Personal Data Security Control Set

Annex A reference	Control title	Control description	Deter / DnR / Defend / EC	Comments
A.5	**Security Policy**			
A5.1	**Information security policy**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**		
A.5.1.1	Information security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	EC	The supplier is required to operate to ISO 27001 and evidence this through regular assessment
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and	EC	
A.6	**Organization of information security**			
A.6.1	**Internal Organization**	**To manage information security within the organization.**		
A.6.1.1	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.	EC	The supplier is required to ensure that all operations and management is aligned with ISO27001 requirements. The supplier is expected to evidence this with appropriate policy, governance and audit. A SIRO must be appointed.
A.6.1.2	Information security coordination	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job function.	EC	As 27K
A.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.	EC	GPG 47 should be utilised as a guide and evidence must be provided that all mandatory areas of responsibility in the organisation are appropriately covered even if the direct roles as specified in GPG 47 are not allocated.
A.6.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented.	EC	The solution must be accredited to IL2 however the solution must demonstrate compliance with IL3 control sets through internal accreditation
A.6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.	EC	As per IS2 or equivalent
A.6.1.6	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	EC	As per IS2 or equivalent
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	EC	As per IS2 including requirement to provide equivalent monitoring and reporting to a central HSC function as defined.
A.6.1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	EC	The supplier is required to engage with the contracting authority audit and assurance functions on a defined basis (once per year by default) to

A6.2	**External parties**	**To maintain the security of organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.**		
A.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	EC	As per IS2
A.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	EC	As per IS2 with regard to any HSC specific guidance on access control, identity and confidentiality
A.6.2.3	Addressing security in third party contracts	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	EC	As per IS2
A.7	**Asset Management**			
A.7.1	**Responsibility for assets**	**To achieve and maintain appropriate protection of organizational assets.**		
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	DnR for Supplier Solution DETER for Customer	DnR for supplier environment - demonstrate through audit and assurance DETER for customer, core service may provide tooling to assist customers (reporting/logging) however the scope for the supplier is to protect against malicious endpoints not enforce overly prescriptive security controls on them.
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	DETER for Supplier	As per IS2 Supporting guidance for consuming orgs
A.7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	DnR for Supplier	DETER for users - IGT / GPGs / IGTT DnR - supplier to ensure security awareness and education of all staff related to the service provision which should also be provided to HSCIC staff operating at a detailed level with the supplier.
A.7.2	**Information classification**	**To ensure that information receives an appropriate level of protection.**		
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	DETER	As per IS2
A.7.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.	DnR	Assessed as part of the initial NHSMail2 risk assessment provided to suppliers
A.8	**Human resources security**			
A.8.1	**Prior to employment**	**To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.**		

A.8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	DnR Supplier will need to evidence compliance or equivalence to the vetting and personnel controls described in Personnel Security. This should be applied in response to the appropriate levels of access to the system and service	As per 6.1.3
A.8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	DnR	IS2 or equivalent
A.8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.	DnR	IS2 or equivalent
A.8.2	**During employment**	**To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**		
A.8.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	DnR	As per IS2
A.8.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	DnR	As per IS2
A.8.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	DnR	As per IS2
A.8.3	**Termination or change of employment**	**To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.**		
A.8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	DnR	As per IS2
A.8.3.2	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	DnR	As per IS2
A.8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	DnR	As per IS2
A.9	**Physical and environmental security**			

A9.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's premises and information.**		
A9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	DETER / DnR	Appropriate accreditation and assurance must be evidenced to demonstrate compliance or equivalence to the controls as set out in Security Policy 4.
A9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	DETER / DnR	Section 9 is DETER for supporting office environments which do not connect or directly engage with the service environment
A9.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	DETER / DnR	Section 9 is DnR for data halls, service support environment and any supporting facilities which connect to or directly engage with the service environment
A9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.	DETER / DnR	NOTE: we do not expect full compliance with high level control GPGs such as TEMPEST
A9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.	DETER / DnR	
A9.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	DETER / DnR	
A9.2	**Equipment security**	**To prevent loss, damage, theft or compromise of assets and interruption to organization's activities.**		
A9.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	DETER / DnR	
A9.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	DETER / DnR	
A9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	DETER / DnR	
A9.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	DETER / DnR	
A9.2.5	Security of equipment off-premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	DETER / DnR	
A9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	DETER / DnR	
A9.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.	DETER / DnR	
A10	**Communications and operations management**			
A10.1	**Operational procedures and responsibilities**	**To ensure the correct and secure operation of information processing facilities.**		

