Statement of Applicability including the templates supplied

Clause	Heading	Implemented?	Templates supplied
5.1	**Management direction for information security**		
5.1.1	Policies for information security	Y	Information Security Manual Section 5.2
5.1.2	Review of the policies for information security	Y	ISM 001- Information Security Manual Section 5.2
6.1	**Internal organization**		
6.1.1	Information security roles and responsibilities	Y	Information Security Manual Annex A6.1.1 Information Security Manual Section 5.3 Document Register
6.1.2	Segregation of duties	Y	Information Security Manual Annex A6.1.2
6.1.3	Contact with authorities	Y	Information Security Manual Annex A6.1.3 Special interest groups contacts
6.1.4	Contact with special interest groups	Y	Information Security Manual Annex A6.1.4 Special interest groups contacts
6.1.5	Information security in project management	Y	Information Security Manual Annex A6.1.5 Information Security Manual Annex A13.2 Internal Checklist for Projects With Third Parties
6.2	**Mobile devices and teleworking**		
6.2.1	Mobile device policy	Y	Information Security Manual Annex A6.2.1 Mobile and remote working policy Public WiFi Policy BYOD Policy
6.2.2	Teleworking	Y	Information Security Manual Annex A6.2.2 Mobile and remote working policy Business Continuity Plan
7.1	**Prior to employment**		
7.1.1	Screening	Y	Information Security Manual Annex A7.1.1 Scoping Form Asset Declaration Form HR record IDPr 058 - Employment Procedure
7.1.2	Terms and conditions of employment	Y	Information Security Manual Annex A7.1.2 Staff Handbook
7.2	**During employment**		
7.2.1	Management responsibilities	Y	Information Security Manual Annex A7.1.2 Compliance Register Policy Document Register Compliance Register Form HR Record
7.2.2	Information security awareness, education and training	Y	Information Security Manual Annex A7.2.2 Compliance Register Staff Training Record HR Record Security Awareness Presentations Social Engineering Policy
7.2.3	Disciplinary process	Y	Information Security Manual Annex A7.2.3 Staff Handbook

7.3	**Termination and change of employment**		
7.3.1	Termination or change of employment responsibilities	Y	Information Security Manual Annex A7.3.1 Exit Interview Procedure
8.1	**Responsibility for assets**		
8.1.1	Inventory of assets	Y	Information Security Manual Annex A8.1.1 Risk Assessment Workbook
8.1.2	Ownership of assets	Y	Information Security Manual Annex A8.1.2 Risk Assessment Workbook
8.1.3	Acceptable use of assets	Y	Information Security Manual Annex A8.1.3 Acceptable Use Policy Email Policy Internet Usage Policy Public WiFi Policy Mobile and remote working policy Information Classification and Data Handling Policy
8.1.4	Return of assets	Y	Information Security Manual Annex A8.1.4 Staff Handbook Exit Interview Procedure Risk Assessment Workbook
8.2	**Information classification**		
8.2.1	Classification of information	Y	Information Security Manual Annex A8.2.1 Information Classification and Data Handling Policy
8.2.2	Labelling of information	Y	Information Security Manual Annex A8.2.2
8.2.3	Handling of assets	Y	Information Security Manual Annex A8.2.3 Information Classification and Data Handling Policy
8.3	**Media handling**		
8.3.1	Management of removable media	Y	Information Security Manual Annex A8.3.1 Risk Assessment Workbook Information Classification and Data Handling Policy
8.3.2	Disposal of media	Y	Information Security Manual Annex A8.3.2 Disposal and Destruction Policy
8.3.3	Physical media transfer	Y	Information Security Manual Annex A8.3.3
9.1	**Business requirements of access control**		
9.1.1	Access control policy	Y	Information Security Manual Annex A9.1.1 Access Control Policy Keys and Locking Up Procedure
9.1.2	Access to networks and network services	Y	Information Security Manual Annex A9.1.2 Access Control Policy
9.2	**User access management**		
9.2.1	User registration and de-registration	Y	Information Security Manual Annex A9.2.1 Exit Interview Procedure
9.2.2	User access provisioning	Y	Information Security Manual Annex A9.2.2
9.2.3	Management of privileged access rights	Y	Information Security Manual Annex A9.2.3 Risk Assessment Workbook

