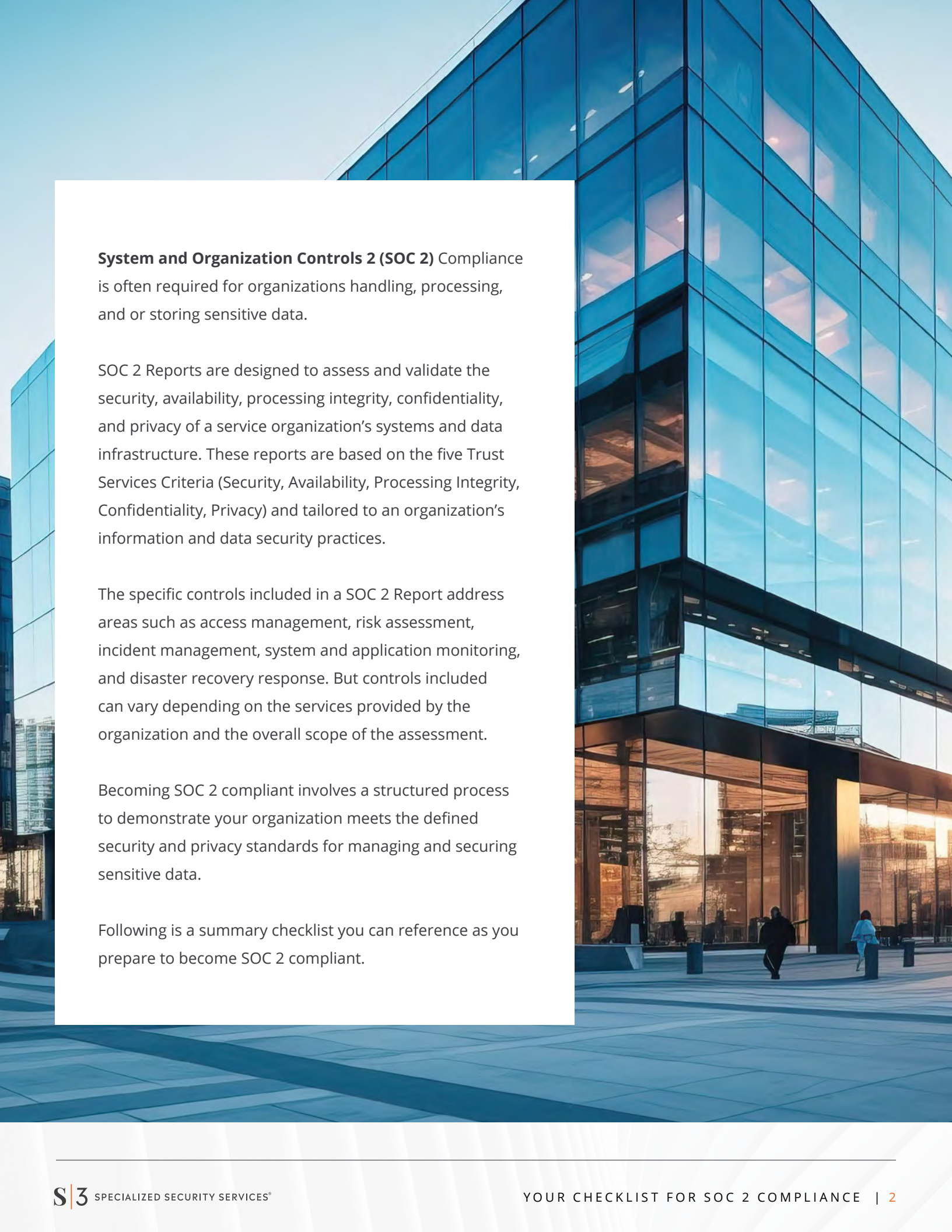


S|3 SPECIALIZED SECURITY SERVICES

YOUR CHECKLIST FOR SOC 2 COMPLIANCE



System and Organization Controls 2 (SOC 2) Compliance is often required for organizations handling, processing, and or storing sensitive data.

SOC 2 Reports are designed to assess and validate the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems and data infrastructure. These reports are based on the five Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy) and tailored to an organization's information and data security practices.

The specific controls included in a SOC 2 Report address areas such as access management, risk assessment, incident management, system and application monitoring, and disaster recovery response. But controls included can vary depending on the services provided by the organization and the overall scope of the assessment.

Becoming SOC 2 compliant involves a structured process to demonstrate your organization meets the defined security and privacy standards for managing and securing sensitive data.

Following is a summary checklist you can reference as you prepare to become SOC 2 compliant.



1. UNDERSTAND THE SOC 2 FRAMEWORK

SOC 2 is based on five Trust Service Criteria (TSC):

- » **Security:** Protection against unauthorized access (both physical and logical).
- » **Availability:** Systems should be available for operation and used as agreed.
- » **Processing Integrity:** System processing must be complete, accurate, timely, and authorized.
- » **Confidentiality:** Sensitive data must be protected per agreements or policies.
- » **Privacy:** Personal information must be collected, used, retained, and disclosed in conformity with privacy laws and regulations.

