

SOC 1 Compliance Checklist

SOC 1 compliance Checklist

- Does organization have a defined organizational structure?
- Has your organization designated authorized employees to develop and implement policies and procedures?
- What is your organization's background screening procedure?
- Does your organization have established workforce conduct standards?
- Do clients and employees understand their role in using your system or service?
- Are system changes effectively communicated to the appropriate personnel in a timely manner?
- Has organization performed a formal risk assessment?
 - Has your organization identified potential threats to the system?
 - Has your organization analyzed the significance of the risks associated with each threat?
 - What are your organization's mitigation strategies for those risks?
- Does your organization perform regular vendor management assessments?
- Has your organization developed policies and procedures that address all controls?
- Does organization perform an annual policy and procedure review?
- Does your organization have physical and logical access controls in place?
- Is access to data, software, functions, and other IT resources limited to authorized personnel based on roles?
- Does your organization restrict physical access to sensitive locations to authorized personnel only?
- Has your organization implemented an access control system and implemented monitoring to identify intrusions?
- Has your organization developed and tested incident response procedures?
- Is software, hardware, and infrastructure updated regularly as necessary?
- Does your organization have a change management process to address deficiencies in controls?
- What is your organization's data backup and recovery policies?
- How is your organization addressing environmental risks?
- Have your organization's disaster recovery and business continuity plans been tested and documented?
- How is your organization ensuring data being processed, stored, and maintained accurately and timely?
- How is your organization protecting confidential information (especially financial information) against unauthorized access, use, and disclosure?
- Does your organization have a fully documented data retention policy?