INDEX

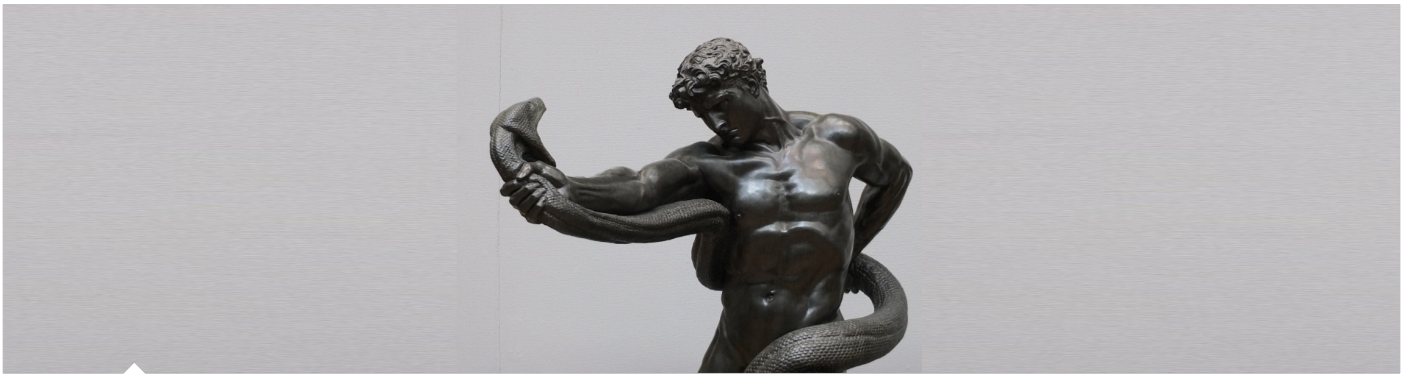


Photo Credit: An Athlete Wrestling with a Python (1877) by Sir Frederic Leighton (1830-1896) at the Tate, London

SOC2

How to get a CPA attestation report on each service organization's information security controls, so salespeople can close faster with prospective customers by providing a SOC 2 Type II report.

OVERVIEW

NOTE: Content here are my personal opinions, and not intended to represent any employer (past or present). "PROTIP:" here highlight information I haven't seen elsewhere on the internet because it is hard-won, little-know but significant facts based on my personal research and experience.

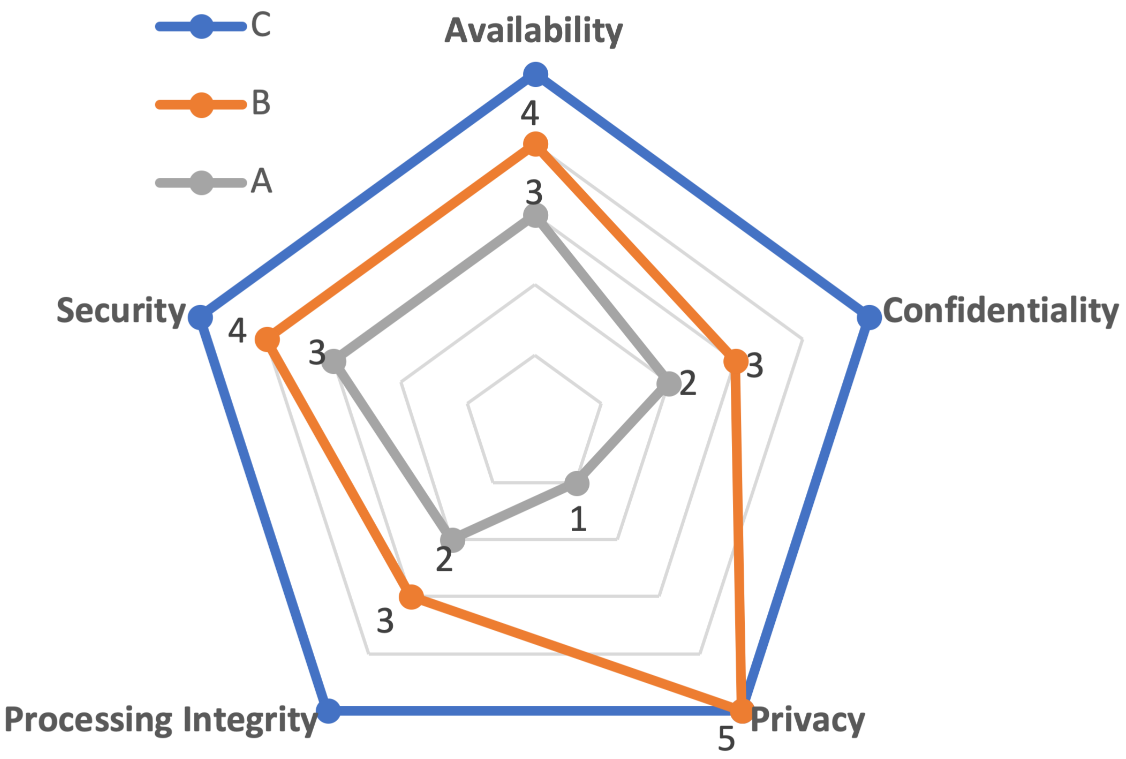
Why?

VIDEO: Summary A SOC 2 audit is not a legal or regulatory requirement like HIPAA, PCI DSS, or SOX.

PROTIP: Preparing for and conducting a SOC2 audit "pays for itself" because, by strengthening the organization's overall security posture, the effort lowers the potential impact of a security breach. The effort also decreases sales cycles and increases win rates. Cloud salespeople report that it is "table stakes" to provide a **SOC2 Type II report** to prospects. The document contains an attestation from a CPA firm hired by each service provider to evaluate and attest that there is proof the service provider indeed has measures in place to protect the integrity, confidentiality, and privacy of data on behalf of customers. This is done typically each year.