A10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	DETER	This to be enforced as part of regular audit and assurance by the contracting authority
A10.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	DETER	
A10.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	DETER	
A10.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	DETER	
A10.2	**Third party service delivery management**	**To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.**		
A10.2.1	Service Delivery	It shall be ensured that the security controls, service definitions, and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	DETER	
A10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.	DETER	
A10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	DETER	
A10.3	**System planning and acceptance**	**To minimize the risk of systems failure.**		
A10.3.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	DETER	
A10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system's) carried out during development and prior to acceptance.	DETER	
A10.4	**Protection against malicious and mobile code**	**To protect the integrity of software and information.**		
A10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	DnR for Supplier DETER for customer	DETER for users - IGT / GPGs / IGTT
A10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	DnR for Supplier DETER for customer	Covered by Requirement 3.1.3.2
A10.5	**Back-up**	**To maintain the integrity and availability of information and information processing facilities.**		

A10.5.1	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	DnR	Refer to Availability requirement(s) 3.5.2
A10.6	**Network security management**	**To ensure the protection of information in networks and the protection of the supporting infrastructure.**		
A10.6.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	DnR	
A10.6.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	DnR	
A10.7	**Media handling**	**To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.**		
A10.7.1	Management of removable media	There shall be procedures in place for the management of removable media.	DEFEND - supplier	
A10.7.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	DETER	
A10.7.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.	HSC SPECIFIC	This is determined by HSC guidance and policy as issued by the DoH
A10.7.4	Security of system documentation	System documentation shall be protected against unauthorized access.	DETER	
A10.8	**Exchange of information**	**To maintain the security of information and software exchanged within an organization and with any external entity.**		
A10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.	DEFEND - supplier	This applies to the operation of the service and the back end services and operations only. It DOES NOT apply to customer connectivity.
A10.8.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.	DEFEND - supplier DETER - users	DETER for users will be covered by access agreement/ToU etc.
A10.8.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	DnR	This applies to the potential for physical "man in a van" type migration activities and other backup operations.
A10.8.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	DETER	
A10.8.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	DETER	
A10.9	**Electronic commerce services**	**To ensure the security of electronic commerce services, and their secure use.**		

A10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	DETER	There is no intention for the service to directly support or provide e-commerce services.
A10.9.2	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message	DETER	
A10.9.3	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	DETER	
A10.10	**Monitoring**	**To detect unauthorized information processing activities.**		
A10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	DnR	
A10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	DnR	
A10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	DnR	
A10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	DnR	
A10.10.5	Fault logging	Faults shall be logged, analyzed, and appropriate action taken.	DETER	
A10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	DETER	Current HSC advice is to use a STRATUM 2 time source
A11	**Access Control**			
A11.1	**Business requirement for access control**	**To control access to information.**		
A11.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	DnR	
A11.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to information systems.**		
A11.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	DnR	IS7 or equivalent
A11.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	DnR	
A11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	DnR	
A11.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	DnR	

A11.3	**User responsibilities**	**To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**		
A11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	DnR - Supplier DETER - User	User to be defined in ToU/AuP enforced in system controls - User awareness driven through IGT / IGTT and GPGs
A11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	DnR - Supplier DETER - User	User to be defined in ToU/AuP enforced in system controls - User awareness driven through IGT / IGTT and GPGs
A11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	DnR - Supplier DETER - User	User to be defined in ToU/AuP enforced in system controls - User awareness driven through IGT / IGTT and GPGs
A11.4	**Network access control**	**To prevent unauthorized access to networked services.**		
A11.4.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.	DnR	Stated control Policies/GPGs or evidenced equivalence
A11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	DnR	
A11.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	DnR	
A11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	DnR	
A11.4.5	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	DnR	
A11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	DnR	
A11.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	DnR	
A11.5	**Operating system access control**	**To prevent unauthorized access to operating systems.**		
A11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	DnR	Evidenced demonstration of compliance or equivalence of controls. A number of control recommendations in this section may be provided by alternate and equivalent means where the risk mitigation is demonstrated to be equivalent or better.
A11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	DnR	
A11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	DnR	
A11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	DnR	

