Controls List for SOC2 Framework

TRUE NORTH

• PSR

Table of Contents

What is the SOC2 Framework?

SOC2 is filled with plenty of jargon but, at its core, it's about what resources (e.g. files, applications, permissions) the users of your systems have access to, and whether there are any time-based or location-based restrictions placed on their access.

SOC2 compliance is an audit framework designed to help service organizations (e.g., software services, and service agencies) demonstrate how they keep customers' data secure. Commonly adopted by software vendors, it establishes enforceable policies to secure companies' systems and protect the privacy of their customer data.

If this is the first time you've heard about the SOC2 framework, before you dig into this document, you would find it helpful to first check out our "No-Nonsense SOC2 Guide," which you can download on the same page where you downloaded this document.

If you're already acquainted with SOC2, read on.

What you see below is a description of all the operational requirements—or 'controls'—needed to align with what is perhaps the most common (and widely regarded) information security framework in North America. Further, implementing these controls is paramount if you wish for your company to become SOC2 certified.

Happy reading.

SOC2 Control Requirements

CRITERIA (OBJECTIVE)		CONTROL (COMPETENCY)
CONTROL ENVIRONMENT		
CC 1.1	The Entity ("Company") demonstrates a commitment to integrity and ethical values.	Company has established behavioural standards, which are defined in its Code of Conduct (CoC), which is available to all staff members on Company intranet.
		Company requires that new employees review and acknowledge the CoC upon hire and that all staff members review and acknowledge it annually.
CC 1.2	The Board of Directors (Board) demonstrates independence from management and exercises oversight of the development and performance of internal controls.	Company's Senior Management reviews and approves all Company policies annually.
		Company's Senior Management reviews and approves the state of the information security program annually.
		Company's Senior Management reviews and approves

		the Organizational Chart for all employees annually.
		Company's Senior Management reviews and approves the 'Risk Assessment Report' annually.
		Company's Senior Management reviews and approves the 'Vendor Risk Assessment Report' annually
CC 1.3	Management establishes structures, reporting lines, and appropriate authorities and responsibilities, with board oversight, to pursue its objectives.	Company maintains an Organizational Structure to define authorities, facilitate information flow, and establish responsibilities.
		Company ensures clarity in job responsibilities for client serving, IT, and engineering positions (e.g., via OKRs, job descriptions) to increase the operational effectiveness of the organization
CC 1.4	Company demonstrates a commitment to attract, develop, and retain competent individuals in alignment with its objectives.	Company ensures that new hires have been duly evaluated for competence in their expected job responsibilities.
		Company ensures that new hires go through a background check as part of their onboarding process.
CC 1.5	Company holds individuals accountable for their internal control responsibilities in the pursuit of its objectives.	Company has established information security awareness training, and its contents are available for all staff on Company intranet.
		Company requires that new staff members complete information security awareness training upon hire; and that all staff members complete it annually thereafter.
		Company requires that all employees in client serving, IT, engineering, and information security roles are periodically evaluated regarding their job responsibilities.
		Company requires that all staff members review and acknowledge company policies annually.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
COMMUNICATION AND INFORMATION		
CC 2.1	Company obtains or generates and uses relevant, quality information to support the functioning of internal control.	Company systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.
		Company makes all policies and procedures available to all staff members via Company intranet.
		Company displays the most current information about its services on its website, which is accessible to its customers.
CC 2.2	Company internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on Company intranet.

		Company requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.
		Company requires that all staff members review and acknowledge company policies annually
		Company makes all policies and procedures available to all staff members via Company intranet
		Company has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Company in the event there are problems.
		Company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
CC 2.3	Company communicates with external parties regarding matters affecting the functioning of internal control.	Company displays the most current information about its services on its website, which is accessible to its customers.
		Company has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Company in the event there are problems.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
RISK ASSESSMENT		
CC 3.1	Company specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Company has formally documented policies and procedures to govern risk management.
		Company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.
CC 3.2	Company identifies risks to the achievement of its objectives across Company and analyzes risks as a basis for determining how the risks should be managed.	Company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.
		Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		Company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their

		responsibilities and are willing to comply with them.
		Company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements.
CC 3.3	Company considers the potential for fraud in assessing risks to the achievement of objectives.	Company considers the potential for fraud when assessing risks. This is an entry in the risk matrix.
CC 3.4	Company identifies and assesses changes that could significantly impact the system of internal control.	Company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements
		Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		Company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
MONITORING ACTIVITIES		
CC 4.1	Company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Company 's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.
		Company uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		Company 's Senior Management reviews and approves all company policies annually.
		Company 's Senior Management reviews and approves the state of the Information Security program annually.
		Company 's Senior Management reviews and approves the Organizational Chart for all employees annually.
		Company 's Senior Management reviews and approves the "Risk Assessment Report" annually.
		Company 's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually

		Company reviews and evaluates all subservice organizations periodically, to ensure commitments to Company ’s customers can be met.
CC 4.2	Company evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Company has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Company in the event there are problems.
		Company uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		Company ’s Senior Management reviews and approves all company policies annually.
		Company ’s Senior Management reviews and approves the state of the Information Security program annually.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
CONTROL ACTIVITIES		
CC 5.1	Company selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Company has developed a set of policies that establish expected behavior with regard to Company ’s control environment.
		Company ’s Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.
CC 5.2	Company also selects and develops general control activities over technology to support the achievement of objectives.	Company uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		Company ’s Senior Management reviews and approves all company policies annually.
		Company ’s Senior Management reviews and approves the state of the Information Security program annually.
		Company ’s Senior Management reviews and approves the Organizational Chart for all employees annually.
		Company ’s Senior Management reviews and approves the “Risk Assessment Report” annually.
		Company ’s Infosec officer reviews and approves the list of people with access to production console annually.
		Company ’s Senior Management reviews and approves the “Vendor Risk Assessment Report” annually.
		Company reviews and evaluates all subservice

		organizations periodically, to ensure commitments to Company ’s customers can be met.
		Company has developed a set of policies that establish expected behavior with regard to Company ’s control environment.
CC 5.3	Company deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Company makes all policies and procedures available to all staff members via Company intranet.
		Company requires that all staff members review and acknowledge company policies annually.
		Company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
		Company has developed a set of policies that establish expected behavior with regard to Company ’s control environment.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC 6.1	Company implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet Company ’s objectives.	Company has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.
		Company maintains a matrix that outlines which system components should be accessible to staff members based on their role.
		Company ’s Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to Company ’s system.
		Company ’s Senior Management or the Information Security Officer periodically reviews and approves the list of people with Administative access to Company ’s system.
		Company ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
CC 6.2	Prior to issuing system credentials and granting system access, Company registers and authorizes new internal and external users whose access is administered by Company . For those users whose access is administered by Company , user system credentials are removed when user access is no longer authorized.	Company has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.
		Company maintains a matrix that outlines which system

		components should be accessible to staff members based on their role.
		Staff access to Company ’s systems are made inaccessible in a timely manner as a part of the offboarding process.
CC 6.3	Company authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet Company ’s objectives.	Company maintains a matrix that outlines which system components should be accessible to staff members based on their role.
		Staff access to Company ’s systems are made inaccessible in a timely manner as a part of the offboarding process.
		Company ensures that access to the Infrastructure provider’s environment (production console) is restricted to only those individuals who require such access to perform their job functions.
		Company ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.
CC 6.4	Company restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet Company ’s objectives.	Company relies on an infrastructure provider for hosting the systems supporting its production environment. As a result there is no physical access available to its staff members.
CC 6.5	Company discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet Company ’s objectives.	Company provides guidance on decomissioning of information assets that contain classified information in the Media disposal policy.
CC 6.6	Company implements logical access security measures to protect against threats from sources outside its system boundaries.	Company requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor-authentication.
		Company requires that all endpoints with access to production systems are protected by malware-protection software.
		Company requires that all company-owned endpoints be encrypted to protect them from unauthorised access.
		Company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.
		Company requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity.
		Every Production host is protected by a firewall with a deny-bydefault rule. Deny by default rule set is a default

		on Company ’s cloud provider.
		Company ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
CC 6.7	Company restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet Company ’s objectives.	Company requires that all company-owned endpoints be encrypted to protect them from unauthorised access.
		All production database[s] that store customer data are encrypted at rest.
		User access to Company ’s application is secured using https (TLS algorithm) and industry standard encryption.
		Company maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.
CC 6.8	Company implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet Company ’s objectives.	Company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.
		Every Production host is protected by a firewall with a deny-bydefault rule. Deny by default rule set is a default on Company ’s cloud provider.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
SYSTEM OPERATIONS		
CC 7.1	To meet its objectives, Company uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Company identifies vulnerabilities on Company platform through the execution of regular vulnerability scans.
		Company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Company ’s infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Company ’s Production assets are continuously monitored to generate alerts and take immediate action where necessary.
CC 7.2	Company monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting Company ’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Company identifies vulnerabilities on Company platform through the execution of regular vulnerability scans.

