Continue

If youre preparing for a SOC 2 audit and want to ensure your success, downloading our SOC 2 Compliance Checklist will guide you along the process. This checklist can be used by IT Security and Compliance professionals to not only achieve SOC 2 Compliance, but also to evaluate Cyber Risk.Download your FREE SOC 2 Compliance Checklist MSPs: Get Your SOC2 Proposal in 5 Minutes! Start Your Self-Assessment Now Starting a SOC 2 audit can be overwhelming.You know you need a SOC 2 audit, but dont know what to expect or how to get started. The SOC 2 Compliance Checklist below will prepare you for what your auditors look for and how to confidently begin your SOC 2 compliance journey.What is a SOC 2 Compliance Audit?A SOC 2 audit attests that the system or service you provide to your clients is secure, trustworthy, and prepared to handle risks. This attestation is achieved through a quality examination of your people, processes, and technologies by an experienced, licensed CPA firm.A SOC 2 audit validates your organizations commitment to delivering high quality, secure services to your clients.Whats Included in the SOC 2 Compliance Checklist?This exclusive SOC 2 compliance checklist, prepared by KirkpatrickPrices SOC 2 compliance professionals, outlines the specifics of each system component that will be evaluated during your SOC 2 audit.The SOC 2 Checklist will cover:The Trust Services CriteriaThe system components evaluated in your auditWhich policies and procedures need to be in placeAverage length of a SOC 2 auditAnswers to frequently asked SOC 2 questionsWhat Makes a SOC 2 Audit Successful?After completing your SOC 2 audit, you might have concerns about completing it correctly. Here are four main metrics to help you evaluate a SOC 2 audits success:Receiving C-Level SupportC-level executives and stakeholders must understand and support the audit as it relates to the organizations information security needs. Without it, how can the business implement policies or procedures, approve funding, or drive the audits outcome?Authentically Taking Company-wide ActionWhile SOC 2 audits help strengthen and enhance a business, many organizations fall hesitant to the lengthy process and overlook the benefits as a result. An audit isnt something to be completed haphazardously. Instead, a business should perceive audits as an opportunity to improve internal processes, security, and organizational wellness amongst staff.For example, a quality SOC 2 audit could have helped Clorox take action and avoid a significant cybersecurity breach. Unfortunately, few companies value cybersecurity enough to include security experts on their board, despite its requirement of information security compliance frameworks. A successful audit helps companies remain vigilant in safeguarding their organization from the threat of a breach.Using Compliance as a Competitive AdvantageWhen an organization leverages compliance achievements as a competitive edge, they take full advantage of the achievement, incorporating audit insights into marketing materials and sales conversations.The opportunities are endless when you can demonstrate that you care about your customers data and have the evidence to prove it.Continuing the SOC 2 JourneyAfter completing a SOC 2 audit for the first time, many of our clients agree the process was difficult but worth it.By following remediation guidance, you can proactively prepare for the next audit. They know what to expect, how to use the Online Audit Manager, how to build a stronger information security program, and can show their auditor all the improvements made every year.Keep in mind, you dont have to have everything perfectly in place to start your audit. This checklist should just be a tool to help you prepare for your audit. If you need help putting controls in place, contact one of our experts today! We want to make sure you feel ready to successfully complete your SOC 2 audit.Prepare to successfully start and complete your SOC 2 audit by downloading the SOC 2 Compliance Checklist! Tags: SOC 2 Resources Photo by Luke Chesser on UnsplashSOC 2, or Service Organization Control 2, is a framework designed to guide service organizations in managing and safeguarding customer data.Developed by the American Institute of CPAs (AICPA), SOC 2 is a critical standard for businesses that handle sensitive information, particularly those offering cloud-based services.The framework is centered around five key trust service criteria security, availability, processing integrity, confidentiality, and privacy.Each criterion represents a fundamental aspect of data management and security, ensuring that organizations have robust measures in place to protect customer data.For organizations, achieving SOC 2 compliance is not merely a matter of adhering to best practices; it is a commitment to maintaining high standards of data security and privacy.This compliance helps organizations demonstrate their dedication to safeguarding sensitive information, thus enhancing their credibility and trustworthiness in the eyes of clients and stakeholders.By adhering to SOC 2 standards, organizations can also mitigate risks, improve operational efficiency, and avoid potential legal and financial repercussions associated with data breaches.The Role of SOC 2 Controls ListThe SOC 2 Controls List is an essential tool for organizations seeking SOC 2 compliance. It serves as a comprehensive checklist of the controls and processes required to meet SOC 2 standards.The purpose of this list is to provide a structured and organized approach to implementing and monitoring the necessary controls, ensuring that all aspects of SOC 2 compliance are addressed systematically.The SOC 2 Controls List XLS tool is particularly valuable because it allows organizations to access a detailed, customizable list of controls in a user-friendly format.This Excel-based tool offers several benefits, including the ability to tailor the controls to fit specific organizational needs, track compliance progress, and streamline audit preparation.By leveraging the SOC 2 Controls List XLS, organizations can effectively manage their compliance efforts and enhance their security posture.What is SOC 2?SOC 2, or Service Organization Control 2, is a framework that focuses on managing and protecting data based on five trust service criteria.These criteria are designed to ensure that service organizations handle customer data in a secure, reliable, and compliant