9.2.4	Management of secret authentication information of users	Y	Information Security Manual Annex A9.2.4 Password Policy
9.2.5	Review of user access rights	Y	Information Security Manual Annex A9.2.5
9.2.6	Removal or adjustment of access rights	Y	Information Security Manual Annex A9.2.6
9.3	**User responsibilities**		
9.3.1	Use of secret authentication information	Y	Information Security Manual Annex A9.3.1 Password Policy
9.4	**System and application access control**		
9.4.1	Information access restriction	Y	Information Security Manual Annex A9.4.1 Access Control Policy
9.4.2	Secure log-on procedures	Y	Information Security Manual Annex A9.4.2 Access Control Policy MFA devices and users
9.4.3	Password management system	Y	Information Security Manual Annex A9.4.3
9.4.4	Use of privileged utility programs	Y	Information Security Manual Annex A9.4.4 Acceptable Use Policy
9.4.5	Access control to program source code	Y	Information Security Manual Annex A9.4.5
10.1	**Cryptographic controls**		
10.1.1	Policy on the use of cryptographic controls	Y	Information Security Manual Annex A10.1.1 Cryptographic Controls policy Cryptographic Controls Policy Information Classifications and Handling Policy
10.1.2	Key management	Y	Information Security Manual Annex A10.1.2 Cryptographic Controls Policy
11.1	**Secure areas**		
11.1.1	Physical security perimeter	Y	Information Security Manual Annex A11.1.1
11.1.2	Physical entry controls	Y	Information Security Manual Annex A11.1.2 Keys and Locking Up Procedure
11.1.3	Securing offices, rooms and facilities	Y	Information Security Manual Annex A11.1.3 Keys and Locking Up Procedure
11.1.4	Protecting against external and environmental threats	Y	Information Security Manual Annex A11.1.4
11.1.5	Working in secure areas	Y	Information Security Manual Annex A11.1.5
11.1.6	Delivery and loading areas	Y	Information Security Manual Annex A11.1.6
11.2	**Equipment**		
11.2.1	Equipment siting and protection	Y	Information Security Manual Annex A11.2.1 Keys and Locking Up Procedure
11.2.2	Supporting utilities	Y	Information Security Manual Annex A11.2.2
11.2.3	Cabling security	Y	Information Security Manual Annex A11.2.3
11.2.4	Equipment maintenance	Y	Information Security Manual Annex A11.2.4 Mobile and remote working policy
11.2.5	Removal of assets	Y	Information Security Manual Annex A11.2.5 Information Classification and Data Handling Policy Mobile and remote working policy Public WiFi Policy

11.2.6	Security of equipment and assets off-premises	Y	Information Security Manual Annex A11.2.6 Information Classification and Data Handling Policy Mobile and remote working policy Acceptable Use Policy
11.2.7	Secure disposal or re-use of equipment	Y	Information Security Manual Annex A11.2.7 Commissioning and Re-Use Procedure
11.2.8	Unattended user equipment	Y	Information Security Manual Annex A11.2.8 Mobile and remote working policy
11.2.9	Clear desk and clear screen policy	Y	Information Security Manual Annex A11.2.9 Clear Desk Policy Mobile and remote working policy
12.1	**Operational procedures and responsibilities**		
12.1.1	Documented operating procedures	Y	Information Security Manual Annex A12.1.1 Documentation Register
12.1.2	Change management	Y	Information Security Manual Annex A12.1.2 Request for Change Policy RFC ID Record RFC request form
12.1.3	Capacity management	Y	Information Security Manual Annex A12.1.3
12.1.4	Separation of development, testing and operational environments	Y	Information Security Manual Annex A12.1.4
12.2	**Protection from malware**		
12.2.1	Controls against malware	Y	Information Security Manual Annex A12.2.1 Malware Protection Policy
12.3	**Backup**		
12.3.1	Information backup	Y	Information Security Manual Annex A12.3.1 Backup Policy
12.4	**Logging and monitoring**		
12.4.1	Event logging	Y	Information Security Manual Annex A12.4.1
12.4.2	Protection of log information	Y	Information Security Manual Annex A12.4.2
12.4.3	Administrator and operator logs	Y	Information Security Manual Annex A12.4.3
12.4.4	Clock synchronization	Y	Information Security Manual Annex A12.4.4
12.5	**Control of operational software**		
12.5.1	Installation of software on operational systems	Y	Information Security Manual Annex A12.5.1 Request for Change Policy
12.6	**Technical vulnerability management**		
12.6.1	Management of technical vulnerabilities	Y	Information Security Manual Annex A12.6.1 Technical Vulnerability Management Policy
12.6.2	Restrictions on software installation	Y	Information Security Manual Annex A12.6.2 Acceptable Use Policy
12.7	**Information systems audit considerations**		
12.7.1	Information systems audit controls	Y	Information Security Manual Annex A12.7.1
13.1	**Network security management**		
13.1.1	Network controls	Y	Information Security Manual Annex A13.1.1

