

#	Baseline security area	Key requirement	Self-evaluation checkpoints	Score
1	Information Security Governance	Information security is formally directed and supported by leadership.	☐ Information security policies approved ☐ Security objectives defined ☐ Leadership oversight performed ☐ Cybersecurity risk assessments performed periodically ☐ Risks and remediation reviewed	___ / 5
2	Accountability & Communication	Security responsibilities, monitoring, and communication are clearly assigned.	☐ Security owner assigned ☐ Roles and responsibilities documented ☐ Security performance monitored ☐ Issues communicated to appropriate stakeholders ☐ Remediation actions tracked	___ / 5
3	People & Awareness	Employees and contractors understand their security responsibilities.	☐ Security responsibilities acknowledged ☐ Confidentiality obligations signed ☐ Security awareness training completed ☐ Acceptable use/code of conduct acknowledged ☐ Phishing simulations conducted ☐ Role-based security training performed	___ / 6
4	Access Management	Access to systems and data is limited to authorized users.	☐ Access requires approval ☐ Role-based access applied ☐ MFA enabled for key systems ☐ Separate administrative accounts used for privileged users ☐ Privileged access restricted ☐ Access reviewed periodically ☐ Access removed when no longer needed	___ / 7
5	Asset, Device & Network Security	Physical assets, virtual assets, endpoints, and networks are protected and monitored.	☐ Asset register maintained for physical and virtual assets ☐ Approved software inventory maintained ☐ Unsupported software identified and addressed ☐ Secure configuration baselines applied ☐ Endpoint Detection and Response (EDR) or equivalent endpoint protection enabled ☐ Infrastructure monitoring performed ☐ Endpoint patches applied timely ☐ Infrastructure patches applied timely ☐ Firewalls configured ☐ Network access restricted	___ / 10
6	Data Protection & Privacy	Sensitive and personal information is identified, protected, retained, and disposed of securely.	☐ Sensitive data identified ☐ Encryption used where required ☐ Privacy notice/consent in place ☐ Retention and disposal process defined ☐ Personal/customer data protected ☐ Non-production data use controlled ☐ Data classification policy defined	___ / 7
7	Monitoring & Incident Response	Security events are monitored and incidents are handled consistently.	☐ Logs enabled for key systems ☐ Alerts reviewed ☐ Incident response process documented ☐ Incidents tracked to resolution ☐ Breach notification process defined ☐ Tabletop exercises performed periodically	___ / 6
8	Change Management	System and application changes are	☐ Changes documented ☐ Changes risk-assessed ☐ Changes tested before production	___ / 6

		controlled before implementation.	☐ internally developed applications and AI-generated code reviewed prior to approval for deployment ☐ Changes approved before deployment ☐ Emergency changes reviewed after implementation	
9	Vulnerability Assessment & Penetration Testing	Vulnerabilities are identified, prioritized, tested, and remediated.	☐ Vulnerability scans performed periodically ☐ Penetration testing performed where applicable ☐ Findings risk-rated ☐ Critical/high findings remediated timely ☐ Remediation validated through rescanning and retesting prior to closure	___ / 5
10	Resilience & Recovery	The organization can recover from operational or cyber disruptions.	☐ Backups performed and monitored ☐ Backup restoration tested ☐ Business continuity plan documented ☐ Disaster recovery plan documented ☐ Recovery roles, call tree and communication defined ☐ Business continuity and disaster recovery plans tested periodically	___ / 6
11	Third-Party Risk Management	Vendors and service providers are assessed and managed.	☐ Critical vendors classified based on risk ☐ Vendor risk assessed before onboarding ☐ Security expectations documented for higher-risk providers ☐ Vendor access restricted and reviewed ☐ Vendor assurance reports reviewed where available	___ / 5
12	AI Governance & Responsible Use	AI tools are used responsibly, securely, and with appropriate human oversight.	☐ AI acceptable use expectations defined ☐ Inventory of approved AI tools maintained ☐ Staff trained on safe AI use ☐ Sensitive/client data restricted from unauthorized AI tools ☐ AI outputs reviewed before business use ☐ AI-developed applications or automations reviewed before production deployment ☐ AI risks, incidents, or misuse monitored and escalated	___ / 7

Total possible score: 75 points

Source: Sanjay Chadha