Year End Governance Checklist

POLICY AND PROCEDURES

Policy and Procedure Review	DONE	Policy and Procedure Review	DONE
Information Security	□	Acceptable Use	□
Disaster Recovery Plan	□	Backup and Restoration	□
Change Management	□	Security Awareness and Training	□
Network Security	□	Cloud Security	□
Access Control	□	Incident Response Plan	□
Configuration Management	□	Vendor Risk Management	□
Privileged Access Management	□	Data Protection and Privacy	□
Data Retention and Disposal	□	Patch Management	□
Encryption	□	Mobile Device Management	□
Business Continuity Plan	□	Vulnerability Management	□

CONTROL ACTIVITIES

Task Category	Description	DONE
Risk Assessment	Conduct annual risk assessment. This includes identifying new risks, updating existing risks, defining and implementing mitigation strategies.	□
Awareness Trainings	Perform annual awareness training(s). Security, privacy, and other role or industry-specific training may be required.	□
Access Control Reviews	Perform annual access reviews. Include human and non-human identities, verify completeness and accuracy of applications and systems included.	□

Task Category	Description	DONE
Incident Response Testing	Conduct annual tabletop exercise. Review playbooks, stakeholders (internal and external), and documentation standards, and adjust based on results of the exercise.	□
BC/DR Testing	Test disaster recovery plan. Include backup restorations, configuration review (completeness of systems and accuracy of settings to defined policies/expectations), and recovery SLA.	□
Vulnerability & Patch Management	Review VA/PM configurations and backlog. Ensure proper coverage and KPI are met around remediation. Lastly, review latest scans for known exploitable vulnerabilities (KEV).	□
Third-Party Risk Management	Perform annual third-party vendor reviews. Review of critical vendors to new and resolved risks, and ensure completeness and accuracy of vendor inventories.	□

TECHNICAL ASSESSMENTS

Vulnerability Assessment	Perform independent vulnerability assessment. Consider out-of-band vulnerability assessment to ensure all critical systems, including networks, applications, IoT, and cloud infrastructure are properly covered in the regularly scheduled efforts.	□
Penetration Testing	Conduct annual penetration test. Identify any exploitable weaknesses throughout the internal/external network, web applications, and cloud environments. Special focus on internally developed or contracted customer-facing systems.	□
Firewall/Router Configuration Reviews	Perform cybersecurity technology assessment(s). Identify security and operational improvements on firewalls, routers, and other critical network devices to ensure security.	□

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com

Have questions or need further details?
Email us today for personalized support.
Solutions@sdgc.com