13.1.2	Security of network services	Y	Information Security Manual Annex A13.1.2 Firewall Configuration Policy
13.1.3	Segregation in networks	Y	Information Security Manual Annex A13.1.3
13.2	**Information transfer**		
13.2.1	Information transfer policies and procedures	Y	Information Security Manual Annex A13.2.1 Information Clasification Data handling Policy
13.2.2	Agreements on information transfer	Y	Information Security Manual Annex A13.2.2
13.2.3	Electronic messaging	Y	Information Security Manual Annex A13.2.3 Email Policy Information Classification and Data Handling Policy Social Engineering Policy
13.2.4	Confidentiality or non-disclosure agreements	Y	Information Security Manual Annex A13.2.4 Risk Assessment Workbook
14.1	**Security requirements of information systems**		
14.1.1	Information security requirements analysis and specification	Y	Information Security Manual Annex A14.1.1 Secure Development Policy
14.1.2	Securing application services on public networks	Y	Information Security Manual Annex A14.1.2 Information Classification and Data Handling Policy, Cryptographic Controls Policy Email Policy
14.1.3	Protecting application services transactions	Y	Information Security Manual Annex A14.1.3 Secure Development Policy
14.2	**Security in development and support processes**		
14.2.1	Secure development policy	Y	Information Security Manual Annex A14.2.1 Secure Development Policy
14.2.2	System change control procedures	Y	Information Security Manual Annex A14.2.2
14.2.3	Technical review of applications after operating platform changes	Y	Information Security Manual Annex A14.2.3
14.2.4	Restrictions on changes to software packages	Y	Information Security Manual Annex A14.2.4
14.2.5	Secure system engineering principles	Y	Information Security Manual Annex A14.2.5 Secure Development Policy
14.2.6	Secure development environment	Y	Information Security Manual Annex A14.2.6
14.2.7	Outsourced development	Y	Information Security Manual Annex A14.2.7
14.2.8	System security testing	Y	Information Security Manual Annex A14.2.8
14.2.9	System acceptance criteria	Y	Information Security Manual Annex A14.2.9
14.3	**Test data**		
14.3.1	Protection of test data	Y	Information Security Manual Annex A14.3.1
15.1	**Information security in supplier relationships**		
15.1.1	Information security policy for supplier relationships	Y	Information Security Manual Annex A15.1.1 Information Security Policy for Third Party Relationships
15.1.2	Addressing security within supplier agreements	Y	Information Security Manual Annex A15.1.2 Information Security Procedure for Third Party Relationships Checklist for Internal Projects With Third Parties Risk Assessment Workbook
15.1.3	Information and communication technology supply chain	Y	Information Security Manual Annex A15.1.3

15.2	**Supplier service delivery management**		
15.2.1	Monitoring and review of supplier services	Y	Information Security Manual Annex A15.2.1
15.2.2	Managing changes to supplier services	Y	Information Security Manual Annex A15.2.2
16.1	**Management of information security incidents and improvements**		
16.1.1	Responsibilities and procedures	Y	Information Security Manual Annex A16.1 Security Report Log Building Security Report Log Incident Management Procedure
16.1.2	Reporting information security events	Y	
16.1.3	Reporting information security weaknesses	Y	
16.1.4	Assessment of and decision on information security events	Y	
16.1.5	Response to information security incidents	Y	Information Security Manual Annex A16.1.5 Incident Response Procedure
16.1.6	Learning from information security incidents	Y	Information Security Manual Annex A16.1 Security Report Log Building Security Report Log
16.1.7	Collection of evidence	Y	
17.1	**Information security continuity**		
17.1.1	Planning information security continuity	Y	Information Security Manual Annex A17.1.1 Business Continuity Plan
17.1.2	Implementing information security continuity	Y	Information Security Manual Annex A17.1.2
17.1.3	Verify, review and evaluate information security continuity	Y	Information Security Manual Annex A17.1.3
17.2	**Redundancies**		
17.2.1	Availability of information processing facilities	Y	Information Security Manual Annex A17.2.1
18.1	**Compliance with legal and contractual requirements**		
18.1.1	Identification of applicable legislation and contractual requirements	Y	Information Security Manual Annex A18.1.1 Legislation document Documentation Register Records of Processing Computer Misuse Act
18.1.2	Intellectual property rights (IPR)	Y	Information Security Manual Annex A18.1.2
18.1.3	Protection of records	Y	Information Security Manual Annex A18.1.3
18.1.4	Privacy and protection of personally identifiable information	Y	Information Security Manual Annex A18.1.4 Documentation Register Records of Processing
18.1.5	Regulation of cryptographic controls	Y	Information Security Manual Annex A18.1.5 Cryptographic Controls Policy
18.2	**Information security reviews**		
18.2.1	Independent review of information security	Y	Information Security Manual Annex A18.2.1
18.2.2	Compliance with security policies and standards	Y	Information Security Manual Annex A18.2.2
18.2.3	Technical compliance review	Y	Information Security Manual Annex A18.2.3