

hicomply

SOC 2 Compliance Checklist: A Step-By-Step Guide



Does your SOC 2 report need to address:

- Security
- Availability
- Confidentiality
- Privacy
- Processing integrity
- Define organisational structure
- Designate authorised employees to develop and implement policies and procedures
- Establish working committees
- Implement background screening procedures
- Establish workforce conduct standards
- Ensure clients and employees understand their role in using your system or service
- Effectively communicate system changes to the appropriate personnel in a timely manner
- Define your organisation's policies and procedures relevant to the selected Trust Services Criteria
- Undertake SOC 2 gap analysis
- Implement necessary policies and procedures identified by gap analysis
- Test and validate new policies and procedures

Perform a risk assessment:

- Identify potential threats to the system
- Analyse the significance of the risks associated with each threat
- Develop mitigation strategies for those risks
- Conduct regular fraud risk assessments
- Perform regular vendor management assessments
- Undertake annual policy and procedure review
- Implement physical and logical access controls
- Limit access to data, software, functions, and other IT resources to authorised personnel based on roles

- Restrict physical access to sensitive locations to authorised personnel only
- Implement an access control system
- Implement monitoring to identify intrusions
- Develop and test incident response procedure
- Update software, hardware, and infrastructure regularly as necessary
- Execute a change management process to address flaws in controls
- Establish and identify backup and recovery policies
- Establish and identify how are you addressing environmental risks
- Test and record your disaster recovery plan
- Ensure data is being processed, stored, and maintained accurately and in timely manner
- Protect confidential information against unauthorised access, use, and disclosure
- Identify your documented data retention policy

You've completed your SOC 2 checklist!

To learn more about how you can automate the process to a successful SOC 2 audit, [get in touch with team Hicomply](#) - or explore the options below:

[Book a demo](#)



[Read the Hicomply blog](#)



[Visit the SOC 2 hub](#)

