

SOC Readiness Assessment

Sample Information Security Program Requirements

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

Change Management section	
Data Classification section	
Data Disposal section	
Data Retention section	
Data Loss Prevention section	
Employee Offboarding section	
Employee Onboarding section	
Incident Response section	
Monitoring section	
Physical Security section	
Risk Management section	
SDLC section	
Security Management section	
Third Party Testing section	
Vendor Management section	

Sample Evidence Requirements

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

Inspect annual Information Security Program update and approval	
Inspect security policies in place	
Inspect annual logical access review	
Inspect annual card key security group review	
Inspect annual third -party network vulnerability test report	
Inspect prior SOC report or third-party security audit	
Inspect audit finding tracking log	
Inspect strategic plans, business plans, forecasts	
Inspect public website	
Inspect internal wiki website	
Inspect board member profiles, resumes	
Inspect management meeting minutes, meeting agendas	
Inspect vendor agreements	
Inspect organizational chart	
Inspect card key security groups	

Inspect CCTV cameras and system	
Inspect data disposal form/tracking	
Inspect software development system	
Inspect incident reports	
Inspect incident response escalation process	
Inspect incident response communication process	
Inspect post incident process	
Inspect incident log	
Inspect incident response tabletop test	
Inspect password requirements	
Inspect network diagram	
Inspect firewall configurations	
Inspect antimalware software reports	
Inspect IPS/IDS reports	
Inspect local admin rights	
Inspect mobile device configuration	
Inspect system/network monitoring alerts/reports	
Inspect SFTP configuration	
Inspect TLS certificates	
Inspect signed job descriptions	
Inspect employee handbook and last update	
Inspect signed employee handbooks	
Inspect completed employee background checks	
Inspect employee offboarding forms	
Inspect employee onboarding forms	
Inspect employee training examples	
Inspect annual risk assessment	
Inspect annual risk assessment review by management	
Inspect sample changes for change management	

Robert Kluba CISM CISSP
Managing Director
Phone: 408.656.9300
Robert.Kluba@AuditOneLLP.com

<https://www.AuditOneLLP.com>