manner. The five criteria are:Security: This criterion addresses the protection of systems and data against unauthorized access and attacks. It involves implementing measures such as firewalls, encryption, and access controls to safeguard data from potential threats.Availability: Availability ensures that systems are accessible and operational as per the agreed-upon service levels. It includes measures to maintain system uptime, perform regular backups, and ensure disaster recovery capabilities.Processing Integrity: This criterion focuses on ensuring that data is processed accurately, completely, and reliably. It involves implementing controls to prevent errors, fraud, and unauthorized changes to data.Confidentiality: Confidentiality involves protecting sensitive information from unauthorized disclosure. It includes measures to restrict access to confidential data and ensure that it is handled in accordance with privacy policies.Privacy: Privacy pertains to the collection, use, and disclosure of personal information in accordance with established privacy principles. It includes measures to protect personal data and ensure compliance with relevant privacy regulations.The primary objective of SOC 2 is to provide assurance to clients and stakeholders that an organization has implemented effective controls to manage and protect data.By adhering to SOC 2 standards, organizations can demonstrate their commitment to data security and build trust with their clients.Importance of SOC 2 ComplianceSOC 2 compliance offers numerous benefits for organizations and their customers.For organizations, compliance helps streamline operations, improve data security, and enhance their reputation in the marketplace.Achieving SOC 2 compliance also provides a competitive edge, as clients and partners often prefer to work with organizations that adhere to recognized security standards.From a customer perspective, SOC 2 compliance provides confidence that their data is being handled securely and responsibly.This assurance is crucial for maintaining trust and fostering strong business relationships.Additionally, SOC 2 compliance can help organizations meet legal and regulatory requirements, reducing the risk of fines and legal issues related to data breaches.Types of ControlsSOC 2 controls can be categorized into three main types: preventive, detective, and corrective. Each type of control plays a different role in managing and protecting data.1. Preventive Controls:These controls are designed to prevent security incidents from occurring.Examples include implementing strong access controls, conducting regular security training, and deploying antivirus software.Preventive controls aim to address potential vulnerabilities before they can be exploited.2. Detective Controls:Detective controls are focused on identifying and detecting security incidents as they occur.Examples include intrusion detection systems, log monitoring, and regular security audits.Detective controls help organizations identify and respond to security incidents in a timely manner.3. Corrective Controls:Corrective controls are implemented to mitigate the impact of security incidents and prevent them from recurring.Examples include incident response plans, data recovery procedures, and root cause analysis.Corrective controls aim to address the root cause of incidents and improve overall security posture.Features of the SOC 2 Controls List XLSThe SOC 2 Controls List XLS is a comprehensive tool that provides a detailed list of controls required for SOC 2 compliance.This list includes all the necessary controls for meeting SOC 2 standards, organized into relevant categories and sections.One of the key advantages of the SOC 2 Controls List XLS is its customization capability.Organizations can tailor the controls list to fit their specific needs and operational requirements, ensuring that it aligns with their unique security challenges and compliance objectives.User-Friendly FormatThe SOC 2 Controls List XLS is designed to be user-friendly, presented in an Excel format that is easy to navigate and use.The Excel format allows users to search for and filter controls based on their requirements, making it simple to find and review specific controls.The intuitive layout and structure of the Excel sheet enhance usability, ensuring that users can efficiently manage and track their compliance efforts.Regular UpdatesOne of the significant benefits of the SOC 2 Controls List XLS is that it is regularly updated to reflect the latest SOC 2 requirements.This ensures that organizations are always working with the most current and relevant controls.The tool also provides automatic updates and notifications, keeping users informed about any changes or additions to the controls list.This feature helps organizations stay up-to-date with evolving SOC 2 standards and maintain compliance effectively.How to Use the SOC 2 Controls List XLSGetting started with the SOC 2 Controls List XLS is straightforward. The file can be downloaded from the providers website, and it is accessible on various devices, including desktops, laptops, and tablets.Users can follow detailed instructions provided with the download to ensure a smooth start. The file is designed to be compatible with different devices and operating systems, making it easy to access and use.Navigating the Controls ListNavigating the SOC 2 Controls List XLS is made easy with its well-organized layout.The controls are categorized into sections based on the trust service criteria and types of controls.This organization allows users to quickly find and review specific controls relevant to their compliance efforts.The Excel format also includes features such as search and filter options to enhance navigation and usability.Customizing for Your OrganizationCustomizing the SOC 2 Controls List XLS to meet specific organizational needs is one of its most valuable features.Organizations can add, modify, and remove controls based on their unique requirements and operational practices.This customization ensures that the controls list aligns perfectly with the organizations security policies and compliance objectives.The ability to tailor the controls list allows organizations to address their specific security challenges effectively and efficiently.Benefits of Using the SOC 2 Controls List XLSUsing the SOC 2 Controls List XLS streamlines the compliance process, making it easier for organizations to achieve SOC 2 