Annex-A	Title	Implemented	Corresponding Template
Clause	Organisational Controls		
5.1	Policies for information security		Information Security Manual Section 5.2 Information Security Policy
5.2	Information security roles and responsibilities		Information Security Manual Annex A5.2 Information Security Manual Section 5.3 Document Register
5.3	Segregation of duties		Information Security Manual Section 5.3 (Roles and Responsibilities) Information Security Manual Annex A5.3
5.4	Management Responsibilities		Information Security Manual Annex A5.4 Compliance Register Policy Document Register
5.5	Contact with Authorities		Information Security Manual Annex A5.5 Emergency, Authority and Special Interest Contacts
5.6	Contact with special interest groups		Information Security Manual Annex A5.6 Emergency, Authority and Special Interest Contacts
5.7	Threat intelligence		Information Security Manual Annex A5.7
5.8	Information security in project management		Information Security Manual Annex A5.8 Checklist for Internal Projects Involving Third Parties
5.9	Inventory of information and other associated assets		Information Security Manual Annex A5.9 Risk Assessment Workbook
5.10	Acceptable use of information and other associated assets		Information Security Manual Annex A5.10 Acceptable Use Policy Email Policy Internet Usage Policy Public WiFi Policy Mobile and remote working policy Information Classification and Data Handling Policy
5.11	Return of Assets		Information Security Manual Annex A5.11 Exit Interview Procedure Risk Assessment Workbook (assets tab)
5.12	Classification Of Information		Information Security Manual Annex A5.12 Information Classification and Data Handling Policy
5.13	Labelling of Information		Information Security Manual Annex A5.13
5.14	Information Transfer		Information Security Manual Annex A5.14 Information Classification Data Handling Policy Email Policy
5.15	Access Control		Information Security Manual Annex A5.15 Access Control Policy Keys and Locking Up Procedure
5.16	Identity Management		Information Security Manual Annex A5.16 Exit Interview Procedure
5.17	Authentication information		Information Security Manual Annex A5.17 Password Policy
5.18	Access rights		Information Security Manual Annex A5.18
5.19	Information security in supplier relationships		Information Security Manual Annex A5.19 Information Security Policy for Third Party Relationships
5.20	Addressing information security within supplier agreements		Information Security Manual Annex A5.20 Information Security Procedure for Third Party Relationships Checklist for Internal Projects Involving Third Parties Risk Assessment Workbook
5.21	Managing information security in the ICT supply chain		Information Security Manual Annex A5.21
5.22	Monitoring, review and change management of supplier services		Information Security Manual Annex A5.22
5.23	Information security for use of cloud services		Information Security Manual Annex A5.23
5.24	Information security incident management planning and preparation		Information Security Manual Annex A5.24 Information Security Manual Annex A6.8 (informaton Security Event Reporting) Information Security Manual Annex A5.25-28 Security Report Log Incident Management Procedure Incident Response Procedure
5.25	Assessment and decision on information security events		
5.26	Response to information security incidents		
5.27	Learning from information security incidents		
5.28	Collection of evidence		
5.29	Information security during disruption		Information Security Manual Annex A5.29 Business Continuity Plan
5.30	ICT readiness for business continuity		Information Security Manual Annex A5.30 Information Security Manual Annex A8.14

5.31	Legal, statutory, regulatory and contractual requirements		Information Security Manual Annex A5.31 Legislation document Documentation Register Records of Processing Cryptographic Controls Policy
5.32	Intellectual property rights		Information Security Manual Annex A5.32
5.33	Protection of records		Information Security Manual Annex A5.33
5.34	Privacy and protection of PII		Information Security Manual Annex A5.34 Documentation Register Records of Processing
5.35	Independent review of information security		Information Security Manual Annex A5.35
5.36	Compliance with policies, rules and standards for information security		Information Security Manual Annex A5.36
5.37	Documented operating procedures		Information Security Manual Annex A5.37 Documentation Register
6	People Controls		
6.1	Screening		Information Security Manual Annex A6.1 Employment Procedure
6.2	Terms and conditions of employment		Information Security Manual Annex A6.2
6.3	Information security awareness, education and training		Information Security Manual Section 7.3 (Awareness) Information Security Manual Annex A6.3 Compliance Register Policy Social Engineering Policy Acceptable Use of Assets Data Classification and Handling Policy
6.4	Disciplinary process		Information Security Manual Annex A6.4 Disciplinary Procedure
6.5	Responsibilities after termination or change of employment		Information Security Manual Annex A6.5 Exit Interview Procedure
6.6	Confidentiality or non-disclosure agreements		Information Security Manual Annex A6.6 Risk Assessment Workbook
