



SOC 2 Audit Checklist

*This checklist is provided for informational purposes only and does not constitute legal advice or a comprehensive SOC 2 compliance solution.



1. Security

- Implement and maintain firewalls
- Use intrusion detection systems
- Conduct regular vulnerability scans and penetration testing
- Implement strong access controls (e.g., multi-factor authentication)
- Establish and follow a formal change management process
- Implement security incident response procedures
- Conduct regular security awareness training for employees



2. Availability

- Implement and test disaster recovery and business continuity plans
- Monitor system performance and capacity
- Implement redundancy for critical systems and data
- Establish and maintain backup procedures
- Conduct regular failover testing

3. Processing Integrity

- Implement data input and processing controls
- Establish quality assurance procedures
- Monitor system processing
- Implement error handling procedures
- Maintain system documentation and operating procedures



4. Confidentiality

- Implement data classification policies
- Use encryption for data in transit and at rest
- Establish and maintain access control lists
- Implement secure data disposal procedures
- Use non-disclosure agreements with employees and third parties

5. Privacy (if applicable)

- Develop and maintain a privacy policy
- Implement procedures for collection, use, retention, and disposal of personal information
- Establish procedures for addressing privacy-related inquiries and complaints
- Implement controls for third-party data sharing
- Conduct privacy impact assessments for new systems or processes



6. General Controls

- Establish and maintain information security policies and procedures
- Implement HR security controls (background checks, termination procedures)
- Conduct regular risk assessments
- Manage vendor and third-party risks
- Maintain an asset inventory
- Implement physical and environmental security controls

7. Documentation

- Prepare system descriptions
- Document control objectives and related controls
- Maintain evidence of control execution
- Keep records of security incidents and resolutions
- Document risk assessment results and mitigation plans



Make SOC 2 Compliance Simple with Gart Solutions

SOC 2 compliance doesn't have to be complicated. At Gart Solutions, we specialize in DevOps and cloud services to help you protect your customers' sensitive data and stay fully compliant with SOC 2 standards.

Here's how we can help:

- Perform a full risk assessment based on the five key areas of SOC 2
- Set up strong security measures to protect your data
- Manage vendor risks and processes
- Provide ongoing training and support for your team

Let's work together to boost your data security and keep your business safe. Contact Gart Solutions today!

gart.

 [gartsolutions.com](https://www.gartsolutions.com)

 info@gartsolutions.com