SIG 2025

Scoped As: Standard SIG 2025 Lite

Jump To:

Licensed to: Snyk

Progress: 100%

Tab Automation: Enable

Questionnaire Instructions:

- For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the Additional Information field in column E to provide an explanation.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page and filters are enabled.
- There may be gaps in the question number sequence depending on how the outsourcer generated the SIG.

MODIFICATION OF THIS DOCUMENT IS A VIOLATION OF THE COPYRIGHT AND MAY RESULT IN FINANCIAL PENALTY FOR YOU OR YOUR SERVICE PROVIDER

Ques Num	Question/Request	Response	Additional Information	Control Family	Control Attribute	Shared Assessments SCA 2025	ISO 27001:2022	Doc Ref
A.1	Is there a formalized risk governance policy approved by management that defines the Enterprise Risk Management program requirements?	Yes	Snyk maintains a formal Enterprise Risk Policy and process in line with ISO27001:2022 and SOC2 requirements. Strategic reviews occur annually, whilst operational risk reviews are continuous. Results of internal and third party risk assessments are considered confidential and are not available for release. Snyk can provide evidence of external Penetration tests on request, however if for a prospect a MNDA will be required prior to release. Customer can gain assurance that adequate risk processes are in place through our ISO/IEC 27001:2022 certification as well as our ISAE3402 SOC2 Type II report.	Risk Management Principles	Policies, Standards and Procedures	A.1 Enterprise Risk Governance|A.2 Risk Assessment and Treatment		A.1
B.1	Is there a third party risk management program that is reviewed and approved by management which includes 4th and Nth parties as part of the program?	Yes	Snyk makes use of a range of subcontractors and data sub processors in order to deliver services to customers. All security or service impacting suppliers undergo a security review as part of procurement, and at least annually thereafter. All security impacting suppliers must agree to our data processing agreement and security addendum, or otherwise include the controls therein in contractual language. Snyk's third party management is also externally validated as part of our ongoing ISO/IEC 27001:2022 certification process and ISAE3402 SOC2 Type II annual report. Please see an up to date list of subcontractors and sub-processors here: https://snyk.io/policies/subprocessors/	Risk Management Principles	Third-Party Risk Management	C.2 Information Security Policy Maintenance		C.2
B.2	For all organizational entities (e.g., vendor's vendors, subcontractors, fourth parties, Nth parties) is there a contractual relationship that extends obligations to each entity?	Yes		Risk Management Principles	Contracts and Agreements	B.1 Assessed Third Party Risk Management Program		B.2.1
C.1	Is there a documented, approved cybersecurity risk management policy communicated across the organization?	Yes		Program Management	Policies, Standards and Procedures		4.4 Information Security Management System|6.2 Information Security Objectives and Planning to Achieve Them|7.3 Awareness|7.4 Communication	C.2
C.4	Is there a documented risk assessment process for information security with consistent and comparable results?	Yes		Risk Management Principles	Risk Assessments	C.2 Information Security Policy Maintenance	6.1.2 Information security risk assessment	
D.1	Is there a management-approved asset management program that is communicated to constituents and has an owner to maintain, review, and manage IT assets (e.g. systems, hardware, services, and data), and respective controls, throughout their life cycles?	Yes	Snyk maintains an ISO27001:2022 certified asset management policy. This is provided to all employees and associated training provided. All employees are required to read and accept our Information Security policy which in-turn refers to the acceptable use of assets and media.	Managed Assets	Asset Program Management			
D.2	Is there an acceptable use policy for information and associated assets that has been approved by management, communicated to appropriate constituents, and assigned an owner to maintain and periodically review the policy?	Yes	Snyk has implemented an acceptable use policy in line with ISO27001:2022 requirements. All staff are required to read and sign an Employee Security Policy on hire which includes our acceptable use controls. This process is managed via our People team.	Identity and Access Management	Policies, Standards and Procedures	E.2 Terms and Conditions for Employment		E.2
D.3	Is there a records retention policy and retention schedule covering paper and electronic records, including email in support of applicable regulations, standards, and contractual requirements?	Yes	Snyk maintains a formal information retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements.	Governance and Oversight	Documents, Records and eDiscovery Management	P.5 Data Processing Obligations		P.5
E.1	Are Human Resources policies and procedures approved by management, communicated to constituents and have an owner to maintain and review?	Yes		Personnel Security	Policies, Standards and Procedures	E.1 Pre-Employment Screening	7.3 Awareness|7.4 Communication	E.1
E.3	Does the organization have an employee performance process that is documented, maintained, and reviewed by management periodically?	Yes		Personnel Security	Human Resources Management	E.4 Performance and Appraisal Process	7.2 Competence|9 Performance evaluation|9.3 Management review	E.4