certification.The comprehensive nature of the controls list reduces the time and effort required to prepare for audits, simplifying the compliance journey.By providing a structured and organized approach to managing controls, the SOC 2 Controls List XLS helps organizations navigate the complexities of SOC 2 compliance more efficiently.Enhanced Security and TrustImplementing the SOC 2 Controls List XLS demonstrates an organizations commitment to data security and compliance.This commitment is crucial for building trust with clients, stakeholders, and partners.By adhering to SOC 2 standards and using the controls list to manage and monitor controls, organizations can enhance their security posture and strengthen their reputation in the marketplace.Cost-Effective SolutionThe SOC 2 Controls List XLS offers a cost-effective solution for achieving SOC 2 compliance.By leveraging the SOC 2 Controls List XLS, organizations can streamline their compliance journey, enhance their security posture, and build trust with clients and stakeholders.Future Trends in SOC 2 ComplianceAs technology and data security continue to evolve, so do the standards and practices associated with SOC 2 compliance.Staying informed about future trends and developments in SOC 2 is crucial for organizations to maintain compliance and ensure ongoing data security.Increased Focus on AutomationAutomation is becoming an increasingly important aspect of SOC 2 compliance.Automated tools and processes can help organizations streamline their compliance efforts, reduce the risk of human error, and improve overall efficiency.Future trends in SOC 2 compliance are likely to include greater integration of automated solutions for monitoring, reporting, and managing controls.Enhanced Security MeasuresAs cyber threats become more sophisticated, SOC 2 standards are expected to place greater emphasis on advanced security measures.This includes the adoption of next-generation security technologies, such as artificial intelligence and machine learning, to detect and prevent security incidents.Organizations will need to stay ahead of these trends to ensure their security practices remain effective and compliant with SOC 2 standards.Evolving Privacy RegulationsPrivacy regulations are continually evolving, with new laws and requirements being introduced worldwide.SOC 2 standards will likely adapt to these changes, placing increased emphasis on data privacy and protection.Organizations will need to stay informed about these regulatory developments and ensure their SOC 2 compliance efforts align with the latest privacy requirements.Greater Emphasis on Risk ManagementFuture trends in SOC 2 compliance are expected to include a greater focus on risk management.This involves identifying, assessing, and mitigating risks associated with data security and privacy.Organizations will need to adopt a proactive approach to risk management, implementing robust controls and practices to address potential vulnerabilities and threats.ConclusionAchieving SOC 2 compliance is essential for organizations that handle sensitive customer data.The SOC 2 Controls List XLS is a comprehensive, customizable, and user-friendly tool that simplifies the compliance process.By using this tool, organizations can enhance their security posture, build trust with clients, and achieve cost-effective compliance.The SOC 2 Controls List XLS provides all the necessary controls and resources to manage and monitor compliance efforts effectively, ensuring ongoing adherence to SOC 2 standards.Building a secure foundation for your startup is crucial, but navigating the complexities of achieving compliance can be a hassle, especially for a small team.SecureSlate offers a simpler solution:Affordable: Expensive compliance software shouldnt be the barrier. Our affordable plans start at just $99/month.Focus on Your Business, Not Paperwork: Automate tedious tasks and free up your team to focus on innovation and growth.Gain Confidence and Credibility: Our platform guides you through the process, ensuring you meet all essential requirements, and giving you peace of mind.Get Started in Just 3 MinutesIt only takes 3 minutes to sign up and see how our platform can streamline your compliance journey.Getting a SOC 2 report is an important step for any service organization.But getting compliant for the first time can be confusing. How do you know when youre ready for an audit?After all, theres no one-size-fits-all approach, and SOC 2 compliance requirements can vary.But that doesnt mean you cant go into an audit with confidence. In this article, well explain how to prepare for a SOC 2 audit, and share an interactive checklist to help you gauge your audit readiness.SOC 2 stands for Service Organization Controls 2. Its an attestation report created by the American Institute of Certified Public Accountants (AICPA) thats designed to help build trust between service organizations and their customers. aims to provide more clarity on the security controls used by service organizations.SOC 2 compares a service organizations security controls against five Trust Services Criteria:Security: How you secure data against unauthorized accessAvailability: How available and accessible your services are to usersConfidentiality: How you protect confidential information from a data breachProcessing integrity: How you ensure data is processed in a timely, accurate mannerPrivacy: How you keep user and customer data anonymous and protectedWell cover these Trust Services Criteria a bit more in-depth later, but first, lets answer a crucial question.Why does your organization need a SOC 2 report?SOC 2 compliance is not mandatory or legally required. However, if youre a service organization that directly affects users operational efficiency (e.g., cloud service provider, SaaS, data center, etc.) and you carry customer data, you probably need to become SOC 2 compliant.Why?Its likely that prospects and customers will request a SOC 2 report during vendor selection or for their own auditing processes. Not providing this report may stall sales cycles, affect credibility with customers, and hinder your ability to move upmarket.A SOC 2 audit will also help you better understand the current performance of your security controls and spot potential gaps. Youll be able to identify vulnerabilities, keep your organization safe, and build more efficient business processes.Some of the main benefits of SOC 2 compliance include:Build