		Company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Company ’s infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Company ’s Production assets are continuously monitored to generate alerts and take immediate action where necessary.
CC 7.3	Company evaluates security events to determine whether they could or have resulted in a failure of Company to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Company uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		Company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.
		Company maintains a record of information security incidents.
		Company identifies vulnerabilities on Company platform through the execution of regular vulnerability scans.
		Company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Company ’s infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Company ’s Production assets are continuously monitored to generate alerts and take immediate action where necessary.
CC 7.4	Company responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Company uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		Company has established an Incident Management & Response Policy, which includes guidelines and procedures to be undertaken in response to information security incidents. This is available to all staff members via Company intranet.
		Company maintains a record of information security incidents.
CC 7.5	Company identifies, develops, and implements activities to recover from identified security incidents.	Company has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
		Company has a documented Data Backup Policy, and makes it available for all staff on Company intranet.

CRITERIA (OBJECTIVE)		CONTROL (COMPETENCY)
CHANGE MANAGEMENT		
CC 8.1	Company authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Company has a documented Change Management Policy, which is available to all Staff Members via Company intranet.
		Company uses a change management system to track, review and log all changes to the application code.
		Company maintains a list of infrastructure assets and segregates production assets from its staging/development assets.
		Company ’s change management system is configured to enforce peer reviews for all planned changes. For all code changes, the reviewer must be different from the author.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
RISK MITIGATION		
CC 9.1	Company identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Company has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Company ’s service commitments and system requirements.
		Company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems’ security commitments and requirements.
		Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
CC 9.2	Company assesses and manages risks associated with vendors and business partners.	Company has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Company ’s service commitments and system requirements.
		Company has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.
		Company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment

		and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
CONTROL CRITERIA FOR AVAILABILITY		
A 1.1	Company maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Company 's Production assets are continuously monitored to generate alerts and take immediate action where necessary.
A 1.2	Company authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Company has a documented Data Backup Policy, and makes it available for all staff on Company intranet.
		Company backs-up their production databases periodically.
		Company 's data backups are restored and tested annually.
		Company has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
A 1.3	Company tests recovery plan procedures supporting system recovery to meet its objectives.	Company has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
		Company 's data backups are restored and tested annually.
CRITERIA (OBJECTIVE)		**CONTROL (COMPETENCY)**
CONTROL CRITERIA FOR CONFIDENTIALITY		
C 1.1	Company identifies and maintains confidential information to meet Company 's objectives related to confidentiality.	Company has a documented Confidentiality Policy, and makes it available for all staff on Company intranet.
		Company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
		Company requires that all staff members review and acknowledge company policies annually.
		Company has a documented Data Classification Policy,

		and makes it available for all staff on Company intranet.
		All production database[s] that store customer data are encrypted at rest.
		Company requires that all company-owned endpoints be encrypted to protect them from unauthorised access.
C 1.2	Company disposes of confidential information to meet Company 's objectives related to confidentiality.	Company has a documented Data Retention Policy, and makes it available for all staff on Company intranet.
		Company provides guidance on decomissioning of information assets that contain classified information in the Media disposal policy.

What's My Next Step?

As you've navigated through this guide, we hope you've gained a deeper understanding of the SOC2 compliance journey and the value it could add to your business. Embracing SOC2 is not just about meeting a regulatory requirement; it's about securing trust in your services and protecting your customers' personal or otherwise confidential — a fundamental aspect of data-driven business.

At True North PSR, we recognize that the path to SOC2 compliance can seem daunting. If you determine you don't have sufficient in-house resources to adeptly execute such an undertaking, this is where our expertise can make a crucial difference.

Our team is ready to assist you at every step, ensuring that your compliance efforts are as seamless and efficient as possible. By partnering with us, you gain access to a wealth of knowledge and a partner who is as committed to securing your systems as you are.

Consider visiting our website at <www.TrueNorthPSR.com> to learn more about how we can help streamline your compliance program, ease the burden on your internal teams, and enhance your security posture. We would be happy to help you turn the complexities of SOC2 compliance into a strategic advantage for your business.