F.1	Has management approved a physical security program that is communicated to all parties involved, with an assigned owner responsible for maintenance and review?	Yes	Snyk outsources all office and hosting functions to third parties. All hosting services are provided by GCP and AWS. They are responsible for the physical and environmental security policies of their hosting environments. (See GCP https://cloud.google.com/security & https://cloud.google.com/security/overview/whitepaper#technology_with_security_at_its_core. See AWS https://aws.amazon.com/artifact/, https://aws.amazon.com/compliance/faq/ for more information on their security controls and compliance reports.) All Snyk offices are leased, with the majority of workers being remote. Where leased premises are in place, all employees follow our ISO/IEC27001:2022 compliant Physical security policy. The landlords of the leased buildings are responsible for the physical and environmental security of each individual site. All security requirements for third party vendors are managed as part of our supply chain process.	Physical and Environmental Protection	Policies, Standards and Procedures			
G.1	Are the organization's Information Technology Operations policies and procedures monitored, aligned with the organizational strategy, and communicated to the entire organization?	Yes		Personnel Security	Policies, Standards and Procedures		5.1 Leadership and Commitment	
G.2	Is there an operational Change Management/Change Control policy or program that has been documented, approved by management, communicated to appropriate constituents, and assigned an owner to maintain and review the policy?	Yes	Snyk operates a strongly DevOps oriented operational model which includes rapid, decentralised but technically enforced change management, widespread use of orchestration, testing, documentation, approval and rollback procedures. As we operate a CI/CD approach, changes are continually deployed	Change Management	Policies, Standards and Procedures			
G.3	Are information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?	Yes		Program Management	Information Security Program	G.1 Change Management		G.1

H.1	Has management approved an access control policy, communicated it to constituents, appointed an owner to maintain it, and reviewed it?	Yes		Identity and Access Management	Policies, Standards and Procedures	C.1 Information Security Standards|H.1 Access Control Policy		C.1
H.2	**Has management approved, communicated, and enforced a password policy for systems that transmit, process, or store scoped data on all platforms and network devices?**	Yes	Snyk's Internal Password Policy: - Complexity: - Minimum 10 characters in length. - Must include: - Uppercase and lowercase letters. - A number. - A special character. - Cannot contain parts of the username, first name, or last name. - Cannot be a common or easily guessable password. - History: - Maintains a password history of at least four months. - Passwords are not arbitrarily forced to change. - Passwords will only be changed when there is evidence of a compromise. - This aligns with NIST SP 800-63B Section 5.1.1.2 paragraph 9, which discourages arbitrary password changes. - Account Lockout: - Accounts are locked for sixty minutes after ten unsuccessful login attempts.	Identity and Access Management	Access Control Management			
H.2.1	Does the password policy require keeping passwords confidential?	Yes		Identity and Access Management	Policies, Standards and Procedures			
I.1	**Are applications used to transmit, process, or store scoped data?**	Yes		Application Development	Application Program Security			
I.1.1	Are the development, testing, and staging environments kept separate from the production environment?	Yes		Program Management	Secure Architecture Design Standards	G.1 Change Management		G.1
I.2	**Is application development performed?**	Yes		Application Development	Application Program Security			
I.2.1	Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain, and review the policy?	Yes		Program Management	Secure Software Development Life Cycle (SSDLC) Management	I.3 Secure Systems Development Life Cycle (SDLC)		I.3
I.3	**Is a web site or web application supported, hosted, or maintained that processes scoped systems and data?**	Yes	app.snyk.io	Web Server Security	Web Management			
I.3.1	Are security configuration standards documented for web server software?	Yes		Web Server Security	Web Management			
I.3.2	Is an Application Programming Interface (API) available to clients?	Yes	Snyk has a fully-featured API. Most features available in the standard GUI can be automated via our API including importing projects, initiation and results of project scans, issue reporting, user and group membership listing. Snyk API v1 is supported by Apiary and API Blueprint. Snyk REST API is based on the JSON:API standard, defined in OpenAPI 3, and represents an evolutionary approach to API development, with each endpoint versioned. Full details of our APIs are here: https://snyk.docs.apiary.io/ https://apidocs.snyk.io/	API Security	Application Program Security			
J.1	Has management approved and communicated a Cybersecurity Incident Management Program with a designated owner to maintain and review it?	Yes		Incident Response	Incident Management	J.1 Cybersecurity Governance		J.1
J.4	Does the organization have a documented Incident Response Plan that outlines the escalation process?	Yes	Snyk maintains a formal incident response plan as per ISO/IEC 27001:2022 requirements. The IRM plan is reviewed at least annually with regular training, exercises and drills. The Director of Business Resilience is responsible for ensuring adequate incident management processes are in place.	Incident Response	Incident Management	G.9 System Monitoring|P.2 Data Privacy Program		G.9
J.5	**Is there a specific methodology to regularly review events on scoped systems or systems containing scoped data to uncover potential incidents?**	Yes		Incident Response	Incident Management			