Status Summary

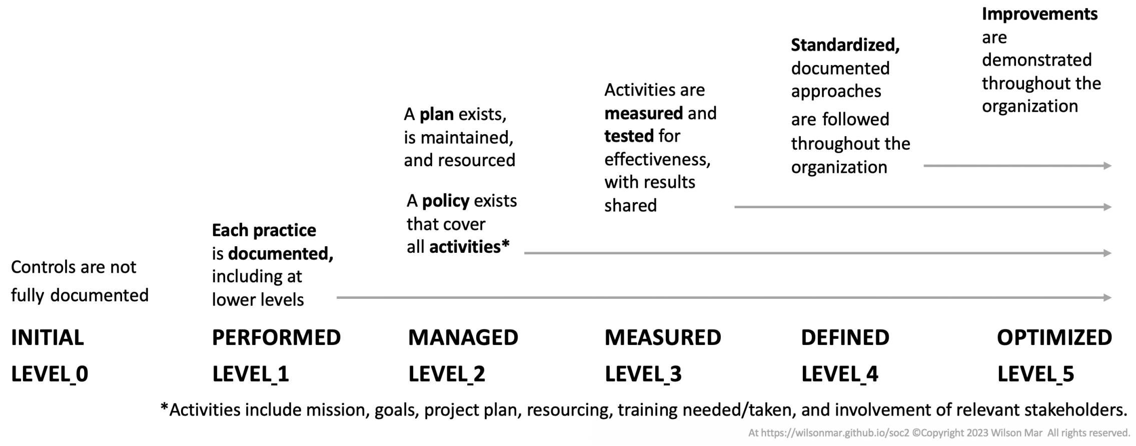
Our organization's status toward achieving the five TSCs (Trust Services Criteria) for SOC2 developed by the AICPA Assurance Services Executive Committee (ASEC) is summarized in (this polar chart, with a line for each moment of time, starting from A to B to C at completion: SAMPLE:



VIDEO: This chart summarizes several charts for each part of our organization.

Maturity Model Levels

Levels for rating status are adapted from this SOMM (Security Operations Maturity Model) illustration:



Controls are not fully documented

Each practice is **documented,** including at lower levels

A **plan** exists, is maintained, and resourced

A **policy** exists that cover all **activities***

Activities are **measured** and **tested** for effectiveness, with results shared

Standardized, documented approaches are followed throughout the organization

Improvements are demonstrated throughout the organization

INITIAL **LEVEL_0**

PERFORMED **LEVEL_1**

MANAGED **LEVEL_2**

MEASURED **LEVEL_3**

DEFINED **LEVEL_4**

OPTIMIZED **LEVEL_5**

*Activities include mission, goals, project plan, resourcing, training needed/taken, and involvement of relevant stakeholders.

At https://wilsonmar.github.io/soc2 ©Copyright 2023 Wilson Mar All rights reserved.

- 0 = INITIAL = Controls are not fully documented.
- 1 = PERFORMED = Controls **documented** for each practice
- 2 = MANAGED = Controls also **follow plans and policies**
- 3 = MEASURED = Controls also **measured and tested**
- 4 = DEFINED = Controls also **standardized**
- 5 = OPTIMIZED = Controls also (“continuosly”) **improved**

BTW, an alternative is CMMC maturity model rating which was deprecated in 2021 in favor of a "Fundamental, Advanced, and Expert" levels.

Org Levels

When considering that there are 17 COSO Principls, that's 17 x 3 x 4 = 204 items for an organization with 4 levels.

- Executive (Leadership) & Finance (Budget)
- Marketing & Sales (to prospects and customers)
- Legal, HR, PR, IAM & SOC teams
- Operations & R&D - Physical & Digital Infrastructure

Please refer to the spreadsheet/database of people, their role in the organization, and other metadata.

Who Does What

Who	Deliverables	# Walkthroughs	Auditor Hours
Sales & Marketing	Timeline, Description of product/service in auditor reports	1-2	4-8
Leadership	Auditor agreement, Assertion of Mangement in Draft auditor reports	1-2	4-8
Legal, HR, PR	Customer Agreements, Employee Policies & Agreements, Breach Communications	1-2	4-8
Security SOC	Risk management, Business Continuity, Monitoring, Malware detection, Audit & Compliance	1-2	10-20
Facilities	Facilities Access Control, Asset Management	1-2	1-2
Info technology Operations	Security Operations (Security Policies, Network security), Data Security (in IT Operations), Information & Communications	1-2	10-20
Engineering, DevSecOps, Development	Systems Access Control, SDLC (Change Controls)	1-2	10-20
Total		7-13	43-98

[2] 16:32

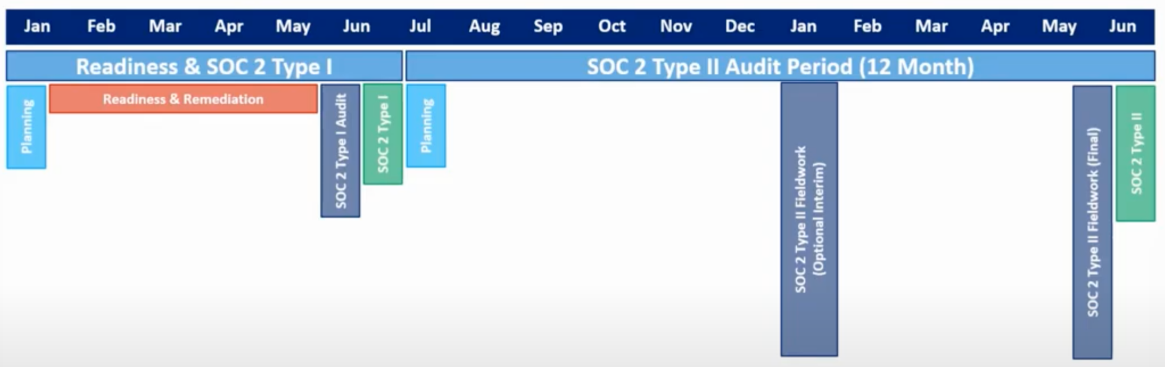
$30-50K by a boutique CPA firm such as risk3sixty[2], 4x for a “Big Four” firm.

