

SPARTA

SPARTA is an assessment framework for evaluating an organization's security, privacy, assurance, and risk posture.



What it is

SPARTA — Security, Privacy, Assurance, and Risk Trust Assessment is a comprehensive assessment framework that supports organizations in evaluating and enhancing their cybersecurity posture, privacy protections, and risk management practices. This framework provides a structured approach for identifying gaps and establishing safeguards to address security threats and regulatory requirements.

Developed and maintained by industry experts and regulatory authorities, SPARTA is utilized by compliance teams, risk managers, and IT security professionals across various sectors. Its scope encompasses cybersecurity controls, privacy governance, assurance processes, and risk assessment activities, allowing organizations to address regulatory compliance and operational resilience alongside standard frameworks like ISO 27001 and NIST SP 800-53.

At a glance

PUBLISHER SPARTA is an EU-funded cybersecurity research and innovation project under Horizon 2020, hosted via the SPARTA project's official website (sparta.eu), and coordinated by CEA (French Alternative Energies and Atomic Energy Commission)(sparta.eu) (https://www.sparta.eu/assets/deliverables/SPARTA-D12.3-Updated-dissemination-and-communication-plan-and-evaluation-PU-M12.pdf?utm_source=openai). CEA (Coordinator)	TYPE Assessment / Maturity Model	VERSION 2017 (with 2022 revised Points of Focus)
EFFECTIVE March 2023	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Very High

Source: <https://sparta.distrinet-research.be/>

Why it matters

- **Strengthen comprehensive risk governance** Establish consistent structures for managing security, privacy, and assurance across complex organizational environments.
- **Enhance regulatory compliance** Support adherence to diverse legal and regulatory requirements, enabling organizations to demonstrate conformance with applicable standards and obligations.
- **Improve data protection practices** Implement structured controls for protection and privacy, reducing unauthorized access and promoting data confidentiality across systems.
- **Increase audit readiness** Facilitate ongoing compliance monitoring and documentation to support efficient internal and

How SmartSuite supports SPARTA

SPARTA Assessment Library

Organize SPARTA questionnaire domains and questions to standardize vendor security and privacy evaluations.

Vendor Response and Evidence Management

Collect supplier responses, documentation, and validation evidence in a centralized assessment repository.

Vendor Risk Scoring and Prioritization

Evaluate supplier security posture and prioritize remediation based on risk exposure and business impact.

Vendor Corrective Action Tracking

Track corrective actions for vendor findings and monitor remediation progress through completion.

Recurring Vendor Assessment Schedule

Schedule recurring vendor assessments and monitor evolving third-party risk posture.

Vendor Risk Reporting Dashboard

Provide dashboards summarizing vendor risk ratings, assessment results, and outstanding remediation tasks.

Common framework mappings

COBIT 2019

GDPR

HIPAA

ISO 27001:2022

ISO 27701

NIST CSF 2.0

NIST Privacy Framework v1.0

NIST 800-53 Rev.5

SOC 2

Official resources

SPARTA Framework Overview

Provides an overview of the Security, Privacy, Assurance, and Risk Trust Assessment framework.
sparta.eu/index.html

SPARTA Security and Privacy Guidelines

Outlines guidelines for implementing security and privacy measures within the SPARTA framework.
sparta.eu/security-privacy.html

Frequently asked questions

What is SPARTA used for?

SPARTA is a unified framework designed to help organizations assess and manage their security, privacy, assurance, and risk posture. It provides structured methodologies and criteria for evaluating controls and ensuring that risks are identified, mitigated, and monitored effectively.

Is SPARTA required or certifiable?

SPARTA is not a regulatory mandate but serves as a self-assessment or third-party assessment standard. It is not certifiable in the traditional sense like ISO 27001, but organizations can use it to demonstrate due diligence and maturity in their risk management and compliance programs.

What is the scope of SPARTA and who should use it?

SPARTA is applicable to organizations of all sizes and industries seeking to align their security, privacy, assurance, and risk management practices. Its modular structure allows tailoring the scope to cover specific domains, including information security, data privacy, operational resilience, and regulatory compliance.

What are the key concepts or artifacts in SPARTA?

Core artifacts within SPARTA include risk registers, control self-assessments, privacy impact assessments, assurance reports, and evidence logs. These documents support the ongoing evaluation and improvement of controls across multiple compliance domains.

How do organizations implement SPARTA in practice?

Implementation of SPARTA involves mapping organizational risks to defined controls, conducting gap analyses, documenting evidence, and regularly reviewing control effectiveness. Organizations typically perform periodic assessments and integrate SPARTA principles into existing governance, risk, and compliance programs.
SPARTA is a registered trademark of SmartSuite Inc. All rights reserved.

How does SPARTA relate to other frameworks such as NIST, ISO, or SOC 2?

SPARTA is designed as an integrative layer, mapping to requirements and controls from established frameworks like NIST CSF, ISO 27001, and SOC 2. It provides a holistic view by consolidating requirements, streamlining assessments, and reducing duplication across different standards.

What are the ongoing compliance requirements for SPARTA?

Maintaining SPARTA alignment requires periodic risk assessments, continuous monitoring of controls, regular updates to documentation, and prompt remediation of identified issues. Ongoing evidence collection and management ensure that organizations remain audit-ready and can demonstrate control effectiveness over time.

How would SmartSuite support SPARTA?

SmartSuite facilitates SPARTA management by centralizing risk tracking, control documentation, and collection of evidence within a unified workspace. It enables automated workflows, reporting, and dashboards for audit readiness, ensuring that compliance teams can monitor, update, and demonstrate adherence to SPARTA requirements efficiently.

License included / downloadable: Yes. The SPARTA framework is published by the SPARTA consortium (EU H2020) and is publicly available from the project's website and publications. License included with platform Framework text is licensed by its publisher and is included only where stated above.

Full framework page and mappings: smartsuite.com/frameworks/sparta-security-privacy-assurance-and-risk-trust-assessment