Each of these criteria should be addressed within your organization to demonstrate secure management standards of your data.

2. ASSESS CURRENT PRACTICES

Conduct an internal assessment to determine your organization's current security and privacy practices and identify gaps against SOC 2 standards. A gap analysis/readiness assessment can help you understand where improvements are needed.

3. DEFINE YOUR SCOPE

Determine which areas of your organization will be included in the SOC 2 assessment. You might choose to focus on specific departments (e.g., IT and HR) or specific systems (e.g., customer databases and software applications).

4. IMPLEMENT NECESSARY CONTROLS AND POLICIES

Establish policies and procedures to ensure that the Trust Service Criteria are met. These may include:

- » **Access Control:** Policies to restrict unauthorized access to data.
- » **Incident Response:** Procedures for managing security breaches and other incidents.
- » **Data Encryption:** Protecting sensitive data through encryption.
- » **Network and Application Monitoring and Logging:** Ensuring systems and applications are regularly monitored and logs are maintained for auditing purposes.
- » **Employee Training:** Training staff on security and privacy requirements.
- » **Third-Party Risk Management:** Ensuring that vendors and partners adhere to appropriate security frameworks (e.g., PCI DSS, SOC 2, etc.).



5. THOROUGH DOCUMENTATION

Documentation is critical for SOC 2 compliance.

You'll need to create clear and comprehensive records of your controls, policies, procedures, and any actions taken to meet the criteria. This will be crucial for the assessment process.

6. CONDUCT AN INTERNAL ASSESSMENT OR SOC 2 READINESS ASSESSMENT

Before undergoing the official assessment, conduct a mock internal assessment and review. This can help you identify any remaining gaps in your controls or documentation and provide an opportunity to address them before the formal assessment. It may be advisable to contract with a qualified assessing organization to perform a SOC2 readiness assessment to help you identify and report on control gaps.





7. UNDERGO THE SOC 2 ASSESSMENT

During the assessment, the auditor will review your organization's systems, policies, procedures, and controls to ensure they are designed and operating effectively.

There are two types of SOC 2 reports:

- » **Type I:** Evaluates the design of controls at a specific point in time.
- » **Type II:** Evaluates both the design and the operating effectiveness of controls over a longer period (usually 6-12 months).

8. REVIEW THE SOC 2 REPORT

After the assessment, the auditor will provide a signed SOC 2 report, typically called an Opinion Letter. Review this report thoroughly to ensure that it accurately reflects your organization's compliance status. This report can then be shared with stakeholders, clients, and partners to demonstrate your commitment to security and privacy.



9. MAINTAIN AND CONTINUOUSLY IMPROVE COMPLIANCE

SOC 2 compliance is not a one-time process. It requires continuous monitoring and improvement of your organization's controls and practices to ensure they remain effective. You should regularly review and update your security policies and controls – especially in response to changes in the threat landscape or your organization's operations.



KEY CONSIDERATIONS FOR SOC 2 COMPLIANCE

» Automation

Use tools to automate certain security tasks like monitoring, patching, and data backups.

» Risk Management

Continuously assess and mitigate risks to your systems, applications, and data.

» Third-Party Security

Ensure any third-party vendors and contractors adhere to appropriate security frameworks (e.g., PCI DSS, SOC 2, etc.).