A11.5.5	Session time-out	Inactive sessions shall be shut down after a defined period of inactivity.	DnR	
A11.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	DnR	
A11.6	**Application and information access control**	**To prevent unauthorized access to information held in application systems.**		
A11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	DETER	
A11.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	DETER	
A11.7	**Mobile computing and Teleworking**	**To ensure information security when using mobile computing and teleworking facilities.**		
A11.7.1	Mobile computing and communications	A formal policy shall be in place, and security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	DnR - Supplier DETER - User	User to be defined in ToU/AuP enforced in system controls - User awareness driven through IGT / IGTT and GPGs
A11.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	DnR - Supplier DETER - User	
A12	**Information systems acquisition, development and maintenance**			
A12.1	**Security requirements of information systems**	**To ensure that security is an integral part of information systems.**		
A12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	DnR	
A12.2	**Correct processing in applications**	**To prevent errors, loss, unauthorized modification or misuse of information in application.**		
A12.2.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.	DETER	To be validated through assurance and security testing
12.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	DETER	
12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.	DETER	
12.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	DETER	
A12.3	**Cryptographic controls**	**To protect the confidentiality, authenticity or integrity of information by cryptographic means.**		
A12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	DETER	HSC ACS Standard

12.3.2	Key management	Key management shall be in place to support the organization's use of cryptographic techniques.	DETER	HSC ACS Standard
A12.4	**Security of system files**	**To ensure the security of system files**		
A12.4.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems	DETER	As per IS2
A12.4.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	DETER	
A12.4.3	Access control to program source code	Access to program source code shall be restricted.	DETER	As per IS2
A12.5	**Security in development and support processes**	**To maintain the security of application system software and information.**		
A12.5.1	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	DETER	Additional controls provided by suppliers should demonstrate good management and awareness in this area potentially above DETER but not at a level which would warrant significant system or operation change
A12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	DETER	
A12.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	DETER	
A12.5.4	Information leakage	Opportunities for information leakage shall be prevented.	DETER	
A12.5.5	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.	DETER	
A12.6	**Technical Vulnerability Management**	**To reduce risks resulting from exploitation of published technical vulnerabilities.**		
A12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	DnR	
A13	**Information security incident management**			
A13.1	**Reporting information security events and weaknesses**	**To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**		
A13.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	DETER	As per IS2 including requirement to provide equivalent monitoring and reporting to a central HSC function as defined.
A13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	DETER	

A13.2	**Management of information security incidents and improvements**	**To ensure a consistent and effective approach is applied to the management of information security incidents.**		
A13.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	DETER	
A13.2.2	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	DETER	
A13.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	DETER	
A14	**Business continuity management**			
A14.1	**Information security aspects of business continuity management**	**To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**		
A14.1.1	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	DETER	Refer to Availability requirement(s) 3.5.2
A14.1.2	Business continuity and risk analysis	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	DETER	
A14.1.3	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	DETER	
A14.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	DETER	
A14.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.	DETER	
A15	**Compliance**			
A15.1	**Compliance with legal requirements**	**To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.**		

A15.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.	DETER	
A15.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	DETER	
A15.1.3	Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	DETER	
A15.1.4	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	DETER	
A15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.	DETER	
A15.1.6	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.	DETER	
A15.2	**Compliance with security policies and standards, and technical compliance**	**To ensure compliance of systems with organizational security policies and standards**		
A15.2.1	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	DETER	
A15.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	DETER	
A15.3	**Information system audit considerations**	**To maximize the effectiveness of and to minimize interference to/from the information systems audit process.**		
A15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	DETER	
A15.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	DETER	

Please refer to HMG IA Standard Numbers 1 & 2 - Supplement Technical Risk Assessment and Risk Treatment where any additional detail is needed.

Key	
EC	Enterprise Control
DnR	DETECT & RESIST