J.5.1	Does regular security monitoring include alerts for malware infections and suspicious activity?	Yes		IT Services and Infrastructure	Logging and Monitoring Management			
J.11	Has the organization outsourced its incident reporting responsibilities to a third-party service provider?	No		Contingency Planning	Business Resilience Plan Management			
J.14	Are the actions conducted during an incident investigation formally documented and protected from unauthorized changes?	Yes		Incident Response	Incident Management			
K.1	Has the organization established a Business Resilience Policy, designated an owner to maintain and review it, and communicated it?	Yes	Snyk maintains a formal incident response plan as per ISO/IEC 27001:2022 requirements. The IRM plan is reviewed at least annually with regular training, exercises and drills. The Director of Business Resilience Senior Manager, Incident Response is responsible for ensuring adequate incident management processes are in place.	Contingency Planning	Board Structure, Independence and Accountability			
K.2	Is there a formal, documented information technology disaster recovery exercise and testing program in place?	Yes		Contingency Planning	Policies, Standards and Procedures	K.6 Exercising and Testing		K.6
K.3	Are there any dependencies on critical third party service providers?	Yes	Snyk makes use of a range of subcontractors and data sub processors in order to deliver services to customers. All security or service impacting suppliers undergo a security review as part of procurement, and at least annually thereafter. All security impacting suppliers must agree to our data processing agreement and security addendum, or otherwise include the controls therein in contractual language. Snyk's third party management is also externally validated as part of our ongoing ISO/IEC 27001:2022 certification process and ISAE3402 SOC2 Type II annual report. Please see an up to date list of subcontractors and sub-processors here: https://snyk.io/policies/subprocessors/	Contingency Planning	Business Resilience Plan Management	K.3 Operational Risk Assessment		K.3
K.4	Is there a pandemic/infectious disease outbreak plan?	Yes		Risk Management Principles	Policies, Standards and Procedures			

K.5	Is scoped data backed up and stored offsite?	Yes	Full database snapshots are taken daily and stored with a minimum retention of 90 days. Each snapshot is propagated to multiple GCP & AWS cloud storages in multiple availability zones and in multiple regions within the same geographic location.. Daily backups provide a last resort recovery in case of massive data corruption or loss. Snyk regularly tests the integrity and validity of it's backups. Full restore tests take place quarterly as part of our Business Continuity plan	Contingency Planning	Data Management			
K.6	Is there a formal process focused on identifying and addressing risks of disruptive events to business operations (e.g., operational risk assessment?)	Yes	Snyk maintains a formal Enterprise Risk Policy and process in line with ISO27001:2022 and SOC2 requirements. Strategic reviews occur annually, whilst operational risk reviews are continuous. Results of internal and third party risk assessments are considered confidential and are not available for release. Snyk can provide evidence of external Penetration tests on request, however if for a prospect a MNDA will be required prior to release. Customer can gain assurance that adequate risk processes are in place through our ISO/IEC 27001:2022 certification as well as our ISAE3402 SOC2 Type II report.	Contingency Planning	Business Continuity Management	K.3 Operational Risk Assessment		K.3
K.7	Have formal procedures for business continuity been developed and documented?	Yes	Snyk maintains a formal business continuity and disaster recovery programme and working group, aligned to the requirements of ISO/IEC 27001:2013	Contingency Planning	Business Continuity Management			
K.11	Is there a data retention policy or process with a retention schedule for scoped data?	Yes	Full database snapshots are taken daily and stored with a minimum retention of 90 days. Each snapshot is propagated to multiple GCP & AWS cloud storages in multiple availability zones and in multiple regions within the same geographic location.. Daily backups provide a last resort recovery in case of massive data corruption or loss. Snyk regularly tests the integrity and validity of it's backups. Full restore tests take place quarterly as part of our Business Continuity plan	Contingency Planning	Policies, Standards and Procedures	L.1 Legal, Regulatory and Standards Compliance		L.1
K.30	Is there a resiliency strategy that includes a multi-vendor strategy that mitigates key dependencies on third-party service providers?	Yes		Data Governance	Business Resilience Plan Management			
L.1	Are there policies and procedures to ensure compliance with applicable legislative, regulatory, and contractual requirements?	Yes	Snyk Legal team maintain a formal legal register which contains all relevant legislation and regulations that Snyk must adhere to as well as documented controls that must be in place in order to maintain compliance.	Governance and Oversight	Policies, Standards and Procedures			
L.2	Is a web site(s) maintained or hosted for the purpose of advertising, offering, managing, or servicing accounts, products, or services to clients' customers?	No		Industry Regulatory Compliance	Consumer Protection			
L.3	Are there policies and procedures for addressing antitrust and anti-competitive business practices?	Yes		Industry Regulatory Compliance	Logging and Monitoring Management			
