MITRATECH
Prevalent

AICPA Trust Services Criteria & Third-Party Risk Management

A Checklist for SOC 2 Compliance

AICPA Trust Services Criteria & Third-Party Risk Management

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) developed trust services criteria for organizations to use as a framework for demonstrating the confidentiality, integrity and availability of systems and data. Organizations familiar with System and Organization Control (SOC) 2 audits will recognize that these trust services criteria are used to report on the effectiveness of their internal controls and safeguards over infrastructure, software, people, procedures, and data.

With technology outsourcing becoming ever more widespread, organizations must ensure that their third-party vendors store, process, and maintain data in accordance with the highest levels of security control.

This guide examines controls and guidance in the AICPA standard and identifies capabilities in the Mitratech Third-Party Risk Management Platform that can be used to meet SOC 2 requirements for stronger data security throughout the supply chain.

Once the controls audit is complete, outputs can include either a Type 1 report, which looks at a service provider's system and the suitability of the design of controls at a point in time; **or a Type 2 report,** which adds to the Type 1 report by also looking at the operating effectiveness of controls over a period of time.

Organizations across multiple industries use SOC 2 reports to demonstrate due diligence to clients, differentiate themselves from competitors based on their security posture, or be proactive with auditors in measuring compliance against data protection regulations.

However, with 61 criteria across more than 300 points of focus, it can quickly become overwhelming for organizations standardizing on a SOC 2 report to understand how to evaluate third parties for control weaknesses that could result in a business disruption.

Trust Services Criteria in SOC 2 Reports

SOC 2 audits provide a comprehensive view into the following AICPA trust services categories:

- **Security:** Protecting information and systems against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Availability:** Ensuring the availability of information and systems for operation and use to meet the entity's objectives.
- **Processing integrity:** Ensuring that system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality:** Protecting information designated as confidential to meet the entity's objectives.
- **Privacy:** Ensuring that personal information collected, used, retained, disclosed, and disposed meets the entity's objectives.

Mapping Prevalent Capabilities to AICPA Trust Service Criteria for SOC 2 Reporting

Many companies have third parties that choose to submit SOC 2 reports instead of complete third-party risk assessments, so it's important to consistently evaluate all vendors. The summary table below maps capabilities in the Prevalent Third-Party Risk Management Platform to select AICPA trust services criteria. Organizations can leverage the Prevalent platform to understand and mitigate risks, regardless of how risks are reported.

NOTE: *This table should not be considered definitive guidance. For a complete list of controls, please review the complete AICPA standard in detail and consult your auditor.*

Trust Services Criteria	How Prevalent Helps
CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
Communicates Objectives Related to Confidentiality and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality. **Communicates Objectives Related to Privacy and Changes to Objectives** — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.	The Mitratech Third-Party Risk Management (TPRM) Platform centrally manages dialogue about risks, reporting and remediations between organizations and their third-party vendors, suppliers and partners. In addition, the Platform enables reporting, policy documents, contracts and supporting evidence to be stored for dialogue, attestation and sharing. Together, these capabilities ensure that organizations have a single repository for visualizing and managing risks, vendor documentation and remediations.
CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	The Mitratech TPRM Platform enables organizations to automate the critical tasks required to assess, manage, continuously monitor, and remediate thirdparty security, privacy, compliance, supply chain and procurement-related risks across every stage of the vendor lifecycle – from onboarding to offboarding. The solution includes the ability to issue and manage point-in-time risk assessments using more than 75 different templates, analyze the results, as well as continuously monitor third-party cyber, business, reputational, and financial risks for a holistic view of third parties. Built-in reporting templates ensure that security and risk management teams can communicate risk assessment results to executives and other decisionmakers and stakeholders.

Trust Services Criteria	How Prevalent Helps
CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.	
Assesses Changes in Vendor and Business Partner Relationships — The risk identification process considers changes in vendor and business partner relationships.	Customizable surveys and workflows help you report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more during offboarding to ensure that as agreements change, so do responsibilities. Contract Essentials, a solution that centralizes the distribution, discussion, retention, and review of vendor contracts, includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding.
CC9.2: The entity assesses and manages risks associated with vendors and business partners.	
Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	Contract Essentials helps vendor management, procurement, and legal teams simplify the process of establishing and negotiating contract terms and SLAs, managing redlines, and securing approvals through workflow. The solution is fully integrated with the complete TPRM Platform ensuring that organizations can manage vendor contracts with the same discipline that they manage vendor risks.
Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners..	With the Mitratech Platform, security and risk-management teams can manually assign tasks related to managing assessments risks, or leverage a pre-packaged library of ActiveRules to automate a range of tasks normally performed as part of the assessment and review processes – such as updating vendor profiles and risk attributes, sending notifications, or activating workflow – utilizing if-this, then-that logic.
Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.	The Platform enables vendor management teams to establish requirements to track and to centralize SLA and performance reporting against those requirements through a single reporting and analytics dashboard.
Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing issues identified with vendor and business partner relationships.	The Platform features reporting that reveals risk trends, status and exceptions to common behavior for individual vendors or groups with embedded machine learning insights. With this capability, teams can quickly identify outliers across assessments, tasks, risks, etc. that could warrant further investigation.
Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.	The Platform leverages customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more during offboarding.

Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements. **Assesses Compliance with Privacy Commitments of Vendors and Business Partners —** On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	The Platform enables risk management and compliance teams to automatically map information gathered from controls-based vendor assessments to regulatory frameworks including ISO 27001, NIST, CMMC, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, SOX, NYDFS, and more to quickly visualize and address important compliance requirements.
P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	
Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	Mitratech offers built-in assessments for data protection regulations such as GDPR, CCPA, HIPAA, and NYDFS. Results from these assessments are mapped into a central risk register where security and risk management teams can visualize and take action on potential risks to data and compare a vendor's actions against their contractual obligations.
Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The Mitratech Platform includes built-in remediation guidance and recommendations. Security and risk management teams can efficiently communicate with vendors and coordinate remediation efforts through the Platform, capture and audit conversations, and record estimated completion dates.
P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.	
Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information. **Reports Actual or Suspected Unauthorized Disclosures —** A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.	The Third-Party Incident Response Service enables security and risk management teams to rapidly identify and mitigate the impact of data privacy incidents by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.

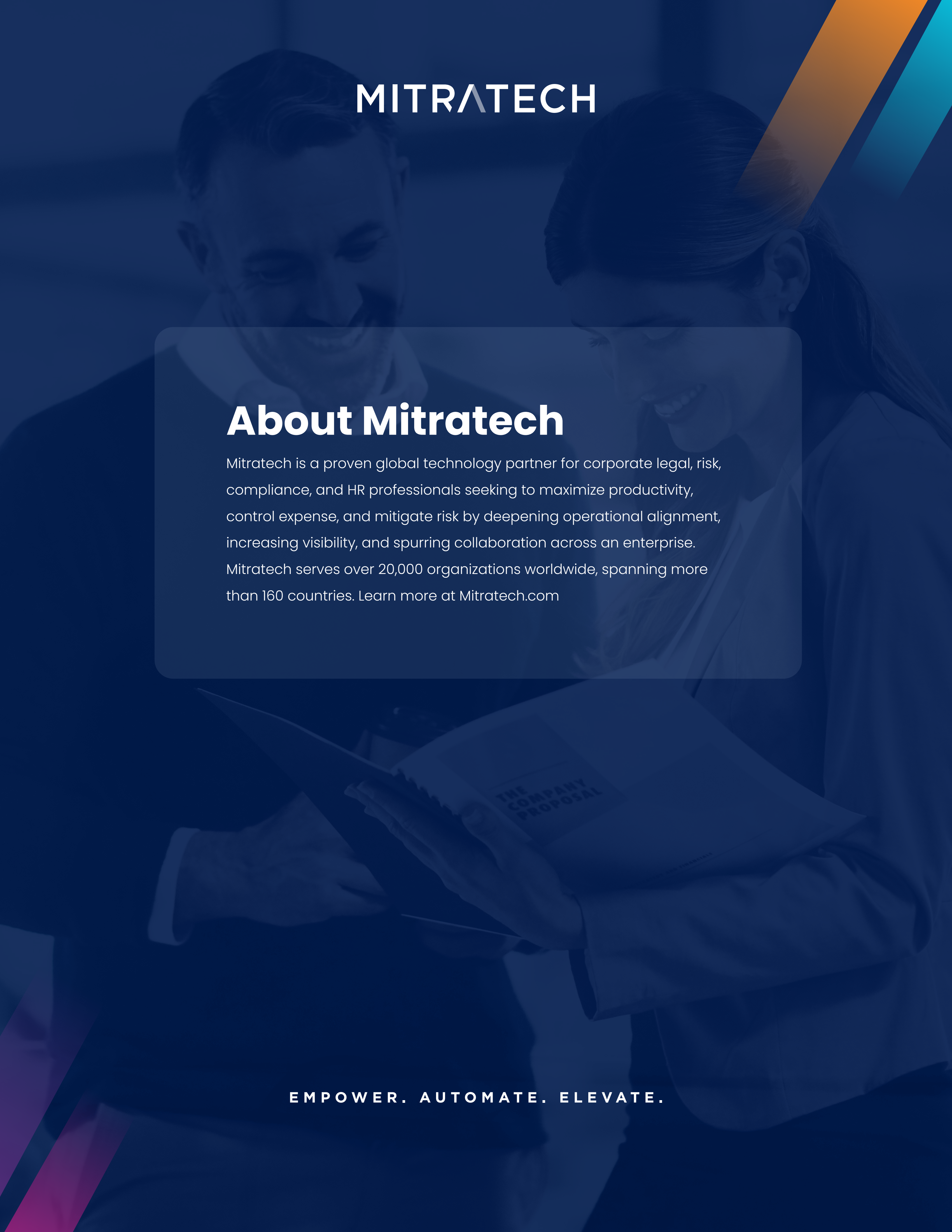
The Mitratech Difference

The AICPA SOC 2 report is an industry-standard framework for IT services companies to assess their controls over customer data. Since some organizations that lack internal resources for responding to security assessments will provide a SOC 2 report to their customers instead, it can be time consuming and complex for teams to map SOC 2 report results into a risk management solution for proper risk tracking.

The SOC 2 Report Review Service is a managed service delivered by the Risk Operations Center (ROC) that transposes SOC 2 report control exceptions into risks in the Third-Party Risk Management Platform. The resulting unified risk register enables coordinated risk response and remediation following a standardized approach and ensures that you have a comprehensive profile of all vendors – even for those that submit a SOC 2 report in lieu of a full security assessment.

Contact us today for a free maturity assessment to determine how your current TPRM policies stack up to the AICPA trust services criteria, or, learn more about how Mitratech Prevalent can help simplify SOC 2 report reviews.

Get In Touch



MITRATECH

About Mitratech

Mitratech is a proven global technology partner for corporate legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across an enterprise. Mitratech serves over 20,000 organizations worldwide, spanning more than 160 countries. Learn more at Mitratech.com

EMPOWER. AUTOMATE. ELEVATE.