DRATA

Get a Demo Today:
https://drata.com/demo

SOC 2 CHECKLIST
HOW AUDIT READY IS YOUR COMPANY?

For the **7 categories** below, you will self-assign a score for your SOC 2 audit readiness based on the following criteria:

1	2	3	4
Not Implemented	**Somewhat Implemented**	**Mostly Implemented**	**100% Implemented**
Few, if any, controls have been defined, documented, or implemented.	Some controls are defined, documented, or implemented but there's clearly still a lot of work to do.	Most of the controls are defined, documented, or implemented but there's still some work to do.	All of your controls are defined, documented, or implemented. Great job!

RISK ASSESSMENT

○ ○ ○ ○
1 2 3 4

A risk assessment should be performed **at least annually** to identify potential threats to your company's information security and privacy program. A typical risk assessment process:

- Identify and prioritize information assets that are critical to business operations
- Identify and assess the impact of threats to those assets where vulnerable
- Assess the likelihood that these threats/vulnerabilities will contribute to a security breach.
- Score the resulting risks associated with all assets.

RISK MITIGATION

○ ○ ○ ○
1 2 3 4

Now that you've performed a risk assessment, have you identified and developed mitigation strategies to address these security risks (both for your business and for any associated vendors and partners)?

Once risks are prioritized, policies and procedures should be put in place to address them using one of four risk management strategies:

Avoid the risk -- Mitigate the risk -- Transfer the risk -- Accept the risk

1	2	3	4
Not Implemented	**Somewhat Implemented**	**Mostly Implemented**	**100% Implemented**
Few, if any, controls have been defined, documented, or implemented.	Some controls are defined, documented, or implemented but there's clearly still a lot of work to do.	Most of the controls are defined, documented, or implemented but there's still some work to do.	All of your controls are defined, documented, or implemented. Great job!

CONTROLS IN POLICIES

○	○	○	○
1	2	3	4

Security controls are designed to secure vulnerabilities, minimize deviations, and close control gaps that were previously identified during the risk assessment process. These policies and procedures need to be documented in order to demonstrate to a SOC 2 auditing firm how the organization is addressing security risks.

Typical Policies: Information Security Policy, Access Control Policy, Change Management Policy, Password Policy, Code of Conduct, Risk Assessment Policy, Incident Response Policy, Vendor Management Policy, Acceptable Use Policy, Data Classification Policy, Business Continuity & Disaster Recovery Plan, Backup Policy

CONTROL MONITORING

○	○	○	○
1	2	3	4

Have you begun documenting all control activities related to security readiness and performance. Examples may include:

- Vulnerability scan and penetration test reports
- Corrective actions undertaken to remediate deficiencies or deviations
- Access control reviews
- Policy review, approval, and acknowledgement from personnel
- Vendor management evaluation and attestation report review
- Compliance, control, and risk assessment review scoring

VENDOR MANAGEMENT

○	○	○	○
1	2	3	4

In order to evaluate risks posed by third-party vendors, you should have an assessment and management process that may include (but not limited to):

- Review of vendor SOC 2 attestation reports
- Periodic discussions with vendors.
- Tests of vendor security controls.

1 Not Implemented

Few, if any, controls have been defined, documented, or implemented.

2 Somewhat Implemented

Some controls are defined, documented, or implemented but there's clearly still a lot of work to do.

3 Mostly Implemented

Most of the controls are defined, documented, or implemented but there's still some work to do.

4 100% Implemented

All of your controls are defined, documented, or implemented. Great job!

CONTROL ACTIVITIES

○	○	○	○
1	2	3	4

Do you have up to date evidence documented for the following:

- Organizational chart
- Board of directors or executive oversight
- Hiring and onboarding/off-boarding checklists
- Personnel background screening
- Security awareness training
- Employee hard disk encryption
- Antivirus/anti-malware software
- Policy distribution and acknowledgement
- Employee evaluations

ASSET INVENTORY

○	○	○	○
1	2	3	4

An asset inventory should be maintained that documents owners and criticality levels. To maintain control of these assets, some of the following should be in place:

- Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Firewall and router procedures and rules
- File integrity monitoring (FIM) software
- Incident response tracking
- Backups, data recovery, and business continuity planning

RISK **ASSESSMENT**	RISK **MITIGATION**	CONTROLS **IN POLICIES**	CONTROL **MONITORING**	VENDOR **MANAGEMENT**	CONTROL **ACTIVITIES**	ASSET **INVENTORY**

YOUR SOC 2 AUDIT **READINESS SCORE:**

DRATA

Get a Demo Today:
https://drata.com/demo

ROBUST MATURITY

Your security program supports a strong control posture through defined policies and processes that address key risks, implement control mitigation strategies, and focus on continuous improvement. You're ready to undergo a SOC 2 examination. Drata can continuously monitor your strong security program, notify your team in real-time when gaps are identified, automatically collect control evidence across your tech stack, and streamline personnel compliance activities. Get a demo today, our team would love to show you what Drata can do!

> 27

STRONG MATURITY

Your security program has clear controls that support a risk-based methodology. You're mostly prepared to undergo a SOC 2 audit, but may benefit from reviewing the Trust Services Criteria that apply to your organization and ensure that your processes and controls are well documented to support an examination process that moves smoothly and without delays. Drata's platform can implement an automation-enabled approach to guide you through an audit and beyond. Get a demo today and let's put SOC 2 on autopilot.

21 - 27

MODERATE MATURITY

Your company has moderate organizational awareness with a focus on control activities but may lack supporting evidence to ensure a smooth SOC 2 audit process. You may consider additional steps to prepare ahead of your initial audit engagement. Talk to a Drata representative to learn more about our SOC 2 readiness platform and how it can help you get ready for an examination and stay ready every day of the year.

13 - 20

LOW MATURITY

Your company is just starting its journey toward SOC 2 readiness, but that's an exciting place to be! You can get started by developing and documenting defined processes and controls with an eye toward risk mitigation. Drata helps you build an automation-enabled approach to continuous compliance that will put you on the fast-track to SOC 2 readiness. Get a demo today and let's put SOC 2 on autopilot.

< 13

Companies of all sizes and compliance maturity levels use Drata to gain visibility into their compliance status, control across their security program, and to build a single picture of controls, people, devices, applications, vendors, and risk across their company.