L.4	Is there a documented internal compliance and ethics program?	Yes	Snyk maintains a formal compliance programme and legal register which is used to monitor all regulatory and legal requirements Snyk must adhere to in line with ISO27001:2022 requirements.	Industry Regulatory Compliance	Business Ethics and Corporate Compliance	L.2 Corporate Compliance		L.2
L.5	Are documented policies and procedures maintained to enforce applicable legal, regulatory, or contractual cybersecurity compliance obligations?	Yes		Industry Regulatory Compliance	Policies, Standards and Procedures	L.1 Legal, Regulatory and Standards Compliance		L.1
L.6	Are there policies and procedures for detecting and preventing internal and external fraud?	Yes	Snyk maintains formal Anti-Fraud, Bribery and Corruption policies.	Industry Regulatory Compliance	Business Ethics and Corporate Compliance	L.2 Corporate Compliance		L.2
M.1	**Do desktops, laptops, tablets, or smartphones transmit, process, or store Scoped data?**	Yes	Snyk has implemented multiple security controls to ensure the security of customer data and solutions. These controls ensure we have ongoing visibility of what our end point is doing, that we can detect and react quickly to any tampering or threats as well as logging and enforcement controls. Controls consist of the following: - All access to critical environments is via SSO with MFA (OKTA Verify) - In terms of engineering, access to production is via Security Defined Perimeter network access layer. (Teleport) - Snyk has full visibility for any application installed on the endpoints via Jamf (MDM) and CrowdStrike (EDR) services. That includes application's version, publisher and an indication if it was installed via the Apple's App store (which is our recommended source for applications). - Jamf monitors that Gatekeeper feature is set to allow installation of apps only from the App Store or identified developers (by signature). - Endpoint can't access production and connect to Snyk's SDP (Teleport) without passing several posture checks that includes active EDR agent (CrowdStrike), MDM agent (Jamf) and disk encryption in place. - Crowdstrike scans continuously on workstations, sending vulnerability data back to the portal every six hours. - Relevant security policy and acceptable usage policy restrict the usage of company endpoints to work related tasks only. - Snyk utilises CrowdStrike, a sensitive next-gen Behavioral AI based EDR engine, that is configured to automatically kill & quarantine any suspicious process and allows our incident response team to immediately disconnect that endpoint from the network. - CrowdStrike alerts are monitored and analysed by our 24x7 SOC (Expel.io) in order to facilitate rapid response. The 24x7 SOC has escalation paths to our Security Engineering team, including PagerDuty alerts.	Network Management	Device Management			
M.1.1	Does the organization's build and hardening standards criteria deploy endpoint security features to secure and prevent cybercriminals from gaining access to their network?	Yes	Snyk maintains internal hardening standards using CIS benchmarks as a baseline which are continosly validated using our own automated testing tools as part of the build process and using continous security monitoring tooling . Policies and processes for hardening configurations are certified as part of our ongoing ISO27001:2022 compliance.	Network Management	Hardening Standards			
M.1.2	Are constituents allowed to utilize mobile devices within the organization's environment?	Yes	Snyk mobiles must run Google MDM to be permitted access to certain corporate applications. MDM ensure minimum set of security controls are in place	Configuration Management	Mobile Device Management			

M.1.3	Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?	Yes	Snyk mobiles must run Google MDM to be permitted access to certain corporate applications. MDM ensure minimum set of security controls are in place	Configuration Management	Mobile Device Management	F.6 Physical Security Testing and Compliance Inspections		F.6
M.1.4	Can constituents access corporate e-mail using mobile devices?	Yes	Snyk mobiles must run Google MDM to be permitted access to certain corporate applications. MDM ensure minimum set of security controls are in place	Configuration Management	Mobile Device Management			
M.1.5	Are non-company managed computing devices used to connect to the company network?	No	We do not allow BYOD	Managed Assets	Asset Program Management			
M.1.6	Are any mobile devices with access to scoped data Constituent owned (BYOD)?	No	We do not allow BYOD	Managed Assets	Mobile Device Management	M.1 Mobile Application Management		M.1
M.3	Does the organization maintain policies and procedures for the access to and the usage of collaborative computing devices or applications e.g., networked white boards, cameras, and microphones?	No		Application Development	Policies, Standards and Procedures	H.11 User Awareness on Remote Sessions|M.3 Secure File Sharing or Exchange		H.1
N.1	Does the organization build and maintain a secure network and systems?	Yes	Aligned to the requirements of ISO/IEC 27001:2013 and SOC2 Type II	Network Management	Device Management			
N.2	Does the organization have a Network Security Program with a defined policy that outlines security requirements, is reviewed regularly by an owner, and communicated to relevant parties?	Yes	Snyk's application cluster is hosted on either AWS or Google's Cloud Environments. In this model, the underlying cloud platform provides network security controls, while Snyk's network and system architects configure the various routing and security groups in collaboration with Snyk's operations personnel. Snyk's application cluster is protected by a security group, which provides network access filtering from the broader Internet. Filtering is maintained to allow incoming connections only on specific ports and protocols required for the cluster's standard operation. Database ports are not exposed to the Internet. Additionally, Snyk uses a configured host-based firewall to further isolate traffic on individual instances.	Network Management	Hardening Standards	C.1 Information Security Standards|C.5 IT Organization Roles and Responsibilities|N.1 Secure Engineering and Architecture		C.1