stronger client relationships: Committing to SOC 2 compliance proves to prospects, customers, and partners that you care about the security and integrity of their data.Prevent security incidents: A SOC 2 report will help you meet the highest security standards to avoid a data breach.Get valuable information about your business: Completing a SOC 2 audit will help you build a stronger security posture and give you valuable insights into the overall design and performance of your security controls.Who conducts a SOC 2 audit?SOC 2 examinations are attestation audits, which means an external, third-party auditor will assess your security controls and issue a final report about how well they meet SOC 2 requirements.This report typically includes:Audit summary: A summary of the audit scope, time period, and auditors final opinion regarding the organizations level of SOC 2 compliance.Management assertion: Organization leadership explains the systems and internal controls that are under audit.System description: A detailed overview of the system under audit, including system components, procedures, and incidents.Control tests: A description of the tests performed during the audit and the results.Keep in mind; SOC 2 examinations are governed by the AICPA and must be performed by a licensed and accredited CPA firm. The auditing firm must also be completely independent from the organization thats undergoing the audit to maintain objectivity.For more information on the who, what, and why of SOC 2, check out the video below from our compliance expert Chris Sesi or keep reading to dive into the readiness process.Get key assets youll need to get your SOC 2 report, including a compliance guidebook, customizable policy templates, readiness checklist, and more.Preparing for a SOC 2 audit without any guidance is like navigating a jungle without a map.To help you stay on track and avoid common pitfalls, weve put together a list of 35+ questions to prepare for a SOC 2 audit.This step-by-step guide will break down the entire process. Lets get into it!First, you need to understand the different types of SOC 2 reports to decide what you need right now.There are two types of SOC 2 reports: Type I and Type II.SOC 2 Type I reports assess your organizations controls at a single point in time. It answers the question: are your internal controls designed in a way that meets SOC 2 requirements? SOC 2 Type II reports evaluate the performance of your controls over a longer period of time, typically 6-12 months, but can be as little as 3 months.How do you decide which report type you need? Ask yourself:Which report type are your customers asking for? While some may accept a Type I report, most require a Type II.How urgently do you need a SOC 2 report? Type I audits are faster to complete and can satisfy customers while you pursue a Type II report.Do you have the resources to complete multiple audits? Some customers will accept a Type I report in the interim as you prepare for a Type II audit. If you opt to go straight for a Type II report, you will only need to complete one annual audit, rather than both a Type I and a Type II.As we stated earlier, SOC 2 audits assess your security controls against five Trust Services Criteria defined by the AICPA:SecurityAvailabilityProcessing integrityConfidentialityPrivacySecurity is the only TSC thats required for every audit. Thats why its often referred to as the common criteria. The other four TSC are optional. Youll need to decide which other TSC to include (if any) based on customer demands and specific industry regulations.For example, a cloud service provider might need to include the availability and security principles, while a payment processor system may need to include processing integrity and privacy.That said, we share some helpful questions for each principle below.SecuritySecurity is the only required principle by the AICPA, so you must pay special attention to the security controls you have in place to protect users sensitive information from unauthorized access.What are you doing to monitor and prevent cyber attacks and data breaches?Do you have specific procedures to monitor and respond to security incidents?Are your devices and applications updated on a regular basis?How do you handle vulnerabilities within your systems?Do you have defined backup and recovery procedures in place?Have you tested and documented your security procedures?Do you have defined access controls in place?AvailabilityAvailability refers to how accessible your system is for user operations. Often companies that need to be available and ready at all times for their customers will include availability within their scope. For example, if you offer payroll management services to large manufacturing companies, you must ensure that your system is available whenever your clients need it.Some helpful questions may include:Are your services available at all times?Are your services restricted to certain users?Do you have business continuity plans in place? How do you handle service issues that could affect your availability?Processing integrityProcessing integrity aims to help service users protect the integrity of their information. Companies that process a lot of data, and/or have a lot of integrations, such as Secureframe, will include processing integrity in the scope of their SOC 2. For example, if you offer a payment gateway service, your system must process customer data quickly, securely, and accurately.Are your processing systems working reliably?Are your processing systems providing timely, accurate data to users?How do you handle system failures and issues?Do you have specific procedures in place to correct errors quickly?ConfidentialityIf youre handling confidential customer information or helping customers manage their users sensitive information, ask yourself.How are you handling and processing data to ensure confidentiality?Is data protected and classified at all times?Do you have strict access controls in place to avoid unauthorized access?PrivacyPrivacy refers to the protection and anonymity of user information. If your company has a lot of sensitive information you may want to include privacy in your scope. Here are some helpful questions:Do you have a data retention policy in place?How and where do you classify, process, and store personal data?What controls are in place to protect personal data?Define the systems and controls you want to include in your audit and define