SOC Readiness

CHECKLIST

AAFCPAs
great minds | great hearts

Plan Ahead. Align Teams. Strengthen Controls.

This checklist is designed to support structured planning for your upcoming SOC examination. Use it to assess the current state of your internal controls, documentation, and audit readiness efforts. For each item, mark **Yes**, **No**, or **Unsure** based on your organization's status.

	Define SOC Scope and Internal Alignment	Yes	No	Unsure
1	The appropriate SOC report type (SOC 1, SOC 2, or SOC for Cybersecurity) has been identified based on business needs and stakeholder requirements.			
2	Internal stakeholders have been designated to manage and support the SOC engagement process.			
3	Requests from clients or prospects for assurance reporting are being tracked and reviewed regularly.			

	Formalize Internal Control Framework	Yes	No	Unsure
1	A formal internal control framework (e.g., COSO 2013, ISO 27001) has been defined and documented.			
2	A risk assessment has been completed to identify key threats to systems, data, and operations.			
3	Policies related to security, availability, confidentiality, and privacy are documented and periodically reviewed.			

	Centralize Documentation and Evidence	Yes	No	Unsure
1	Key policies and procedures are formally documented and accessible to relevant team members.			
2	Evidence is available to demonstrate that controls have operated effectively over a defined period.			
3	An internal system or workflow tool is in place to support documentation and evidence tracking.			

Strengthen Access and System Security		Yes	No	Unsure
1	Access to systems is restricted using least privilege and role-based access controls.			
2	Controls are in place to monitor for, detect, and respond to cybersecurity threats.			
3	Regular penetration testing or vulnerability scanning is conducted to assess risk exposure.			

Oversight, Monitoring, and Response		Yes	No	Unsure
1	Documented processes exist for detecting, reporting, and responding to incidents.			
2	Change management and backup/recovery procedures are well-documented and tested regularly.			
3	Dashboards or key metrics are used to monitor the performance of controls.			
4	Post-incident reviews are conducted, and outcomes are used to improve processes.			

Compliance Integration and Planning		Yes	No	Unsure
1	A SOC readiness assessment has been completed or is planned to identify potential control gaps.			
2	The organization is considering alignment with other frameworks (e.g., HIPAA, ISO) through a SOC 2+ or similar initiative.			
3	Specialists (e.g., Certified Ethical Hackers) have been consulted or engaged to support technical or cybersecurity aspects.			
4	A process is in place to stay current on SOC guidance and evolving regulatory expectations.			

Partner With AAFCPAs to Accelerate Your SOC Success

AAFCPAs is a premier SOC report provider, known for audit efficiency, accuracy, and actionable insight. Our team—including certified ethical hackers—provides readiness assessments, integrated compliance solutions, and support at every stage of your audit journey.

Let's ensure your organization is audit-ready and future-ready.

Partner, Governance, Risk & Compliance

James Jumes, MBA, M.Ed.

774.512.4062 | jjumes@aafcpa.com

Director, Governance, Risk & Compliance

Paula Chamoun, CISA, CISSP, CISM

774.512.9494 | pchamoun@aafcpa.com

Schedule a consultation ➡

Disclaimer

This checklist is intended for general informational purposes only and does not constitute professional advice or an assurance opinion. Completion of this self-assessment does not guarantee readiness for a SOC examination, nor does it replace the need for formal guidance from a qualified CPA or IT assurance professional. Organizations are encouraged to consult with AAFCPAs or another qualified advisor to assess specific requirements, evaluate risks, and determine the appropriate scope and readiness steps for their SOC engagement. AAFCPAs disclaims any liability for actions taken or not taken based on the information provided herein.