N.3	Is every connection to an external network terminated at a firewall e.g., the Internet, partner networks?	Yes		Network Management	Network Segregation and Segmentation Management	N.10 Network Monitoring		N.1
N.4	Are all network devices patched with all, available high-risk security patches applied and verified?	Yes		IT Services and Infrastructure	Patch Management	G.2 Patch Management		G.2
N.5	Has management approved a policy for remote access to scoped systems and data communicated to constituents?	Yes	SSO integration via Software Defined Perimeter (Teleport) and OKTA	Identity and Access Management	Policies, Standards and Procedures	F.3 Workspace Environment|H.8 Remote Access		F.3
N.7	Are Network Intrusion Detection/Prevention Systems (NIDS/NIPS) employed e.g., appliances, software, etc.?	Yes	To further enhance security, Snyk leverages a multi-layered approach. Expel MDR specifically monitors for suspicious activity related to privileged accounts. CrowdStrike Falcon Complete provides comprehensive endpoint protection. Additionally, a Security Information and Event Management (SIEM) system collects and analyzes security logs, enabling proactive threat detection and response. This robust security posture ensures the ongoing security of Snyk's systems and data.	IT Services and Infrastructure	Intrusion Detection and Prevention Systems (IDS-IPS)	N.10 Network Monitoring		N.1
N.8	Is there an DMZ environment within the network that transmits, processes, or stores scoped systems and data e.g., web servers, DNS, directory services, remote access, etc.?	Yes		Network Management	Network Controls and Security	N.1 Secure Engineering and Architecture		N.1
N.9	Is there a wireless policy or program that has been approved by management, communicated to appropriate constituents and has an owner to maintain, and review the policy?	Yes	While Snyk utilizes wireless technology within its internal infrastructure, all access to customer data and production systems is governed by a strict Zero Trust security model. This model assumes no implicit trust and continuously verifies and authorizes every device and user request, regardless of network location. This ensures that even if wireless networks are compromised, customer data remains protected.	Network Management	Policies, Standards and Procedures	M.2 Removable Device Management		M.2.2
N.11	Are there security standards, baseline configurations, patching, access control, and strong passwords for network devices such as Firewalls, Switches, Routers, and Wireless Access Points?	Yes	Snyk maintains internal hardening standards using CIS benchmarks as a baseline which are continosly validated using our own automated testing tools as part of the build process and using continous security monitoring tooling . Policies and processes for hardening configurations are certified as part of our ongoing ISO27001:2022 compliance.	IT Services and Infrastructure	Hardening Standards	N.3 Data Flow Enforcement		N.3
N.12	Are default passwords changed or disabled prior to placing network devices into production?	Yes	Snyk maintains a strict policy of changing all default vendor passwords before any system or device is deployed to a production environment. This critical security practice helps prevent unauthorized access and mitigates the risks associated with using default credentials.	IT Services and Infrastructure	Password Controls	H.1 Access Control Policy		H.1
O.1	**Does the organization have and adhere to an environmental policy that sets out clear commitments and targets to improve the organization's footprint?**	Yes	Please see our Impact page here: https://snyk.io/about/snyk-impact/	(ESG) Environmental	Environmental Management	O.1.11 Policies and procedures that address air pollution		O.1
O.1.1	Does the organization's environmental policy cover climate change issues that could be material to the organization?	Yes		(ESG) Environmental	Climate Change	O.1.4 Policy or statement for green energy usage		O.1
O.2	Does the organization have material discharges to air as a direct result of its operations?	No		(ESG) Environmental	Air Pollution	O.3 Corporate Governance Policy		O.1
O.3	Does the organization have processes to ensure that there are no material discharges to land or water, as a direct result of business operations?	N/A		(ESG) Environmental	Waste Management	O.3.6 Policies and procedures that address compensation		O.1
O.4	Has the organization implemented procedures to ensure the safe use, handling, storage, and disposal of hazardous/toxic chemicals and substances?	N/A		(ESG) Environmental	Hazardous & Toxic Material Management	O.3 Corporate Governance Policy		O.1
O.5	Does the organization maintain processes to ensure there are no adverse impacts on biodiversity, including deforestation, ecosystem integrity, natural resource conservation, and land degradation?	N/A		(ESG) Environmental	Natural Resource Management & Use	O.3 Corporate Governance Policy		O.1
O.6	Are there any financial provisions in the annual accounting statements of the organization to address environmental issues, breaches, non-compliances, enforcements, prosecutions, or fines, if they exist?	N/A		(ESG) Environmental	Regulatory Compliance	O.3 Corporate Governance Policy		O.1