why they matter from the users perspective. If youre pursuing a Type II report, youll also need to set an audit window.Whats the system in scope? (i.e., specific applications or databases, office locations, departments, etc.)For SOC 2 Type II, whats the audit window? A typical audit window is 6-12 months, but its possible to set a shorter, 3-month audit window. A longer audit window requires longer to be in compliance and more evidence to provide, however it also carries more weight than a 3-month report.Once you have defined the scope of your report, its time to identify risks and describe the actual controls youre going to test.Do you understand the risks associated with your information assets and systems?Have you identified the likelihood and potential impact of these risks on your organization?Do you have a risk treatment plan in place to accept or mitigate risks?How often do you perform risk assessments to identify changes in your threat landscape?How do you document and maintain internal controls to mitigate organizational risk?Do you have an access control policy in place to define who can access data and when?Do you maintain access logs to monitor activity and flag anomalies?Do any security controls rely on any third-party software? If so, what steps have you taken to manage vendor risk?A gap analysis can identify any weaknesses in your controls that could affect the outcome of your audit.The most efficient way to run a gap analysis is with an automated compliance tool, which can check all of your systems and controls against SOC 2 criteria to immediately flag any misconfigurations or gaps in your compliance posture. Platforms like Secureframe also offer tailored remediation guidance that make fixing any gaps quick and easy.If you dont opt for an automated tool, your internal compliance or information security team can manually check your controls to ensure compliance before your auditor begins their examination.A readiness assessment is an examination performed by the auditor to determine how prepared your organization is for a SOC 2 examination. This will help you better understand the current state of your organizations controls.A gap analysis and readiness assessment help you answer:Is your organization ready for a SOC 2 examination?Are your current controls sufficient to satisfy compliance requirements?Are there any gaps you need to fix prior to your SOC 2 examination?SOC 2 compliance may be exhaustive, but it doesnt have to be exhausting. Weve created a library of resources to demystify and simplify SOC 2:SOC 2 Compliance Hub: 35+ articles and resources that cover everything you need to know about SOC 2 audits.SOC 2 Compliance Kit: Free policy templates, compliance checklists, and evidence spreadsheets to save you hours of manual work.Expert advice and best practices: Our former auditors and compliance experts share their tips and answer common questions.Automated compliance: Continuous monitoring and evidence collection, vendor and personnel management, risk management, compliance dashboards, and much more to simplify and streamline SOC 2.What is SOC compliance checklist?A SOC 2 compliance checklist isa tool designed to help an organization evaluate its compliance with the SOC 2 framework and ensure it has completed the essential steps to prepare for a successful audit. Using the checklist, organizations can check off the boxes to visualize their level of audit readiness and quickly identify any gaps they need to remediate before undergoing an audit. How do I check my SOC 2 compliance?In addition to using a checklist to check your SOC 2 compliance, you can undergo a SOC 2 self-assessment or SOC 2 readiness assessment During a SOC 2 self-assessment, an organization maps existing information security controls and policies to their selected TSC, identifies any gaps, and creates a remediation plan ahead of their formal SOC 2 audit. A readiness assessment is similar except it's conducted by an auditor accredited by the American Institute of Certified Public Accountants (AICPA). Who is responsible for SOC 2 compliance?An organization may have a dedicated compliance team or individual that's responsible for SOC 2 compliance. This team or individual will work with the engineering team to ensure the technical controls are in place and the HR team to ensure the administrative controls are in place to achieve and maintain SOC 2 compliance. However, it's important that everyone at your organization understands their role and responsibilities in keeping your organization secure and compliant. The SOC 2 Compliance Checklist is a comprehensive tool used by organizations to ensure they meet the criteria set out in the Service Organization Control (SOC) 2 framework. This checklist covers five key trust service principles - security, availability, processing integrity, confidentiality, and privacy - and includes detailed requirements for each principle. By following the checklist, organizations can assess their systems and processes against industry standards, identify gaps in compliance, and implement necessary controls to meet SOC 2 requirements. This helps to enhance trust and confidence in the organization's services and demonstrates their commitment to protecting sensitive data and maintaining a secure environment for their customers. Download our SOC 2 Compliance Checklist to simplify your path to achieving SOC 2 compliance. This resource is designed to help your organization meet all the essential Trust Service Criteria, including Security, Availability, Processing Integrity, Confidentiality, and Privacy.Our checklist provides a step-by-step guide for SOC 2 audit preparation, covering crucial aspects like defining your audit scope, conducting risk assessments, implementing effective security controls, and gathering necessary documentation. Its the ideal tool for organizations looking to understand the SOC 2 compliance process.With this checklist, youll navigate each phase of the journey, from readiness assessment to receiving your final SOC 2 report. Download your free copy today to ensure a successful audit and maintain a strong security posture. With cloud-hosted applications becoming a mainstay in todays world of IT, staying compliant with industry standards and benchmarks like SOC 2 is becoming a necessity for SaaS firms. Therefore, getting SOC 2 compliance isnt a question of why as much as it is a when. With that in mind, heres a handy SOC 2 compliance checklist