- Linford & Co Denver, Colorado

VIDEO: SOC2 Intro by StrongDM by Justin McCarthy in San Mateo, CA, who also has a SOC2 Compliance Couse and COMPLY SaaS.

Videos from the OneTrust (formerly Tugboat Logic) SOC 2 Bootcamp:

Timeline & Strategies



[2]

1. **Identify a CPA firm** and choose timelines.
    - Auditors are in short supply, so the waiting list can extend your certification timeline.
2. Evaluate and **hire a certified external consultant** with experience in your particular industry (such as Truvantis, etc.).
3. **Educate** each department on the need for each control, the audit process, what documents and evidence are needed, and how to prepare (format) them:
    - Send invitations and track attendance and follow-up
    - Outside speakers to provide perspective and enthusiasm
    - Tracking of activities and achievements by individuals
4. **Survey** the organization, conduct document reviews, employee interviews, and walk-throughs to identify the amount of time and work to develop controls needed
    - System to survey opinions about buy-in and guage understanding

  - System to track progress on gaps in each control within each department

5. **Clarify the scope and activities** based on what customers want prioritized against limitations of time and resources.

   - Systems involved and their needs
   - Since internal audit resources are limited, plan **readiness assessments** one department at a time

6. **Specify who is involved** and each of their roles, responsibilities, and activities to achieve the desired objectives

   - Time requests into departmental Jira/Asana or other planning/tracking system in regular use
   - Metrics

7. Prepare the organization for mock and actual audits:

   - Schedules
   - Document **Samples/templates** with guidance on how to prepare (format) policies, procedures, playbooks (with linkages)
   - Traceability from Selection Of Controls through implementation and assessment (OSCAL)

Perform

8. Write/revise and review **security policies and procedures** (System Security Plans) behind each control where prior efforts (ISO) did not cover.

9. **Conduct processes to create evidence data** and System Assessment Plans (SAPs) as the basis for audit and reporting during the **audit period** (6 months to a year). Processes may include internal and external pen-testing.

10. **Track and report progress** each week/month on where each team still needs additional work, with projections toward when audit readiness will occur. Metrics for the Security Operations Center incident response and corrective action:

    - Mean Time to respond/remediate
    - Mean Time to acknowledge
    - Mean Time to close (Incident dwell time)
    - Percentage of false positives

SOC2 Type I audit (single process run)

11. Identify issues in audit preparations. This can be done by an internal auditor or an auditing consultant to provide guidance.

    A few weeks before the start of your audit, your auditor will send you a **PBC (Provided By Client) list** based on the controls identified for auditor review. There is often follow-up questions with some back-and-forth communication.

12. Prepare for and perform a **SOC2 Type 1 mock audit** by ensuring that **procedures and evidence** for each control can be confidently presented for a single process run.

13. Assess System Assessment Results (SARs).

14. Manage auditors on Type 1 audit day if that is part of the strategy. Challange controls auditors ask for, when appropriate.

SOC2 Type 2 audit

15. Perform a Type 2 mock audit. Ensure that evidence for each control can be presented for the audit period (6 months to a year).

16. Prepare for Type 2 audit. Ensure that each department has the evidence at the ready before auditor arrival.

17. Manage auditors on audit day. Challange controls auditors ask for, when appropriate.

18. Dispute draft auditor report language where it’s unfavorable.

19. Publicize/leverage the report with customers and prospects.

Applications

SOC2 doesn’t specify what systems are used.

PROTIP: Here are the most common ones used by enterprises:

- Email: Microsoft Exchange, Google G Suite, etc.
- Phishing education and simulation: KnowBe4, etc.
- Chat: Slack, Microsoft Teams, etc.
- SMS Text to mobile phones: Twilio, etc.

- Video: Zoom, Microsoft Teams, Loom, etc.
- Video editing: Camtasia, Loom, etc.

- Document creation: Microsoft Word, Google Docs, etc.
- Flowcharts: Lucid Chart, Figma, etc.
- File sharing: Microsoft OneDrive, Google Drive, etc.
- Project Management: Excel, Jira, Trello, Asana, etc.

- Payroll: ADP, etc.
- Documents & Signatures: Adobe sign, DocuSign, etc.
- Accounting: QuickBooks, etc.
- Recruiting & HR: Workday, etc.
- Training Presentation & Tracking: Workday, Cornerstone, etc.
- Surveys, Certifications: SurveyMonkey, etc.
- Spiffs: Xactly, etc.

- E-commerce: Shopify, GoDaddy, etc.
- Social media: LinkedIn, Instagram, Facebook, Twitter/X, etc.
- Employee reviews: Glassdoor, Indeed, etc.
- Conference: EventBrite, etc.
- CRM (Customer Relationship Management): HotSpot, Salesforce, Microsoft Dynamics, etc.

- Text editor IDEs: Visual Studio Code, etc.
- Text editor external plugins: Prettier, etc.
- macOS apps: iTerm2, etc.
- Windows apps: PuTTY, etc.
- Linux apps: Vim, etc.
- MDM: Jamf, etc.

- Cloud: AWS, Azure, Google Cloud, etc.
- Endpoint Security: CrowdStrike, etc.
- Cloud IAM: Okta, etc.
- CI/CD: GitHub Actions, Jenkins, etc.
- Source Code Versioning: GitHub, GitLab, etc.
- Containerization: Docker, Kubernetes, etc.
- Artifact (packages, containers): Artifactory, etc.

- SAST: SonarQube, etc.
- DAST: Burp Suite, etc.
- IAST: Contrast Security, etc.

- Configuration Management: Ansible, Chef, Puppet, etc.
- Infrastructure as Code: OpenTofu, Terraform, etc.
- IaC Scanning: Checkov, IPSec, etc.

- SIEM Observability/Monitoring: Prometheus, Grafana, Datadog, New Relic, etc.
- SOAR: Demisto, Phantom, etc.
- Logging: Grafana, Splunk, etc.
- Incident Management: PagerDuty, etc.