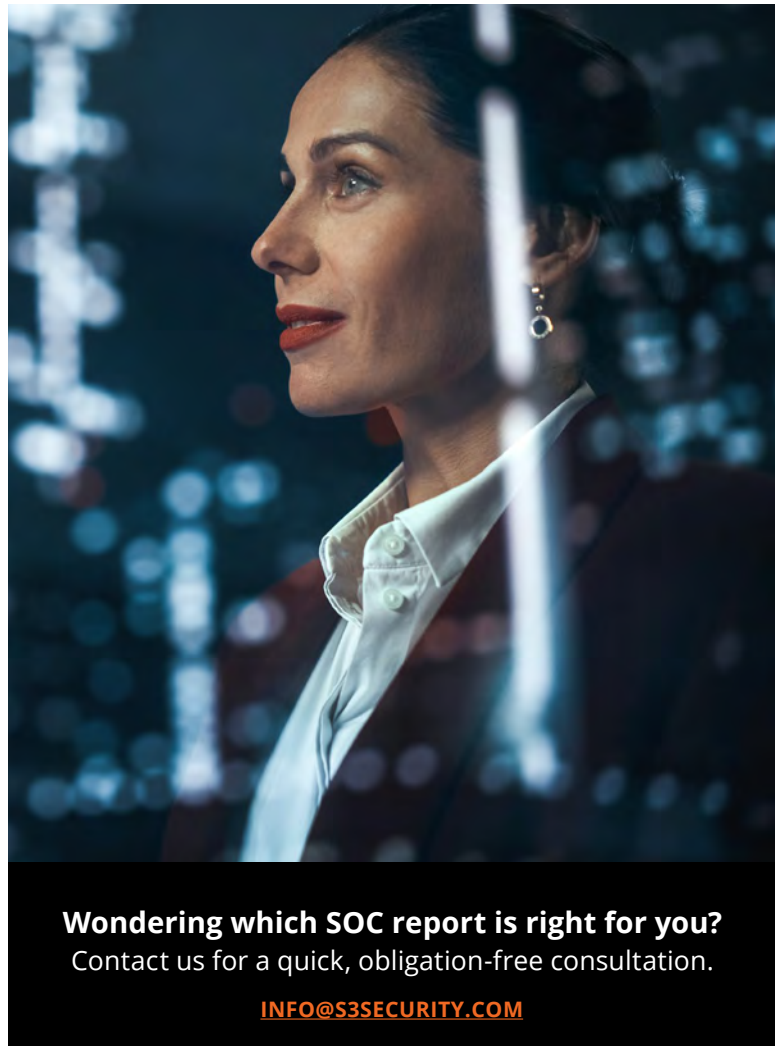
» Employee Awareness

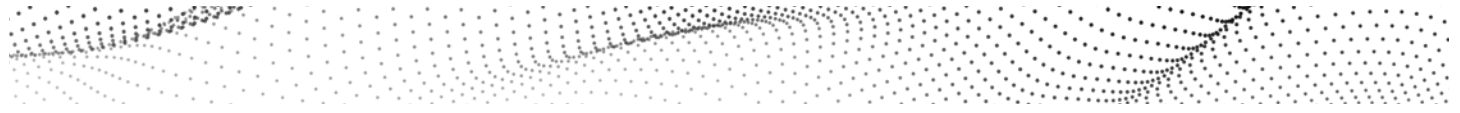
Continuous training and communication about security policies for all organization staff members.

In summary, following the steps above will help prepare your organization to work toward becoming SOC 2 compliant, enhancing your organization's security and privacy posture.

If you're planning to perform a certified SOC audit, you'll also need a partner who can make the process as simple and effortless as possible. S3 Security fits the bill – applying the same principles, protocols and practices that have led to thousands of other successful compliance assessments and made us a leader in cybersecurity.

Our senior leadership collaborate with your team and one of America's Top 100 CPA firms to assess the systems, policies and procedures in place to safeguard data across your information architecture and digital ecosystem. Together, we then evaluate the evidence you've provided regarding controls in each category to deliver your certified SOC 2 report.





S3 SECURITY SOC 2 GUIDE

EXAMPLES OF TSP CONTROLS

Security Controls

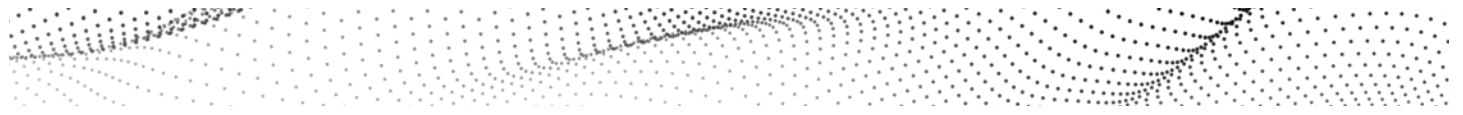
These are measures that ensure systems are protected against unauthorized access, both physical and logical.

- » **Access Controls:** Authentication and authorization procedures (e.g., Multi-factor authentication (MFA), role-based access control (RBAC)).
- » **Firewall Configuration:** Firewall rules are in place to protect network boundaries and restrict unauthorized access.
- » **Intrusion Detection/Prevention Systems (IDS/IPS):** Tools to detect and prevent unauthorized access to the system.
- » **Encryption:** Encryption of data both at rest and in transit to ensure data protection and confidentiality.

Availability Controls

These focus on ensuring that the system is available for operation and use as agreed upon by the service provider.

- » **Incident Response Plans:** Procedures for responding to system downtimes, including recovery measures and communication plans.
- » **Monitoring and Alerts:** Systems in place to monitor the availability of the service and detect outages or performance issues.
- » **Backup Procedures:** Regular backups of critical systems and data, with periodic testing of recovery processes.



Processing Integrity Controls

These controls ensure that system processing is complete, accurate, timely, and authorized.

- » **Data Validation:** Checks to ensure data input and processing are accurate, complete, and consistent.
- » **Change Management Procedures:** Controls to ensure that all changes to the system are properly reviewed, tested, and documented.
- » **Error Handling and Logging:** Automated and manual controls to detect and correct errors in processing.

Confidentiality Controls

These ensure that data classified as confidential is protected from unauthorized disclosure.

- » **Data Classification and Handling:** Policies and procedures to classify and handle data based on sensitivity (e.g., PII, financial data).
- » **Access Control to Confidential Data:** Restricting access to sensitive information based on roles, ensuring only authorized personnel can access specific data.
- » **Encryption of Sensitive Data:** Ensuring that sensitive data, like customer information, is encrypted during storage and transmission.

Privacy Controls

These controls focus on how personal information is collected, used, retained, and disclosed.

- » **Privacy Policy:** A documented policy outlining how personal information is handled, including collection, storage, sharing, and deletion practices.
- » **Data Minimization:** Collecting only the necessary amount of personal data for the intended purpose.
- » **Third-Party Risk Management:** Ensuring that third-party service providers also adhere to privacy policies and practices.