

SOC 2 SELF-ASSESSMENT CHECKLIST

SOC 2 Self-Assessment Checklist	Fully Implemented	Partially Implemented	Not Yet
Has your organization identified the key systems required to provide services to clients?			
Does your organization have monitoring activities in place to evaluate the effectiveness of your internal security controls?			
Has your organization documented control activities to mitigate risks and achieve the organization's objectives?			
Has your organization performed a risk assessment?			
Has your organization identified, selected, and developed mitigation strategies for addressing potential security risks (both for your business and for any associated vendors and partners)?			
Does your organization formally defined and distributed key information security processes and procedures?			
Does your organization conduct background verification for all your employees as a process?			
Does your organization have established processes to offboard employees within three-seven working days once they leave?			
Has your organization established key responsibilities, oversight structures, and organizational objectives that demonstrate a commitment to ethical values?			
Does your organization you have Multi-factor Authentication (MFA) and Password Manager enabled for its employees?			
Does your organization have a formal Code of Conduct and Organizational & Infosec policies in place?			

SOC 2 Self-Assessment Checklist	Fully Implemented	Partially Implemented	Not Yet
Does your organization conduct a vendor risk assessment, and are those conducted periodically?			
Does your organization have an Incident Management Policy in place?			
Does your organization have a Threat Management System in place?			
Does your organization have a formal data retention and disposal policy?			
Does your organization have established privacy policies and notices in accordance with applicable requirements?			
Does your organization have information security policy and established information security controls?			
Does your organization have appropriate change control procedures?			
Does your organization you periodically review the access to code and infra database?			
Does your organization have peer reviews in place for every code change?			
Does your organization encrypt its production databases at REST?			
Does your organization have ransomware/ malware protection installed? And you systems encrypted?			
Does you organization monitor and log access to identify anomalies and incidents?			
Does your organization have Mobile Device Management (MDMs) enabled?			
Does your organization have a code dependency scanner?			