- ERP: SAP, Oracle, etc.

Each of the above is considered an asset to be maintained and protected.

GRC Automation

VIDEO Vanta.com was the first SaaS automated security and compliance system for companies who want to get SOC 2, ISO 27001, HIPAA, or other certifications. Vanta's software automatically gathers evidence and prepares companies for their security audits. Vanta integrates with 100+ cloud services, including AWS, GCP, and GitHub. Vanta obtained funding from Sequoia Capital, Y Combinator, and other investors after it reached $10 in sales.

Reciprocity's ZenGRC provides a platform for integrating compliance, audit, risk management, third-party risk solutions, and governance and policy management applications. It covers 32 domains and over 750 controls. It supports several compliance frameworks in addition to SOC2.

KnowB34, founded by reformed hacker Kevin Mitnick, offers their KCM GRC SaaS product, which claims "KCM GRC has a simple, intuitive user interface, easy to understand workflows, a short learning curve, and will be fully functional in a matter of days."

VIDEO by SecureFrame

Auditors

Here, the "SOC" in "SOC2" stands for ("Systems and Organization Controls", formerly "Service Organization Controls") reports as defined by the American Institute of Certified Public Accountants (AICPA).[1] The AICPA was formed as an association of independent CPA firms (such as PwC, Deloitte, EY, KPMG, etc.) who are approved by a **company's shareholders** to perform audits. Additionally, each CPA is licensed by the government after an examination. So they are built to be an "objective

3rd-party". However, SOC auditing is another line of business for CPAs.

NOTE: "SOC2" is implemented partly by a Security Operations Center", but does not mean "Systems on a Chip" (another acronyms).

Controls

PROTIP: Each GRC vendor and auditor has its own names for controls, organized a different way.

Therefore, a mapping of company internal names and organization needs to be mapped to the auditor's structure.

Specific Controls

Each TSC above contains **points of focus** – specific controls when designing, implementing, and operating controls.

Request the "SOC2 Controls List" Excel file of 291 detailed points of focused controls. From Brett Lieblich at consultantcy DashSDK.com.

TSCs

The Five Trust Services Criteria (TSC) 2022, listed here in alphabetical order:

- (A) **Availability** - Performance monitoring, Disaster Recovery, Security Incident Handling.

  Information and organizational systems are available (accessible) for operation and use to meet the entity's objective requirements. Controls include fail-over.

- (C) **Confidentiality** - Protected information, Data subjects, Privacy. (Additional criteria)

  Information designated as confidential is protected (such as passwords, encryption using security certificates, etc.) to meet the entity's objectives.

- (P) **Privacy** (of Consumer Personal information) - Sector privacy rules, Encryption. (Additional Criteria)

  Personal information is collected, used, retained, disclosed and disposed of to meet the entity’s objectives.

- (PI) **Processing Integrity** (over provisioning) - Payment transactions, Accurate process (via Quality Assurance), Errors corrected. Additional criteria)

  System processing is complete, valid, accurate, timely, and authorized to meet the entity’s objectives.

- (CC) **Security** - (aka required **Common Criteria** applicable to all audits) Firewalls, Security controls, Device configuration.

  Information and system assets are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise security availability, confidentiality, integrity, and privacy of data or systems. That also affects the entity’s ability to meet its objectives.

PROTIP: Service providers are regularly advised to limit their first SOC 2 audit to **just Security** and only include additional criteria if necessary.

COSO

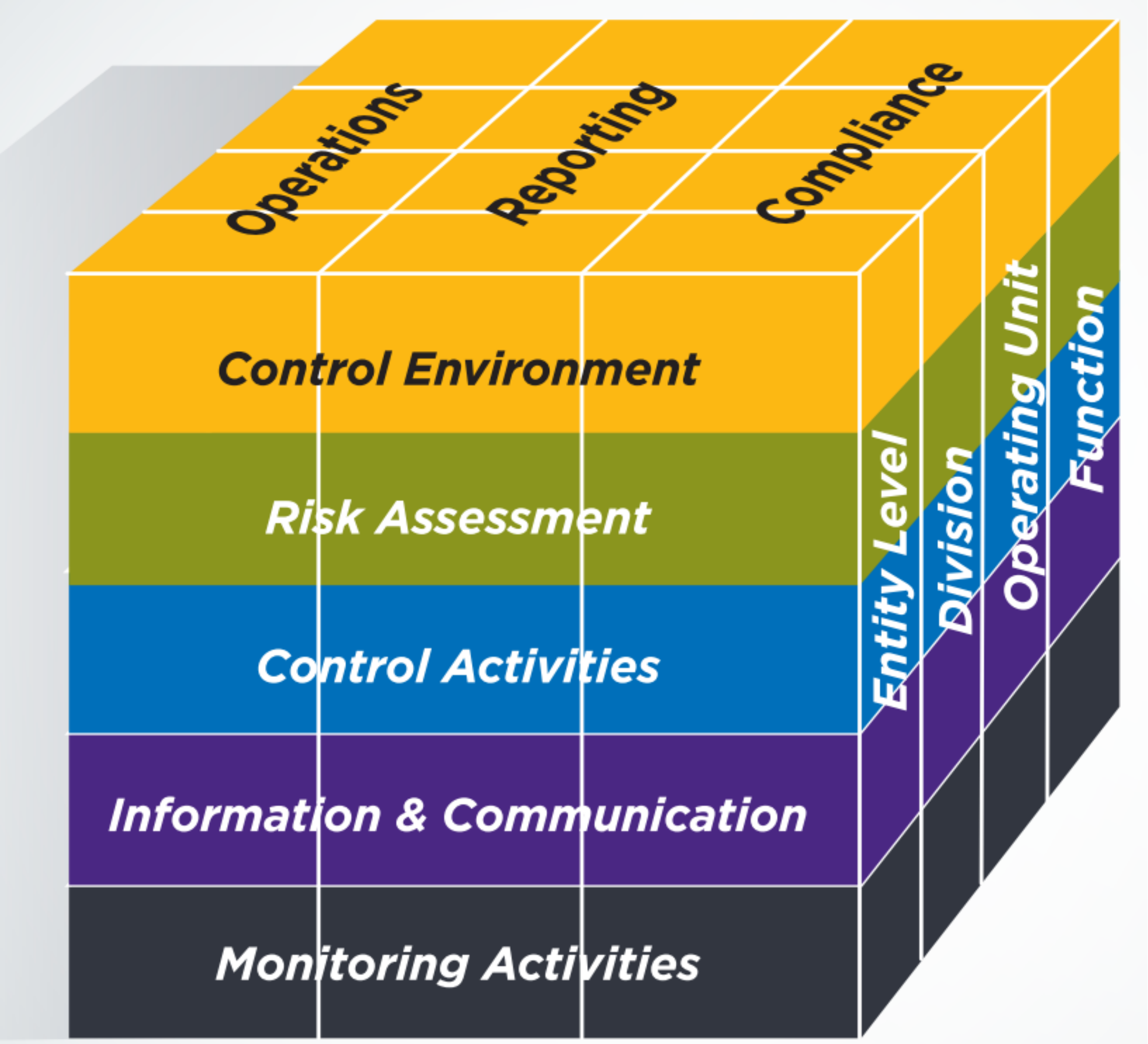
- The 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022) (2017 TSC) from AICPA & CIMA
- https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html
- https://weaver.com/blog/coso-frameworks-17-principles-effective-internal-control

