering enterprises to innovate with confidence in today’s demanding digital economy.