SOC Readiness Assessment

Sample Policy and Procedure Requirements

Please check all the boxes below if you have these policies in place.

Information Security Program	
Performance Review Procedures	
Enterprise Architecture Procedures	
Job Description Procedures	
Background Check Procedures	
Code of Conduct Procedures	
Employee Confidentiality Agreement Procedures	
Security Awareness Training Procedures	
Access Control Procedures	
Penetration Testing Procedure	
Patch Management Procedure	
Vulnerability Scanning Procedures	
Antimalware Procedures	
System Monitoring Procedures	
Asset Inventory Procedures	
Data Retention and Disposal Procedure	
Data Backup Procedures	
Firewall Procedures	
Encryption Procedures	
Third-Party Management Program	
Third-Party Confidentiality Agreement Procedures	
Risk Management Program	
Risk Assessment Procedures	
Change Control Procedures	
System Hardening Procedures	
Physical Security Procedures	
Incident Response Program	
Incident communication procedures	
Incident response testing	
Board of Directors Charter	

Sample Evidence Requirements

Please check the boxes below if evidence is currently available for review.

Inspect signed employee code of conduct acknowledgements	
Inspect signed employee confidentiality agreements	
Inspect performance reviews	
Inspect background checks	
Inspect Board of Directors meeting minutes	
Inspect the organizational chart	
Inspect job descriptions	
Inspect security awareness training	
Inspect quarterly vulnerability scans	
Inspect vulnerability scan item remediation	
Observe log management application	
Inspect client agreements	
Inspect vendor confidentiality agreements	
Inspect publicly available support web site	
Inspect annual risk assessment	
Inspect annual contingency plan testing	
Inspect annual third-party penetration testing	
Inspect third-party SOC report reviews	
Observe login on process for in scope systems	
Inspect user access rights on in scope systems	
Inspect password settings on in scope systems	
Inspect network diagrams	
Inspect asset inventory system	
Inspect encryption settings for customer data	
Inspect access request forms	
Inspect termination tickets	
Inspect quarterly user access reviews	
Inspect remote access users	
Inspect MFA configurations	
Inspect firewall settings	
Inspect TLS and SFTP settings	
Inspect IDS configuration	
Inspect patch level on production servers	
Inspect antimalware software configurations	
Observe infrastructure monitoring tool	
Inspect security event tickets	

Inspect incident communications	
Inspect annual incident response testing	
Inspect software change tickets	
Inspect infrastructure change tickets	
Inspect data removal request tickets	

Robert Kluba CISM CISSP ASOCC
Managing Director
Phone: 408.656.9300

Robert.Kluba@AuditOneLLP.com

https://www.AuditOneLLP.com