The 2017 TSC standards for SOC 2 reports integrate the 2013 framework from COSO (Committee of Sponsoring Organizations of the Treadway Commission) at coso.org, which consists of PDF: 17 principles organized in these 5 categories:

- CC1 = Control Environment
- CC2 = Communication and Information (formerly called Communication and Information)
- CC3 = Risk Assessment
- CC4 = Monitoring Activities
- CC5 = Control Activities

The above aligns with the first five criteria sections within the security/common criteria.

The 2013 version was illustrated by this 5 x 3 x 4 (60 cell) matrix for 4 organizational levels.



©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). Used by permission.

TSP Section 100.08 describes four additional internal controls criteria:

- CC6 = Logical and Physical Access = How an entity restricts access (physical and logical), adds and removes said access, and avoids unauthorized access.
- CC7 = System Operations = How an entity manages the operation of the system(s) and detects and mitigates processing nonconformities, including access (physical and logical) security nonconformities.
- CC8 = Change Management = How an entity recognizes the necessity for changes, executes the changes using a controlled process and stops unauthorized changes from occurring.
- CC9 = Risk Mitigation = How the entity recognizes, chooses, and advances risk mitigation activities that have occurred from business disruptions, and the monitoring and evaluation of the use of business partners and vendors.

That makes for 9 x 3 x 4 = 108 items among 4 organizational levels.

Aspects (of evidence)

Each principle is assessed these aspects of evidence:

- **Operations** - Policies and Procedures
- **Reporting** - Metrics collection, dashboards, alerts
- **Compliance** - Time-stamped evidence stored
- **Strategic** - added

---

17 COSO Principles

Items marked with "FOCUS" added in 2022 are relevant to all SOC2 engagements.

Control Environment (CC1)

CC1.1 \1 The entity demonstrates a commitment to **integrity and ethical values**.

CC1.2 \2 The board of directors demonstrates **independence from management** and exercises **oversight** of the development and performance of internal control.

CC1.3 \3 FOCUS: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

CC1.4 \4 The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

CC1.5 \5 FOCUS: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Communication and Information (CC2)

CC2.1 \13 FOCUS: The entity obtains or generates and uses relevant, **quality information** to support the functioning of internal control.

CC2.2 \14 FOCUS: The entity internally communicates information, including **objectives and responsibilities** for internal control, necessary to support the functioning of internal control.

CC2.3 \15 FOCUS: The entity communicates with **external parties** regarding matters affecting the functioning of internal control.

Risk Assessment (CC3)

CC3.1 \6 The entity specifies objectives with sufficient clarity to enable the **identification and assessment** of risks relating to objectives.

CC3.2 \7 FOCUS: 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**.

CC3.3 \8 The entity considers the **potential for fraud** in assessing risks to the achievement of objectives.

CC3.4 \9 FOCUS: The entity identifies and **assesses changes** that could significantly affect the system of internal control.

Monitoring Activities (CC4)

CC4.1 \16 The entity selects, develops, and performs ongoing and/or separate **evaluations** to ascertain whether the components of internal control are present and functioning.

CC4.2 \17 The entity 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.

Control Activities (CC5)

CC5.1 \10 The entity selects and develops control activities that contribute to the **mitigation of risks** to the achievement of objectives to acceptable levels.

CC5.2 \11 The entity selects and develops general **control activities over technology** to support the achievement of objectives.

CC5.3 \12 The entity deploys control activities through **policies** that establish what is expected and **procedures** that put policies into action.

Logical and Physical Access Security (CC6)

CC6.1 FOCUS: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 The entity 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 the entity's objectives.

CC6.4 FOCUS: The entity 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 the entity's objectives.

CC6.5 The entity 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 the entity's objectives.

CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

CC6.7 The entity 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 the entity's objectives

CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations (CC7)

CC7.1 To meet its objectives, the entity 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

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.3 FOCUS: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 FOCUS: The entity responds to identified security incidents by executing a defined incident -response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management (CC8)

CC8.1 FOCUS: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation (CC9)

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

CC9.2 FOCUS: The entity assesses and manages risks associated with (vulnerabilities arising from) vendors and business partners.

Additional Criteria (A1)

PDF: 2017 Trust Services Criteria TSP Section 100.05 (March 2020 redline version) describes criteria in addition to COSO principles

FOR OPERATIONS (A1)

A1.1 The entity 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.

A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 The entity **tests recovery plan procedures** supporting system recovery to meet its objectives.

