Best practices for meeting security compliance standards

Businesses today are constantly looking for ways to build trust and loyalty with customers. For many companies, from early-stage startups to multinational corporations, winning that trust starts by demonstrating that you have the correct security controls in place. This is why businesses are expected (and in some cases required) to pursue and meet internationally-recognized compliance standards (for example, ISO 27001, PCI DSS, and SOC 2).

This cheat sheet provides guidance on getting started with your compliance program and information about controls that align with specific compliance standards.

01 Identify your requirements

"Compliance" is the set of requirements you need to meet to satisfy established regulatory or corporate standards. Your specific requirements, and the framework you put in place to verify compliance with them, will depend on your industry and the type of data you collect and store. Different frameworks exist for meeting different compliance requirements.

Many security frameworks are based on protecting three main attributes of data security: **confidentiality, integrity, and availability**. These three attributes, referred to as the "CIA Triad," are key to ensuring that your data security practices meet compliance standards. Several security frameworks, although they apply to different industries, share some of the same requirements for satisfying these three attributes. For example, both SOC 2 and PCI compliance address the issue of restricting personnel access to data.

02 Do a gap analysis

With your specific requirements and a security framework in mind, the next step is to do a gap analysis: an assessment of the current state of your organization's security program vs. where you want to be. The gap compliance analysis measures your company's existing assets, procedures, and policies against the security requirements you need to meet and the framework you'll build to do it. Start this analysis by identifying all of the assets, tools, processes, and policies that dictate your existing detection and security controls. Then consider how you would respond to and recover from an incident. With these details, you can assess risks and identify the gaps in your organization's current security program. The results of the assessment should help you set a baseline of controls to use for reference when you're ready to enforce new compliance standards.

03 Set controls

"Controls" are the specific steps or procedures you use to meet a set of compliance requirements. Many controls are shared across security frameworks. No single tool or policy can meet the needs of all of an organization's controls, and some controls require more than one tool or policy to solve. After you identify the requirements your business has to meet, you can start defining your controls. Many resources are publicly available to help you draw a map between the compliance requirements you need to meet and the controls that satisfy those requirements. (For an example, see the Secure Controls Framework.)

Your system of internal controls will be unique to your organization depending on your compliance requirements. Having the right set of controls in place will make it much easier to manage and maintain compliance standards for your organization.

04 Be aware of the changing cybersecurity landscape

Compliance standards change over time. The PCI Security Standards Council released an updated version of the PCI Data Security Standard in March 2022. The criteria for SOC 2 compliance, set by the American Institute of Certified Public Accountants, was last updated in January 2018. And the International Organization for Standardization released a new iteration of ISO compliance standards in February 2022 (with an update expected in October 2022).

As compliance standards evolve, your policies for meeting those standards should also evolve. Remember that a plan for compliance should be dynamic and up-to-date.

Best practices for meeting security compliance standards

Compliance auditors want to see evidence of risk management in your SDLC. The following Snyk features help you establish controls for meeting SOC 2, ISO, and PCI compliance requirements.

01

SOC 2

Vulnerability management controls within SOC 2 require reporting, validation, identification, scoring, prioritization, and radiation tracking. Snyk can help you address the following SOC 2 control requirements:

- Control CC2.1 - Snyk offers reports of vulnerabilities across the entire platform and validates specific logging in Snyk Cloud.
- Control CC3.2 - Snyk identifies, scores, prioritizes, and remediates — and trains developers on — identified code vulnerabilities in scanned projects
- Control CC5 - Snyk Cloud can dictate settings based on policies to define and limit authorized access

Software Development LifeCycle controls within SOC 2 focus on appropriate manual or orchestrated policies that ensure standardization across baseline configurations. This applies to all cloud infrastructure, images, and containers. Snyk can help you address the following SOC 2 control requirements:

- Control CC6.1, 6.2, 6.3, 6.8 (open source code)/ CC7.1, 7.2, CC8.1 - Snyk Cloud provides a single policy to administer baseline configuration and standardization for cloud infrastructure, images, and containers (e.g. logical access, network, encryption, port setting, backups, etc.)

02

ISO 27001

The ISO 27001 controls cover several areas supported by the Snyk platform, including: improved education and training of developers, vulnerability management, standardization of base images, license management and inventory, reporting, monitoring and visibility, and malware identification and management in source code.

Specifically, Snyk can help you address the following ISO 27001 control requirements:

- 5.1/7.2/7.3 Appendix A.7.2.2 - Snyk offers security training targeted directly to developers
- A.8.9/8.25 (14.1.1,14.2.1)/8.26(14.1.2,14.1.3)/8.29(14.2.8,14.2.9)/A.8.28 - Snyk offers policy-based configurations and industry-recognised standardization from code to cloud, for both proprietary and open source code
- 6.2c/A.5.7 - Snyk prioritizes vulnerabilities based upon security intelligence for enhanced risk assessment
- 7.4 Appendix A.15.1.3/A.16.1.3 - Snyk alerts developers and security teams to changes in the risk of code and open source dependencies in all scanned projects
- Appendix A.18.1.1 - Snyk can show all open source licensing in use, including the type of license
- 6.1.2 (c,d,e) - Snyk identifies vulnerabilities from code to cloud and prioritizes threats based on known exploits, social media, and reachability factors
- A.18.2.2/2.3/A.18.2.3 - reporting allows for monitoring and governance of overall application security maturity
- A.8.1.1/8.1.2 - Snyk identifies code repositories and dependencies in use for SBoM creation and risk management of those components
- A.9.2.3/A.9.4.1/A.9.4.2/A.9.4.3/A.9.1.2/A.9.2.5/A.9.2.6/A.13.1.1/A14.2.5 - Snyk provides strict access control within the platform as well as code-level control of baseline secure configuration of Infrastructure, containers, and images in projects
- A.12.2.1 - Snyk Open Source identifies malware present in open source code
- A14.2.6 - Snyk offers secure IDE and CLI options for use in the SDLC
- A.12.6.1 - Snyk delivers comprehensive lists of vulnerabilities in all scanned projects with auto pull request generation for remediation, prioritization, and continuous improvement

03

PCI

The PCI DSS controls focus on the security of payment card data. Within the software development lifecycle, Snyk supports key vulnerability management and education requirements of the following controls:

- Control 1.3 - Snyk Learn offers pointed security training to developers in real-time
- Control 3.1 - The Snyk platform allows users to identify software assets and components and create a software builds of materials (SBOM)
- Controls 3.2.(a,b,c), 3.3.(a,b), 3.4.(a,b) - The Snyk platform identifies vulnerabilities in proprietary code and open source code as related to applications, containers, and infrastructure as code. It offers automated notification, remediation, reporting, security gating, and exception handling
- Controls 4.1.a, 4.1.b, 4.2.a The Snyk platform automatically notifies of vulnerability changes for any project included in the scanning function

Schedule an expert demo to learn how Snyk can help you meet your compliance goals.

Questions? Contact us at sales@snyk.io.