O.7	Does the organization have documented policies and procedures in place that address the prevention of modern slavery?	Yes	Snyk has an anti-slavery policy in place, please see our Anti-Modern Slavery statement here: https://snyk.io/policies/regulatory/ as well as our Supplier Code of Conduct: https://snyk.io/procurement/supplier-code-of-conduct/ for further details.	(ESG) Social	Human Rights & Labor Practices	O.3 Corporate Governance Policy		O.2
O.8	Does the organization ensure that sub-contractors are treated fairly and ethically per local standards and regulations?	Yes		(ESG) Social	Worker Health & Safety	O.3 Corporate Governance Policy		O.2
O.9	Does the organization have a documented policy on Health and Safety?	No		(ESG) Social	Worker Health & Safety	O.3 Corporate Governance Policy		O.2
O.10	Has the organization established formal community relations programs to promote its involvement in the community?	Yes		(ESG) Social	Community Involvement	O.1.1 Policy or statement on climate change		O.2
O.11	Does the organization have policies to ensure products and services do not generate health and safety concerns?	N/A		(ESG) Social	Consumer Safety & Product Safety	O.1.4 Policy or statement for green energy usage		O.2
O.12	**Does the organization have a formalized Environmental, Social, and Governance (ESG) program or set of policies & procedures aligned to its Enterprise Risk Management framework approved by executive management and the Board of Directors?**	Yes	Please see our Impact page here: https://snyk.io/about/snyk-impact/	(ESG) Governance	Board Structure, Independence and Accountability	O.1.4 Policy or statement for green energy usage		O.3

O.12.1	Are the organization's Environmental, Social, and Governance (ESG) policies regularly reviewed and approved by executive management and the Board of Directors?	Yes		(ESG) Governance	ESG Management Practices & Processes	O.1.17 Process for reporting results and recommendations to senior management		O.3
O.13	Does the organization have a formal diversity, equity, and inclusion (DEI) statement or policy?	Yes		(ESG) Governance	Ethics & Codes of Conduct	O.1.4 Policy or statement for green energy usage		O.3
O.14	**Does the organization have a documented policy for Ethical Sourcing?**	Yes		(ESG) Governance	Supply Chain Management	O.2 Social Responsibility Policy		O.3
O.14.1	Does the organization have a responsible purchasing procedure or standard for suppliers?	Yes		(ESG) Governance	Supply Chain Management	O.2 Social Responsibility Policy		O.3
P.1	**Is there collection, access, processing, disclosure, or retention of any classification of personal information or personal data of individuals on behalf of the client?**	Yes	Please see our privacy policy and data processing addendum https://snyk.io/policies/privacy/ & https://snyk.io/policies/dpa/ Additionally Snyk has created a "How Snyk Handles your data guide" for more information. https://docs.snyk.io/working-with-snyk/how-snyk-handles-your-data	Data Governance	Data Privacy, Security & Management			
P.1.2	Is client scoped data collected, accessed, transmitted, processed, disclosed, or retained that can be classified as nonpublic personal information or personally identifiable financial information under the Gramm-Leach-Bliley Act (GLBA) and related Privacy and Security Safeguards Rules?	No		Personally Identifiable Information (PII) Processing & Transparency	Financial Services Privacy	P.1 Personal Information, Identification, and Classification		P.1
P.2	**Does the organization have a policy for preserving privacy and protecting personally identifiable information (PII) and is this policy communicated to all relevant parties?**	Yes	Please see our privacy policy and data processing addendum https://snyk.io/policies/privacy/ & https://snyk.io/policies/dpa/ Additionally Snyk has created a "How Snyk Handles your data guide" for more information. https://docs.snyk.io/working-with-snyk/how-snyk-handles-your-data	Personally Identifiable Information (PII) Processing & Transparency	Data Privacy, Security & Management			
P.2.1	Is client scoped data collected, accessed, processed, disclosed, or retained that can be classified as consumer report information or derived from a consumer report under the Fair and Accurate Credit Transactions Act (FACTA)?	No		Personally Identifiable Information (PII) Processing & Transparency	Financial Services Privacy	P.1 Personal Information, Identification, and Classification		P.1
P.2.2	**Is client scoped data collected, accessed, transmitted, processed, disclosed, or retained that can be classified as Protected Health Information (PHI) or other higher healthcare classifications of privacy data under the U.S. Health Insurance Portability and Accountability Act (HIPAA)?**	No		Personally Identifiable Information (PII) Processing & Transparency	Health Care Privacy	P.1 Personal Information, Identification, and Classification		P.1
P.2.3	Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified under U.S. State Privacy Regulations (e.g., CO, CA, CT, MA, NY, NV, VA, UT, WA, CO etc.)?	No		Data Governance	Domestic and International Privacy and Data Protection	P.1 Personal Information, Identification, and Classification		P.1
P.2.4	Is client scoped data collected, accessed, transmitted, processed, disclosed, or retained that can be classified as European Union Personal Data or Sensitive Personal Data (e.g., racial, or ethnic origin, genetic data, biometric data, health data, sexual orientation, criminal history)?	No		Data Governance	European Privacy and Data Protection	P.1 Personal Information, Identification, and Classification		P.1
P.2.5	Is client scoped data collected, transmitted, processed, disclosed, or retained that can be classified as Personal Information as defined by Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) or Canadian Provincial Privacy Regulations?	No		Data Governance	Canadian Privacy and Data Protection	P.1 Personal Information, Identification, and Classification		P.1