FOR CONFIDENTIALITY (C1)

C1.1 The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality

C1.2 The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.

FOR PROCESSING INTEGRITY (PI1)

PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity’s objectives.

PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.

PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity’s objectives.

PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.

FOR PRIVACY (PI)

P1.1 The entity provides **notice** to data subjects about its privacy practices to meet the entity’s objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity’s privacy practices, including changes in the use of personal information, to meet the entity’s objectives related to privacy.

P2.1 The entity communicates **choices** available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity’s objectives related to privacy. The entity’s basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

P3.1 Personal information is collected consistent with the entity's objectives related to privacy.

P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy

P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.

P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.

P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.

P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

P6.3 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

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.

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.

P6.6 The entity provides **notification of breaches and incidents** to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

P6.7 The entity provides data subjects with an **accounting** of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

P7.1 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

P8.1 The entity implements a process for receiving, addressing, resolving, and communicating the **resolution of** inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

Controls per TugboatLogic

The "Audit Readiness Module" from Tugboat Logic (https://tugboatlogic.com) translated SOC 2 requirements into a set of controls using a questionnaire, service providers can define their own scope. From questionaire answers, a list of 80-90 prebuilt policies and controls is mapped to the SOC2 framework:

- AA = Access Authentication
- AC = Access Control
- AT = Awareness and Training
- CM = Change Management
- CR = Continuity and Resilience

- DS = Data Security
- HR = Human Resources
- IM = Incident Management
- OM = Organization and Management
- RM = Risk Management

- SO = Security Operations
- VM = Vendor Management
- WS = Workstation Security

- SDLC Security?
- Asset Management?
- Audit and Compliance?

Specifically:

ACCESS CONTROL

- ACCESS CONTROL - Access Control Policy defines high-level requirements and guidelines on user account management, access enforcement and monitoring, separation of duties, and remote access.

- KEY MANAGEMENT AND CRYPTOGRAPHY - The organization utilizes the latest commercially accepted encryption protocols.

- SERVER SECURITY - The organization manages, configures, and protects organization servers and hosts based on industry best practices.

- PHYSICAL AND ENVIRONMENTAL SECURITY - The organization protects managed systems and personnel from unauthorized access and from natural and human caused damage or destruction.

- SERVERLESS SECURITY - The organization has established guidelines for the secure deployment and maintenance of the serverless architecture.

- IT ASSET MANAGEMENT - A formal change management policy governs changes to the applications and supporting infrastructure. That aids in minimizing the impact that changes have on organization processes and systems.

SECURITY OPERATIONS

How the organization handle system vulnerabilities, detect system operational issues and respond to security incidents:

- VULNERABILITY MANAGEMENT - The organization conducts scheduled application/network scanning and penetration tests.

- INCIDENT MANAGEMENT - It is critical to the organization that security incidents that threaten the security or confidentiality of information assets are properly identified, contained, investigated, and remediated.

- CHANGE MANAGEMENT - how the organizations conduct scheduled application/network scanning and penetration tests.

- MONITORING ACTIVITIES – how the organizations develop, monitors, and ensure that internal security controls are active and functioning.

RISK MANAGEMENT

- RISK ASSESSMENT - The organization institutes regular risk assessments and uses industry best practices in remediation.

- VENDOR MANAGEMENT - The organization actively manages risks around 3rd party vendors and their access to your company's data.

- INFORMATION SECURITY - The business utilizes (ex. "Tugboat Logic Platform") to manage InfoSec policies, provide security awareness training, implement and document security controls, and track compliance with customers, third party vendors, independent auditors and regulatory agencies.

BUSINESS CONTINUITY

- BUSINESS CONTINUITY AND DISASTER RECOVERY - Your company has a Business Continuity and Disaster Recovery Policy that ensures that the organization can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

ORGANIZATION & MANAGEMENT

The "Control Environment" is how the organization sets security roles, manages oversight and deals with security as related to employees, hiring, and overall management.

- ACCEPTABLE USE - the "Acceptable Use Policy" is a document stipulating constraints and practices that a user must agree to for access to a corporate network and other organizational assets.

- CORPORATE ETHICS - The organization values ethics, trust, and integrity throughout its business practices. How are they promoted and enforced?

- PERSONNEL SECURITY - Organization members understand their roles and responsibilities around security and privacy.

ASSET MANAGEMENT

- IT ASSET MANAGEMENT - A formal change management policy governs changes to the applications and supporting infrastructure.
- TECHNOLOGY EQUIPMENT HANDLING AND DISPOSAL - The organization appropriately disposes of equipment that contains sensitive information.
- BRING YOUR OWN DEVICE (BYOD) - Protect the security and integrity of organization's data and technology infrastructure when employees are using their personal device(s) to connect to organization's assets.

INFORMATION & COMMUNICATIONS

- INFORMATION CLASSIFICATION - Information classification assigns a value to information in order to organize it according to its risk to loss or harm from disclosure.
- WORKSTATION SECURITY - The organization protects laptops and workstations and their contents using industry best practices.
- NETWORK SECURITY - Your business provides a protected, interconnected computing environment through the use of securely configured network devices to meet organizational missions, goals, and initiatives.
- DATA INTEGRITY - Your company ensures that system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.regulatory agencies.

AUDIT & COMPLIANCE

- CUSTOMER SUPPORT AND SLA - Customers are important to your business. You provide Customer Support and a Service Level Agreement (SLA) to support customers.
- INTERNAL AUDIT - The organization conducts Internal Audits on its existing policies and controls to ensure the best level of service to customers.
- CUSTOMER SUPPORT AND SLA - Customers are important to your business. You provide Customer Support and a Service Level Agreement (SLA) to support customers.

DATA SECURITY

- DATA RETENTION AND DISPOSAL - This policy is about the organization's approach for data retention and secure disposal.
- MOBILE DEVICE MANAGEMENT - This policy defines procedures and restrictions for connecting mobile devices to organization's corporate network.

