



# SOC 2 Compliance Checklist

## A Step-By-Step Guide



# SOC 2 Compliance Checklist

## A Step-By-Step Guide

### Does your SOC 2 report needs to address:

- Security
- Availability
- Confidentiality
- Privacy
- Processing integrity
- Define organizational structure
- Designate authorized 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 organization'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



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

## Perform a risk assessment:

- Identify potential threats to the system
- Analyze 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 authorized personnel based on roles
- Restrict physical access to sensitive locations to authorized 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



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

## Perform a risk assessment:

- Test and record your disaster recovery plan
- Ensure data is being processed, stored, and maintained accurately and in a timely manner
- Protect confidential information against unauthorized 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 Midis team](#)