P.2.6	Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified under any other international privacy jurisdictions? If Yes, list the applicable international location in the Additional Information field.	Yes	GDPR and CCPA - Please see our privacy policy and data processing addendum https://snyk.io/policies/privacy/ & https://snyk.io/policies/dpa/	Data Governance	Domestic and International Privacy and Data Protection	P.1 Personal Information, Identification, and Classification		P.1
P.2.7	Is client scoped data of minors collected, transmitted, processed, disclosed, or stored as part of the services? If Yes, specify the age limitation (e.g., Age 16 and under) in the Additional Information Field.	No		Personally Identifiable Information (PII) Processing & Transparency	Data Privacy, Security & Management	P.1 Personal Information, Identification, and Classification		P.1
P.3	**Has the organization developed and maintained a formal privacy program for the protection of personal information collected, accessed, transmitted, processed, disclosed, or retained on behalf of the client?**	Yes	Please see our privacy policy here: https://snyk.io/policies/privacy/	Data Governance	Data Privacy, Security & Management			
P.3.1	Is documentation of the data processing environment, including the role of the processor (such as data flows, schemas, information asset inventories, models, etc.), maintained for the systems/products/services that process client-scoped data based on data classification?	Yes	Please see our privacy policy and data processing addendum https://snyk.io/policies/privacy/ & https://snyk.io/policies/dpa/	Data Governance	Data Management	P.2 Data Privacy Program		P.2
P.4	Is there a training and awareness program that addresses data privacy and data protection obligations based on role for new workers (e.g., officers, directors, employees, contractors) at the time of onboarding?	Yes	Snyk performs security awareness training on-hire and continually according to a schedule throughout a given year. Training is provided and tracked from a formal LMS and includes a testing element.	Personnel Security	Education, Training and Awareness			
P.5	**Are there documented policies and procedures that define limits to the collection and use of personal information to authorized users regarding limiting the personal information collected and used by authorized users (e.g., minimum necessary, need to know, job role)?**	Yes		Personally Identifiable Information (PII) Processing & Transparency	Data Privacy, Security & Management			
P.5.1	Is there a documented policy or process to maintain accurate, complete, timely and relevant records of client scoped data?	Yes		Personally Identifiable Information (PII) Processing & Transparency	Policies, Standards and Procedures	P.5 Data Processing Obligations		P.5
P.5.3	Does the organization obtain personal information directly from the client?	Yes		Data Governance	Data Privacy, Security & Management			
P.6	Does the organization have or maintain internet-facing website(s), mobile applications, platform, or other digital services or applications that collect, use, disclose, process, or retain client-scoped data that are accessed directly by individuals?	Yes		Personally Identifiable Information (PII) Processing & Transparency	Data Privacy, Security & Management			
P.8	Does the organization have a data governance program and designated body accountable to define and implement administrative, technical, and physical and environmental safeguards for the protection of client scoped data?	Yes		Data Governance	Board Structure, Independence and Accountability	P.7 Data Management and Data Analytics		P.7
P.9	Are there policies and procedures in place to detect and report privacy incidents (such as unauthorized disclosure, misuse, alteration, destruction, or other compromises of client data) in accordance with the Gramm-Leach-Bliley Act (GLBA) and the related Privacy and Security Safeguards Rules?	N/A	Please see our privacy policy and data processing addendum https://snyk.io/policies/privacy/ & https://snyk.io/policies/dpa/	Incident Response	Policies, Standards and Procedures			
P.10	Do any other parties (e.g., affiliates, fourth-Nth parties, contractors, subcontractors, sub-processors, sub-service organizations, etc.) have access to, receive, process, or retain client scoped data?	Yes	Snyk makes use of a range of subcontractors and data sub processors in order to deliver services to customers. All security or service impacting suppliers undergo a security review as part of procurement, and at least annually thereafter. All security impacting suppliers must agree to our data processing agreement and security addendum, or otherwise include the controls therein in contractual language. Snyk's third party management is also externally validated as part of our ongoing ISO/IEC 27001:2022 certification process and ISAE3402 SOC2 Type II annual report. Please see an up to date list of subcontractors and sub-processors here: https://snyk.io/policies/subprocessors/	Procurement & Legal Risk	Contracts and Agreements			
P.11	Is there a data privacy or data protection role accountable for compliance, enforcement, and monitoring of its privacy obligations for client scoped data?	Yes		Audit and Accountability	Roles and Responsibilities			
P.12	If necessary, does the organization have a process to ensure that its registration information is accurate and complete with the appropriate competent authority no later than every 3 months?	Yes		Data Governance	European Privacy and Data Protection			
R.1	Does the organization have a process to inform personnel of legal and regulatory considerations and requirements specific to its industry, sector, and business purpose, and the application context of the deployed AI system(s)?	Yes		AI-Govern	Govern 1.1	R.1 AI-Govern-1		R.1