SDLC SECURITY

- SOFTWARE DEVELOPMENT - The organization designs and builds software with security and privacy as design principles.
- CHANGE MANAGEMENT – The organization defines how organizations handle development, testing, and deployment of systems and applications.
- PHYSICAL AND ENVIRONMENTAL SECURITY - The organization protects managed systems and personnel from unauthorized access and from natural and human caused damage or destruction.

CONTINUOUS COMPLIANCE

NIST Open Security Controls Assessment Language (OSCAL) at https://github.com/usnistgov/OSCAL has JSON Schema files

https://www.slideshare.net/MichaelaIorgaPhD/open-security-controls-assessment-language-oscal-1st-workshop-nov-57-2019 https://pages.nist.gov/OSCAL/contribute/devlunch Bi-weekly conf.

ArmorCode provides a tool which integrates DevSecOps pipelines with their tracking

---

Types of SOC2

The "2" in "SOC2" and "Type II" refers to the specific type of report issued. A SOC 2 Type II report of "attestation" is issued by a CPA for the service organization to provide to prospective customers. (By contrast, ISO 27001 auditors issue a "certificate of compliance".)

SOC1 is on audits of a service organization's **Internal Control over Financial Reporting (ICFR)**. It is applicable only to service organizations which perform **outsourced services** that affect the financial statements of another Company (the "User Organization"), such as Payroll Processing, Loan Servicing, Data Center/Co-Location/Network Monitoring Services, Software as a Service (SaaS), Medical Claims Processors, etc.

REMEMBER: “POLICIES” refer to rules defined to protect assets. “CONTROLS” are rules implemented (such as use MFA, etc.).

AICPA FAQ

SOC2 Type I reports address the suitability of policies and procedures in operation at a **specific moment in time**.

“SOC2 Type II” reports address both the suitability and **effectiveness** of policies and procedures over a **period of time** – no less than six months (usually a year). Since this report takes into account historical data generated, it is a more accurate and comprehensive audit. However, many companies are not able to adequately generate data as the basis for an audit until they have adequate controls in place.

Type 3 reports are a simplified version of the SOC 2 report. It is designed to **publicly** attest that the service provider has completed a SOC 2 assessment, while also limiting the information to what is relevant to public parties. SOC 3 report were created as a result of the growing demand for a public facing report.

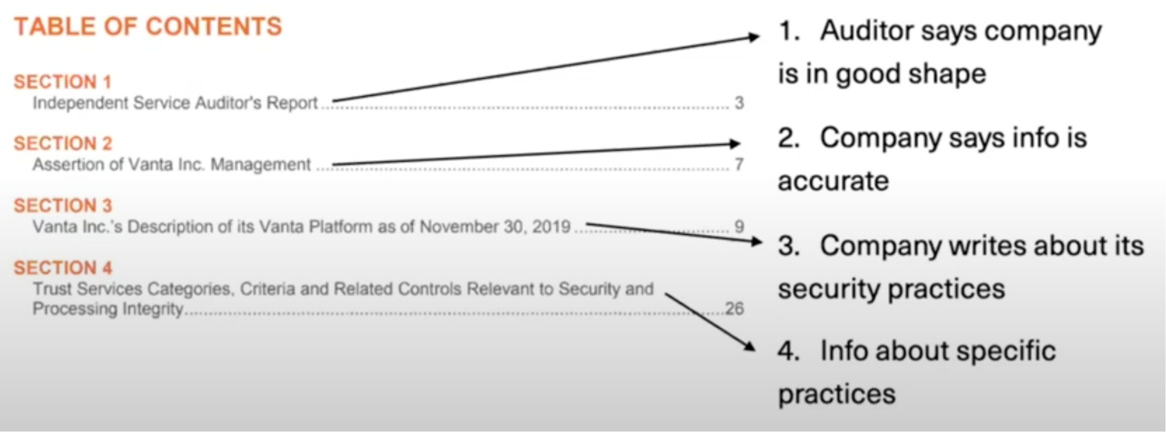


TABLE OF CONTENTS

SECTION 1
Independent Service Auditor's Report 3

SECTION 2
Assertion of Vanta Inc. Management 7

SECTION 3
Vanta Inc.'s Description of its Vanta Platform as of November 30, 2019 9

SECTION 4
Trust Services Categories, Criteria and Related Controls Relevant to Security and Processing Integrity 26

1. Auditor says company is in good shape
2. Company says info is accurate
3. Company writes about its security practices
4. Info about specific practices

[6]

These defined controls are a series of standards designed to help measure how well a given service organization conducts and regulates its information. They are designed to provide clients with confidence that an organization can be trusted to keep their data secure.

SSAE 18

The AICPA “Statement on Standards for Attestation Engagements” (SSAE) define standards auditors use to conduct audits. Verion 16 of SSAE replaced SAS (“Statement on Auditing Standards”) 70 on 2011. SSAE version 18 PDF was created May 2017. Its requirements defines some acronymns:

- **IPE** (Information Produced by the Entity): Companies must provide evidence of the accuracy of any information provided. Examples include SQL queries or Tableau report parameters.

- Vendor management and monitoring of **sub-service organizations**: Service providers or data centers must include controls for sub-service organizations. The goal is to ensure that anybody with access to the data is adhering to control standards.

- **CUECs** or Complementary User Entity Controls: limited to controls that are needed to achieve the stated control objectives

- Internal audit and regulatory examinations: service organizations read the latest reports relating to internal and regulatory examinations. For example, SOC Cybersecurity examination and updated trust services principles went into effect on December 15th, 2018.

The equivalent for SSAE 18 internationally is the ISAE 3402 (International Standards for Audit Engagements) published by the International Auditing and Standards Board (IASB).

Management Insights

Management of the process requires these areas of insight:

- Audit report countdown: When can salespeople provide customers with a current SOC2 Type II report?

- Audit readiness: Are policies, controls, and procedures defined and reviewed in each area?

- Compliance status: Are proofs of compliance being generated for controls in each area?

- Gap analysis: In what areas do compliance gaps exist?

