

Appendix 1 -

#	Baseline security area	Framework references
1	Information Security Governance	- NIST Cybersecurity Framework 2.0 – Govern - ISO/IEC 27001:2022 – Information Security Management Systems - CIS Critical Security Controls v8/v8.1
2	Accountability & Communication	- NIST Cybersecurity Framework 2.0 – Govern / Identify - ISO/IEC 27001:2022 – Roles, responsibilities, communication and monitoring - CIS Critical Security Controls v8/v8.1
3	People & Awareness	- ISO/IEC 27001:2022 – People, policies and technology approach - NIST Cybersecurity Framework 2.0 – Govern / Protect - CIS Critical Security Controls v8/v8.1 – Security awareness and skills training
4	Access Management	- CIS Critical Security Controls v8/v8.1 – Account and access management - NIST Cybersecurity Framework 2.0 – Protect - ISO/IEC 27001:2022 – Access control - UK Cyber Essentials – User access control
5	Asset, Device & Network Security	- CIS Critical Security Controls v8/v8.1 – Enterprise assets, software assets and network infrastructure - UK Cyber Essentials – Firewalls, secure configuration, security update management and malware protection - ASD Essential Eight – Patch applications / patch operating systems
6	Data Protection & Privacy	- ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection - NIST Cybersecurity Framework 2.0 – Identify / Protect - CIS Critical Security Controls v8/v8.1 – Data protection - ISO/IEC 27001:2022 – Information classification and data handling principles
7	Monitoring & Incident Response	- NIST Cybersecurity Framework 2.0 – Detect / Respond - CIS Critical Security Controls v8/v8.1 – Audit log management and incident response management - ISO/IEC 27001:2022 – Monitoring, corrective action and risk management
8	Change Management	- ISO/IEC 27001:2022 – ISMS requirements and continual improvement - NIST Cybersecurity Framework 2.0 – Govern / Protect - CIS Critical Security Controls v8/v8.1 – Secure configuration and software security
9	Vulnerability Assessment & Penetration Testing	- CIS Critical Security Controls v8/v8.1 – Continuous vulnerability management - NIST Cybersecurity Framework 2.0 – Identify / Protect - ASD Essential Eight – Patch applications and operating systems - UK Cyber Essentials – Security update management
10	Resilience & Recovery	- NIST Cybersecurity Framework 2.0 – Recover - ISO/IEC 27001:2022 – Cyber-resilience and operational excellence - CIS Critical Security Controls v8/v8.1 – Data recovery - ASD Essential Eight – Regular backups
11	Third-Party Risk Management	- NIST Cybersecurity Framework 2.0 – Govern / supply chain risk management - ISO/IEC 27001:2022 – Risk management and supplier/security management principles - CIS Critical Security Controls v8/v8.1 – Service provider management
12	AI Governance & Responsible Use	- NIST AI Risk Management Framework - ISO/IEC 42001:2023 - OWASP Top 10 for Large Language Model Applications - NIST AI RMF Generative AI Profile

Source: Sanjay Chadha