R.2	Do organizational policies, processes, and procedures include the characteristics of trustworthy AI?	Yes		AI-Govern	Govern 1.2	R.1 AI-Govern-1		R.1
R.4	Does the organization monitor and perform a periodic review of the AI risk management process and its outcomes that are planned to include organizational roles & responsibilities?	Yes		AI-Govern	Govern 1.5	R.1 AI-Govern-1		R.1
R.5	Does the organization establish policies that define the creation and maintenance of AI system inventories?	Yes		AI-Govern	Govern 1.6	R.1 AI-Govern-1		R.1
S.1	Does your organization have access control policies for suppliers, developers, and service providers that are passed down to sub-tier contractors?	Yes		Identity and Access Management	Policies, Standards and Procedures	S.1 Access Control		S.1

S.32	Is there a documented, approved Cybersecurity Supply Chain Risk Management (C-SCRM) policy or equivalent that addresses the strategy, objectives, and related processes for supplier adoption and contingency planning?	Yes		Contingency Planning	Policies, Standards and Procedures			S.6
S.57	Do the organization's media protection policies and procedures cover supply chain concerns, such as media within the supply chain and throughout the software development life cycle (SDLC)?	Yes		Media Management	Media Protection and Security	S.10 Media Protection		S.10
S.61	Does the organization integrate C-SCRM when developing a security planning policy?	Yes		Program Management	Policies, Standards and Procedures	S.12 Planning		S.12
S.80	Do the security policies and plans clearly define personnel responsibilities for supply chain security risk management activities?	Yes		Personnel Security	Policies, Standards and Procedures	S.14 Personnel Security		S.14
S.100	Do the organization's system and communications protection policies and procedures address cybersecurity risks throughout the supply chain regarding the enterprise's processes, systems, and networks?	Yes		Network Management	Policies, Standards and Procedures	S.18 System and Communications Protection		S.18
T.1	Is there a centrally managed Vulnerability Management Program and associated Policy that has been approved by management, communicated to appropriate constituents and an owner assigned to maintain and review the policy?	Yes		IT Services and Infrastructure	Policies, Standards and Procedures			
T.2	Does the organization maintain policies, standards, and procedures for identifying and managing cyber supply chain risks (i.e., ensuring software and hardware components used as part of delivering a service or product do not present a risk)?	Yes		IT Services and Infrastructure	Supply Chain Management			
U.1	**Are servers used for transmitting, processing, or storing scoped data?**	Yes	All hosting services are provided by GCP and AWS. They are responsible for the physical and environmental security policies of their hosting environments. (See GCP https://cloud.google.com/security & https://cloud.google.com/security/overview/whitepaper#technology_with_security_at_its_core. See AWS https://aws.amazon.com/artifact/, https://aws.amazon.com/compliance/faq/	IT Services and Infrastructure	Secure Architecture Design Standards			
U.1.1	Are server security standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or leading practices?	Yes		Configuration Management	Secure Architecture Design Standards	U.1 Server Security Configuration Standards		U.1
U.1.2	Are all unnecessary/unused services uninstalled or disabled on all servers?	Yes		Configuration Management	Secure Architecture Design Standards	U.1 Server Security Configuration Standards|V.1 Service and Deployment Models		U.1
U.1.3	Are vendor default passwords removed, disabled, or changed prior to placing any device or system into production?	Yes		Identity and Access Management	Password Controls	H.1 Access Control Policy|U.1 Server Security Configuration Standards		H.1
U.1.4	Are all systems and applications patched regularly?	Yes		IT Services and Infrastructure	Patch Management	G.1 Change Management|G.2 Patch Management|U.1 Server Security Configuration Standards|U.3 Server Patch Management Standards		G.1
U.1.5	**Are Windows servers used to process, store data or used for scoped services?**	No		IT Services and Infrastructure	Secure Architecture Design Standards			
U.1.6	Is Unix or Linux used to process, store data or used for scoped services?	Yes		IT Services and Infrastructure	Operating Security Systems	U.1 Server Security Configuration Standards		U.1
U.1.7	Are AS/400s used to process, store data or used for scoped services?	No		IT Services and Infrastructure	Operating Security Systems	U.1 Server Security Configuration Standards		U.1
U.1.8	Are Mainframes used to process, store data or used for scoped services?	No		IT Services and Infrastructure	Operating Security Systems	U.1 Server Security Configuration Standards		U.1
U.1.9	Are Hypervisors used to manage systems used to transmit, process, or store scoped data e.g., cloud hosting?	Yes	All hosting services are provided by GCP and AWS. They are responsible for the physical and environmental security policies of their hosting environments. (See GCP https://cloud.google.com/security & https://cloud.google.com/security/overview/whitepaper#technology_with_security_at_its_core. See AWS https://aws.amazon.com/artifact/, https://aws.amazon.com/compliance/faq/	Cloud Security	Hypervisor and Virtualization Security	U.1 Server Security Configuration Standards		U.1
V.1	Are Cloud Hosting services provided?	No		IT Services and Infrastructure	Cloud Management			
V.2	Does the Cloud Hosting Provider provide independent audit reports for their cloud hosting services (e.g., Service Operational Control - SOC)?	Yes		Audit and Accountability	Independent Audit and Certification Oversight			