- Trend: How has our security posture improved over time?

- Future gap analysis: How much effort is required to comply with additional frameworks?

- Benchmarking: How are we doing relative to competitors?

Additional frameworks

Many controls covered by SOC 2 are also of concern in legal standards as well as ISO, CCPA, GDPR, and customer-specific requirements.

Since 2017, a **SOC 2+** report allow a service organization to address additional criteria from other compliance standards such as HITECH, HIPAA compliance, Cloud Security Alliance (CSA), NIST 800-53, or COBIT 5.

ISO 27001

VIDEO: Customers outside the US will ask for a "Certificate of Compliance" from ISO 2700x independent auditors (not CPAs).

ISO 27001 focuses on the development and maintenance of an information security management system (ISMS). An ISMS provides a systematic approach for managing an organisation's information security.

BLOG: "It should take about two or three months to implement SOC 2 and three to six months to implement ISO 27001."

PROTIP: ISO 27001 Project video tutorial with Excel sheet by Deliotte Germany Lead Auditor Aron Lange. The Gantt chart is based on 100 tasks on a dynamic timeline:

1. Management Support
2. Initiate the ISMS
3. Determine Scope
4. Information Security Policy
5. Competence Assurance
6. Inventory of Assets
7. Risk Management Methodology
8. Risk assessment
9. Risk Treatment Plan
10. Performance Evaluation
11. Improvement
12. Certification audit

VIDEO: ISO 27001 Lead Implementer course on Udemy, with mind maps.

His 6-minute VIDEO "Exploring ISO 27000: A Comprehensive Overview of Information Security Standards" is a good intro to ISO 27000.

Public companies required under Section 404 of the Sarbanes-Oxley Act (SOX) to file annual reports on the design and operating effectiveness of their internal controls.

References

[1] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

[2] Timeline from VIDEO: "SOC 2: Everything You Need to Get a SOC 2 Report" by risk3sixty

[3] TSC by DashSDK.

[4] VIDEO: CertMike Explains SOC Audits by Mike Chapple (who created the preminent tutorials for security certifications)

[5] https://www.ssae-16.com/ssae-16/ssae-16-preparation-checklist

[6] VIDEO: SOC2 Compliance for Startups by Venta CEO Christina Cacioppo

"Jump-start Your SOC Analyst Career: A Roadmap to Cybersecurity Success" (Apress March 2021) by Tyler Wall, Jarrett Rodrick

https://www.strikegraph.com/strikegraph_blog/how-auditors-test-and-what-to-expect

Great pdf intro to SOC2 from PracticalAssurance.com

heylaika.com offers their "Unified SOC 2 Platform".

https://www.youtube.com/watch?v=QV43QDKSRD8 "How to Add SOC 2 to Your ISO 27001" by Schellman notes ISO 27001:

- ISMS scope
- ISMS Leadership
- Risk Assessment
- Internal Audit
- Management Review
- Corrective Action Processes

(AAC-02.1) Cloud vendors post their reports in the Cloud Security Alliance Registry and on their website to signed-on users at:

- https://console.aws.amazon.com/artifact/reports
- https://servicetrust.microsoft.com/
- https://cloud.google.com/security/compliance/soc-2
- etc.

https://www.securitypalhq.com/

https://pages.nist.gov/OSCAL/resources/sources/concepts/terminology/

No longer active is the OpenControl.org tool to customize security control standard and a machine-readable format to enable automation and tooling. for FEDRAMP ATO.

Training

LetsDefend.io offers online text-based **SOC Analyst Learning** (for $199/yr). Topics:

- SOC Fundamentals
- Cyber Kill Chain
- MITRE ATT&CK Framework
- Phishing Email Analysis
- Detecting Web Attacks
- Detecting Web Attacks - 2
- Investigate Web Attack
- Malware Analysis Fundamentals
- SA - Malware - Event ID: 77
- Dynamic Malware Analysis
- MSHTML
- Malicious Document Analysis
- Security Solutions
- Network Log Analysis
- SIEM 101
- Incident Management 101
- Splunk
- Cyber Threat Intelligence
- VirusTotal for SOC Analysts
- SA - Malware - Event ID: 76
- IT Security Basis for Corporates
- Detecting Brute Force Attacks
- Building a Malware Analysis Lab
- Building a SOC Lab at Home on an AMD64 Windows PC running in a VirtualBox with
    - Active Directory
    - MediaCreationTool_22H2.exe Windows Workstation
    - pfSense

  - Sysmon for log analysis
  - CrowdSec IP Blocklist and Windows Firewall Bouncer.

For hands-On labs, pay their $199/year “VIP” pass for

- SOC Analyst Path

Pay their $359/year VIP offering to also add:

- Malware Analysis path
- Incident Responder career path
- Detection Engineering career path

More about Security

This is one of a series about cyber security:

1. Security actions for teamwork and SLSA
2. DevSecOps

3. Code Signing on macOS
4. Transport Layer Security

5. Git Signing
6. GitHub Data Security
7. Encrypt all the things

8. Azure Security-focus Cloud Onramp
9. Azure Networking

10. AWS Onboarding
11. AWS Security (certification exam)
12. AWS IAM (Identity and Access Management)
13. AWS Networking

14. SIEM (Security Information and Event Management)
15. Intrusion Detection Systems (Goolge/Palo Alto)
16. Chaos Engineering

17. SOC2
18. FedRAMP
19. CAIQ (Consensus Assessment Initiative Questionnaire) by cloud vendors

20. AKeyless cloud vault
21. Hashicorp Vault
22. Hashicorp Terraform
23. OPA (Open Policy Agent)

24. SonarQube
25. WebGoat known insecure PHP app and vulnerability scanners
26. Test for OWASP using ZAP on the Broken Web App

27. Security certifications
28. Details about Cyber Security

29. Quantum Supremecy can break encryption in minutes
30. Pen Testing
31. Kali Linux

32. Threat Modeling
33. WebGoat (deliberately insecure Java app)

SOC2 was published on May 04, 2024.