6.7	Remote working		Information Security Manual Annex A6.7 Mobile and remote working policy
6.8	Information security event reporting		Information Security Manual Annex A5.3 (Roles and Responsibilities) Information Security Manual Annex A5.5 (Contact with Authorities) Emergency, Authority and Special Interest Contacts Information Security Manual Annex A6.8
7	Physical Controls		
7.1	Physical security perimeters		Information Security Manual Annex A7.1
7.2	Physical entry		Information Security Manual Annex A7.2 Keys and Locking Up Procedure
7.3	Securing offices, rooms and facilities		Information Security Manual Annex A7.3 Keys and Locking Up Procedure
7.4	Physical security monitoring		Information Security Manual Annex A7.4
7.5	Protecting against physical and environmental threats		Information Security Manual Annex A7.5
7.6	Working in secure areas		Information Security Manual Annex A7.6
7.7	Clear desk and clear screen		Information Security Manual Annex A7.7 Clear Desk Policy Mobile and remote working policy
7.8	Equipment siting and protection		Information Security Manual Annex A7.8 Keys and Locking Up Procedure
7.9	Security of assets off-premises		Information Security Manual Annex A7.9 Information Classifications and Handling Policy Mobile and remote working policy Acceptable Use Policy
7.10	Storage media		Information Security Manual Annex A7.10 Risk Assessment Workbook Information Classification and Data Handling Policy Disposal and Destruction Policy
7.11	Supporting utilities		Information Security Manual Annex A7.11
7.12	Cabling security		Information Security Manual Annex A7.12
7.13	Equipment maintenance		Information Security Manual Annex A7.13 Mobile and remote working policy (describes how users should maintain equipment adequately)
7.14	Secure disposal or re-use of equipment		Information Security Manual Annex A7.14 Commissioning and Re-Use Procedure
8	Technological Controls		

8.1	**User endpoint devices**		Information Security Manual Annex A8.1 Mobile and remote working policy Public WiFi Policy BYOD Policy
8.2	**Privileged access rights**		Information Security Manual Annex A8.2 Risk Assessment Workbook
8.3	**Information access restriction**		Information Security Manual Annex A8.3 Access Control Policy
8.4	**Access to source code**		Information Security Manual Annex A8.4
8.5	**Secure authentication**		Information Security Manual Annex A8.5 Access Control Policy MFA devices and users
8.6	**Capacity management**		Information Security Manual Annex A8.6
8.7	**Protection against malware**		Information Security Manual Annex A8.7 Malware Protection Policy
8.8	**Management of technical vulnerabilities**		Information Security Manual Annex A8.8 Technical Vulnerability Management Policy Information Security Manual Annex A5.36 (Compliance) Information Security Manual Annex A5.7 (Documented Operating Procedures)
8.9	**Configuration management**		Information Security Manual Annex A8.9
8.10	**Information deletion**		Information Security Manual Annex A8.10
8.11	**Data masking**		Information Security Manual Annex A8.11
8.12	**Data leakage prevention**		Information Security Manual Annex A8.12
8.13	**Information backup**		Information Security Manual Annex A8.13 Backup Policy
8.14	**Redundancy of information processing facilities**		Information Security Manual Annex A8.14
8.15	**Logging**		Information Security Manual Annex A8.15
8.16	**Monitoring activities**		Information Security Manual Annex A8.16
8.17	**Clock synchronization**		Information Security Manual Annex A8.17
8.18	**Use of privileged utility programs**		Information Security Manual Annex A8.18 Acceptable Use Policy
8.19	**Installation of software on operational systems**		Information Security Manual Annex A8.19 Request for Change Policy Acceptable Use Policy
8.20	**Networks security**		Information Security Manual Annex A8.20
8.21	**Security of network services**		Information Security Manual Annex A8.21 Firewall Configuration Policy
8.22	**Segregation of networks**		Information Security Manual Annex A8.22
8.23	**Web filtering**		Information Security Manual Annex A8.22
8.24	**Use of cryptography**		Information Security Manual Annex A8.24 Cryptographic Controls policy Information Classifications and Handling Policy
8.25	**Secure development life cycle**		Information Security Manual Annex A8.25 Secure Development Policy
8.26	**Application security requirements**		Information Security Manual Annex A8.26 Information Classification Data Handling Policy Cryptographic Controls policy Email Policy Secure Development Policy
8.27	**Secure system architecture and engineering principles**		Information Security Manual Annex A8.27 Secure Development Policy
8.28	**Secure coding**		Secure Development Policy
8.29	**Security testing in development and acceptance**		Information Security Manual Annex A8.29
8.30	**Outsourced development**		Information Security Manual Annex A8.30
8.31	**Separation of development, test and production environments**		Information Security Manual Annex A8.31
8.32	**Change management**		Information Security Manual Annex A8.32 Request for Change Policy RFC ID Record RFC request form
8.33	**Test information**		Information Security Manual Annex A8.33
8.34	**Protection of information systems during audit testing**		Information Security Manual Annex A8.34