to help you plan and kickstart your compliance journey. But before we get into the SOC 2 checklist, lets understand the various nuances of the SOC 2 framework that will help you prepare better. Getting audit-ready involves months of preparation, planning, and ticking things off on a rather lengthy checklist. Defining a scope, choosing the right trust service criteria, implementing internal risk, and assessing controls these are just a few of your obligations before the reward is certification. Lets understand what each step under SOC 2 compliance checklist entails and also an easy shortcut at the end. TL;DRThe SOC 2 compliance process involves defining objectives, choosing the report type, conducting internal risk assessments, performing gap analysis, contacting an auditor, and more.Automating SOC 2 compliance processes, from policy creation to evidence collection, saves time and resources.Using automation tools for SOC 2 compliance will save you time and reduce costs associated with manual processes and potential non-compliance issues. The SOC 2 compliance checklist acts as a guide that helps organizations assess how customer data is collected, processed, stored, and accessed, thereby ensuring compliance with the Service Organization Control 2 (SOC 2) framework. The SOC 2 checklist also reviews vulnerability management and risk mitigation. The checklist enables organizations to meet SOC 2 requirements, demonstrating effective controls over customer information security, availability, processing integrity, confidentiality, and privacy. Implementing a SOC 2 checklist provides comprehensive coverage and simplifies the audit readiness process. It showcases your commitment to security, reassuring customers that their data is safeguarded. The SOC 2 audit prompts organizations to formalize and document policies, procedures, and controls. Documenting these essential practices significantly diminishes business risks, enhances vendor management, and frequently streamlines operational efficiency. A well-designed SOC 2 requirements checklist will lay out actionable steps organizations can take to meet the extensive criteria of the framework across security, availability, processing integrity, confidentiality, and privacy. Based on our experience of helping hundreds of businessesbecome SOC 2 compliant. Heres a 9-step SOC 2 checklist: 1. Choose your objectives 2. Identify the type of SOC 2 report you need 3. Define your SOC 2 scope 4. Conduct an internal risk assessment 5. Perform gap analysis and remediation 6. Implement relevant controls and test them 7. Undergo readiness assessment 8. Conduct the SOC 2 audit The first action item of the SOC compliance checklist is to determine the purpose of the SOC 2 report. The specific answers to why SOC 2 compliance is important to you would serve as the end goals and objectives to be achieved in your compliance journey. With a clear understanding of your objectives, you can ensure the SOC 2 process addresses your particular reasons for pursuing compliance. This clarity will help drive decision-making as you work through defining the scope, assembling a cross-functional team, evaluating controls, undergoing auditing, and taking necessary actions to remediate gaps. Your customers have asked for it You are entering a new geography, and SOC 2 compliance will add to your strength You want to bolster your organizations security posture to avoid data breaches and the financial and reputation damage that comes with it That said, not wanting SOC 2 compliance because customers arent asking for it or because none of your competitors has it isnt advisable. Its never too early to get compliant. And its always an advantage to be proactive about your information security. Also read: How to make compliance your superpower SOC 2 reports can be Type 1 or Type 2. You decide which one is appropriate based on your compliance goals. A Type 1 report is faster, but only reflects the performance of controls at a point in time and affirms that your internal controls are in place. Type 2 confirms that the controls are working as expected when tracked over a period of time, and it is likely that you will be asked to produce a Type 2 audit report shortly after. It is comprehensive and demands a control monitoring period that can be as long as 6 months, but it produces a more vivid picture of the performance of your security controls. Defining the scope of your audit is crucial as it will demonstrate to the auditor that you have a good understanding of your data security requirements as per SOC 2 compliance checklist. It will also help streamline the process by eliminating the criteria that dont apply to you. You must define the scope of your audit by selecting the TSC that applies to your business based on the type of data you store or transmit. Note that Security as a TSC is a must. Regulatory requirements will also have a bearing on your criteria selection. That said, in our experience, most SaaS businesses typically only need Security, Availability and Confidentiality (or their combination) as TSC in their SOC 2 journey. Choose Availability if your customers have concerns about downtime. Choose Confidentiality if you store sensitive information protected by non-disclosure agreements (NDAs) or if your customers have specific requirements about confidentiality. If you execute critical customer operations, such as financial processing, payroll services, and tax processing, you should include processing integrity. Include Privacy if your customers store PII (Personally Identifiable Information) such as healthcare data, birthdays, and social security numbers. On that note, a bad example here would be leaving a relevant TSC out of your SOC 2 scope. Such oversight could significantly add to your cybersecurity risk and potentially snowball into substantial business risk. A SOC 2 audit looks at your infrastructure, data, people, risk management policies, and software, to name a few items. So, at this stage, you must also determine who and what within categories will be subject to the audit. For instance, you can keep some of your non-production assets from the scope of the audit. Risk assessment is crucial in your SOC 2 compliance journey. You must identify any risks and document the scope of those risks from identified threats and vulnerabilities. Assign a likelihood and impact to each identified risk and then deploy measures (controls) to mitigate them as per the SOC 2 