MOSSADAMS

CHECKLIST

SOC 2 Compliance

MARKET DRIVERS

- [ ] Are you required to demonstrate a standard of security to comply with laws or regulations?
- [ ] Are you being asked to complete questionnaires and security due diligence by your customers and third parties?
- [ ] Is SOC 2 compliance written into your organization's contracts, master services agreement (MSA), or terms of service (ToS) to ensure you're practicing good information security?

MANAGEMENT AND STAKEHOLDER CHAMPIONS

The SOC 2 process and examination require an organization to expend resources in terms of human capital as well as funds.

- [ ] Have you obtained buy-in from key management and stakeholders to pave the way for success?
- [ ] Have the stakeholders clearly communicated their buy-in to the rest of the organization?

DEFINE THE SCOPE OF YOUR SYSTEMS

A SOC 2 examination has a finite scope generally focused on a key product or service. SOC 2 requirements will pertain to systems considered in the scope, but not other systems such as back office productivity tools or accounting software.

- [ ] List the tools, applications or systems used to deliver the product or service
- [ ] Identify subservice organizations utilized to assist in your service offering

UNDERSTAND THE SOC 2 CATEGORIES

SOC 2 examinations can report on different categories in the Trust Services Criteria. Security is the base category included in all SOC 2 reports. In addition, depending on the organization and their operations, the availability, confidentiality, processing integrity or privacy categories could be relevant.

- [ ] Are you hosting a customer's environment? If so, you may need to report on availability.
- [ ] Do you need to protect personal identifying information (PII) or protected health information (PHI)? If so, you may need to report on privacy and confidentiality.
- [ ] Do you process transactions on behalf of your customers or other interested parties? If so, you may need to report on processing integrity.

DETERMINE REPORT TYPE

Organizations can pursue either a SOC 2 Type 1 or a SOC 2 Type 2 report.

- [ ] Have your customers, or other interested third parties, requested a Type 1 or a Type 2 report?
- [ ] Do you need to demonstrate the design and implementation of controls, or the operating effectiveness of controls over a period of time?

Continued

POLICIES & PROCEDURES

- [ ] Have you outlined and formally documented the activities and processes that form the foundation of your organization's control environment?
- [ ] Do you review and update these documents on a regular basis?

TESTING THE CONTROL ENVIRONMENT

- [ ] How is the organization governed?
- [ ] What is the tone and example of executive leadership and management?
- [ ] Have hiring and exit procedures been developed and followed?
- [ ] How is competency assessed for individuals performing or overseeing internal controls?
- [ ] Are potential threats being identified?
- [ ] Have you implemented mitigation strategies?
- [ ] Do you have an incident response procedure and a disaster recovery plan in place?
- [ ] What sort of governance and oversight from management is in place when it comes to your control environment and reporting incidents/security concerns/fraud?

SECURITY

- [ ] Do you have access restricted to roles that require such access with periodic review over appropriateness of access granted?
- [ ] Do you have procedures in place on how to provision and de-provision access to employees, customers, and third parties?
- [ ] Do you encrypt data in transit and at rest?
- [ ] Do you limit administrative access to the technology stack?

RISK MITIGATION

- [ ] Have you performed period vulnerability assessments or penetration testing to identify vulnerabilities in your environment?
- [ ] Do you have backup procedures established?
- [ ] Do you perform annual disaster recovery testing to ensure you can resume operations in the event of a disaster?
- [ ] Do you perform periodic monitoring over intrusion attempts, availability concerns, and system performance?

Continued

SYSTEM CHANGES

- [ ] Are system changes being testing and approved before implementation?
- [ ] Do you communicate system changes to your staff?
- [ ] Are you monitoring your controls on an ongoing basis?
- [ ] Have you enabled configuration-change notifications?
- [ ] Are your technology upgrades up to date?
- [ ] Have you established segregation of duties in the development and production environments?

REMOTE WORK CONSIDERATIONS

- [ ] Is technology consistently applied across all employee locations?
- [ ] Do you perform periodic security awareness training for employees, consider data privacy in shared spaced, secure connections when working from home, and promote awareness of phishing attempts?
- [ ] Do you utilize multifactor authentication for access to the corporate network and other systems?
- [ ] Have you implemented mobile device management to require encryption and authentication on mobile devices?

SELECT THE RIGHT PARTNER

Collaboration and good communication with your SOC 2 auditor are key to completing your first successful SOC 2 examination.

- [ ] Did you choose an auditor with extensive experience and expertise?
- [ ] Does your auditor take a collaborative approach to help you understand your compliance requirements and appropriate response?
- [ ] Can your auditor scale with your organization as it grows, and your controls mature?
- [ ] Is your auditor recognized in the market as a provider of reliable, high quality examinations?