checklist. Once you have identified the risks, score them based on its impact and likelihood of that risk scenario actually playing out. A common mistake organizations make in this stage is scoring risks based on guts rather than reality. A better, auditor approved way of scoring risks is by using industry grade benchmarks. A compliance automation platform like Sprinto builds a true, up-to-date inventory of assets and gives you the tools and capabilities to define risks at an asset level. Using its comprehensive risk register, you can identify, risks associated with your assets. You must examine your current control status and security practices and compare their compliance posture with how they measure against SOC requirements. A compliance automation tool like Sprinto can make this process a lot easier by integrating with your applications and scanning the environment for control gaps and vulnerabilities. From a single dashboard, you can view the health of all controls, risks, and issues that require your attention. The auditor-friendly dashboard also allows you to automatically collect compliance evidence. Following gap assessment, implement controls to meet compliance and keep asset security in check. These may include modifying security workflows, introducing employee training modules, and creating new process documentation, among others. The risk ratings (carried out earlier) will help you prioritize controls. Once you have implemented the control, test them for its effectiveness. This is a critical part of SOC 2 Type 2 because here the auditor tests if the controls are working as they should. Common issues you may face at this stage is not remediating or not getting alerted on failing controls on time and overlooking non-compliance issues which puts you at the risk of not meeting auditor expectations. You can resolve these using a tool like Sprinto that automatically maps risks to compliance criteria and controls, launches automated checks to test controls, and monitors their health on a central dashboard. When anomalies are detected, trigger alerts and remediation workflows to the appropriate risk owners. Context-rich, time-bound alerts ensure timely resolution throughout the risk lifecycle, preventing issues from escalating. Get a demo now to see Sprintos live control dashboard. Undertake a readiness assessment to see if you meet the minimum SOC compliance requirements to undergo a full audit. Here are your focus areas for the assessment: Gap analysis It aims to detect vulnerabilities and gaps and generate a list of specific recommendations and actions. It takes around 2-4 weeks from start to finish. Controls matrix It lists the objectives map, internal controls identification, and control characteristics. Auditor documentation It involves drafting the request list for auditors and testing procedures. Based on the auditors findings, remediate the gaps by remapping some controls or implementing new ones. Even though technically, no business can fail a SOC 2 audit, you must correct discrepancies to ensure you receive a good report. Readiness assessment involves writing policies, linking checks to the right control, evaluating risks without leaving any gaps, and collecting evidence accurately. Doing these manually leaves a lot of room for error and derail the audit process. Sprinto helps you add momentum to compliance activities by offering pre-built templates, pre-mapped controls, automated evidence collecting system, and dedicated auditor dashboard. Get SOC 2 compliant with ease. Talk to our experts today! Authorize an independent certified auditor to complete your SOC 2 audit checklist and generate a report. While SOC 2 compliance costs can be a significant factor, choose an auditor with established credentials and experience auditing businesses like yours.In your Type 2 audit, you may expect a long-drawn exchange of information with the auditor as you answer their questions, provide evidence, review your internal samples, and discover non-conformities. Typically, SOC 2 Type 2 audits may take between two weeks to six months, depending on the volume of corrections or questions the auditor raises. Type 2 has a mandatory monitoring period of three-six months. A Type 2 report, therefore, offers more significant insights into your organizations controls and its effectiveness. Here are some questions the auditor may ask: Can you share evidence to show that all your employees undergo background verification? Can you show proof of how you ensure that the changes in your code repositories are peer-reviewed before it is merged? Can you demonstrate with evidence that you remove access to emails and databases once an employee resigns from your organization? Can you show proof that you run background checks on all your employees? Can you share proof of how you maintain the endpoint security of all systems? The audit for Type 1, in comparison, doesnt require a monitoring period, is less intrusive, and requires you to give a snapshot (with evidence) of the various checks and systems (read as controls) you have put in place to meet the SOC compliance checklist requirements. Note that after you clear your SOC 2 Type 1 audit, you will need to go through an observation period of three-six months before you can apply for Type 2. Getting your SOC 2 compliance report isnt just a one-time event. The report is just a start as security and compliance are on-going efforts . It pays to establish a robust continuous compliance monitoring practice as SOC 2 audits must happen annually. Continuous compliance makes future audits and scaling scope of compliance easy. when you operate with the assurance of compliant practices, you can add more frameworks without disrupting the practice or the org at large. Your monitoring practices should be scalable to grow with your organization, simplify evidence collection, not hamper employee productivity, alert you of non-compliant activities, and paint an accurate picture of entity-level granular overview of your infosec health at any point in time. Monitoring IT infrastructures manually, without the right tools creates gaps, eats up bandwidth, and results in last-minute surprises. Avoid these pitfalls and ensure audit success by continuously, automatically, and comprehensively monitoring your assets and controls for compliance with GRC automation tools like Sprinto. See Sprinto in action Continuous SOC 2 Compliance Made Easy When going through a SOC 2 audit, your organization will be evaluated based on five Trust Service Criteria (TSC) defined by the AICPA. To properly prepare, you should review your internal controls and procedures to ensure they address each of these criteria. Here are some tips for aligning your SOC 2 readiness checklist with the TSC: It must be in scope for every SOC 2 audit and is, therefore, referred to as the common criteria. It requires you to enable access control, network firewalls, and other operational/governance controls to protect your data and applications. Enable entity-level controls that establish baseline security policies. Requires you to demonstrate that your systems meet operational uptime and performance standards. So, implement monitoring for system uptime and performance. Have disaster recovery and incident response processes ready as well. Shows how you safeguard sensitive data throughout its lifecycle. Implement access controls so only authorized users can access data. Have quality assurance checks to validate the accuracy and reliability of data processing. Monitor systems to ensure timely processing and intended outcomes. It includes quality assurance procedures and SOC tools to monitor data processing. Requires you to protect Personally Identifiable Information (PII) from breaches and unauthorized access through rigorous access controls, two-factor authentication, and encryption. Achieving SOC 2 compliance is a major undertaking that comes with some substantial challenges. One hurdle is the time-intensive process of thoroughly documenting all controls, policies, and procedures to SOC 2 standards. You can expect this to take quite some time and effort. There will also likely be costs associated with making required updates to infrastructure or systems to meet compliance criteria. Even after achieving compliance, the work doesnt stop. Maintaining SOC 2 requires rigorous ongoing internal control audits. With strict standards to meet, the process of becoming compliant is far from easy. However, for organizations handling critical customer data, the effort is worthwhile to gain trust and demonstrate security commitments.The Sprinto Advantage: With the help of the SOC 2 automation platform, you can streamline the whole process to eliminate manual repetitive tasks. Talk with Sprintos experts to know more about SOC 2 automation and beyond.Did you know that 95% of companies are trying to build a culture of compliance, but they struggle to translate that culture into their day-to-day work? If you're developing an application interacting with client data, data protection, and code security should be baked in from day zero. DevOps teams must continuously follow secure coding practices and use various security tools to conduct vulnerability assessments and testing. Product and security teams should also embed all the necessary tools and processes into their services, ensuring no gaps get to production. To bridge the security gap, various frameworks can be used, with SOC 2 being the most popular framework for auditing organizations that develop SaaS products or offer online services. Although not mandatory, SOC 2 compliance helps companies improve and prove their security posture.In this article, we focus on what it takes to achieve SOC 2 compliance and provide a downloadable checklist to help companies stay on track.What Is SOC 2?System and Organization Controls (SOC), is a set of frameworks developed by the American Institute of Certified Public Accountants (AICPA) to evaluate and improve the security, availability, processing integrity, confidentiality, and privacy of confidential customer data that organizations store and process. There are three SOC frameworks available: SOC 1 covers accounting and financial reporting;SOC 2 and SOC 3 are more focused on cybersecurity, making them ideal for software development companies;SOC 3 is aimed at the general public and is much less detailed than SOC 2. While it is an American standard, SOC 2 is globally regarded as a minimum requirement for online service providers, SaaS developers, and data processing and storage providers. Proof of SOC 2 compliance may be demanded by security-conscious customers and stakeholders looking to gain confidence in the information security practices of a business entrusted with sensitive customer data. From a software and data security perspective, SOC 2 compliance can be a way to begin putting the Sec in DevSecOps and shifting security left in any growing software development business or initiative. Even if your organization doesnt immediately require a SOC 2 compliance certification, understanding and closing the security gaps in your SDLC is critical to improving your security posture. This is how your approach to security compliance is destroying dev cultureHow Does the SOC 2 Audit Work?SOC 2 typically focuses on security, and looks to analyze how vulnerable your systems are to cyber threats, the processes you use to secure your systems and customer data, and how you implement security best practices across your organization. The official audit comprises five criteria, which we discuss in detail below. Each measure has a set of controls, and you could look at between 80 to 100 controls.SOC 2 audits may all look very differentthere is also no one-approach-fits-all when preparing for it. However, you should take some common best steps to ensure youre as prepared as possible and the official audit goes smoothly.Choose your SOC 2 typeUnderstand the SOC 2 Trust Service CriteriaDetermine your scopeReview your security controlsClose control gapsImplement control maintenanceUndergo the official SOC 2 auditOnce the audit is complete, you get a SOC 2 report which you can share with relevant stakeholders and customers and use internally to improve the safety and stability of your systems continuously.The Complete SOC 2 Compliance Checklist1. Choose Your SOC 2 TypeThe first step on your SOC 2 compliance journey is selecting the type of SOC 2 audit your business needs.SOC 2 audit reports come in two flavors:Type 1: With SOC 2 Type 1, your auditor will review policies, procedures, and control evidence at a specific time to determine if controls suit the applicable SOC 2 criteria. Type 2: With Type 2, the process is more rigorous, and the report is more insightful as it considers your security controls' past and present effectiveness.Though SOC 2 Type 1 is not a prerequisite for the Type 2 report, organizations typically complete a