The Scottish public sector action plan cyber resilience framework Supersedes this and all previous versions of this Information Security Policy Framework.

This Document Has Been Superseded

This Document Has Been Superseded

Network & Information Systems Regulations 2018

Information Security Policy Framework

Guidance

Version 1.4
11 July 2019

Contact email:
HealthCA@gov.scot

Website:
www.healthca.scot

Revision History:
v. 1.4 Final
Superseded 03/11/2021

This Document Has Been Superseded

This Document Has Been Superseded

Contents

This Document Has Been Superseded

1. Purpose

To present a revised NHSS Information Security Policy Framework guidance that incorporates legal compliance requirements for the Network and Information Systems (NIS) Regulations 2018[1] and the information security elements of the General Data Protection Regulation (GDPR)[2].

2. Rationale

NHS Scotland has had an Information Security Policy Framework, aligned to ISO 27001/2, since 2015[3,4]. The introduction of NIS and GDPR in May 2018 placed legal compliance requirements on health boards, the National Cyber Security Centre and Information Commissioner's Office (ICO) presented guidance on the information and cyber security elements of these regulations as the Cyber Assessment Framework (CAF)[5] for NIS and the Security Outcomes for GDPR[2].

To minimise the regulatory burden on health boards the Scottish Health Competent Authority (CA) has incorporated these guidances into the 2018 NHSS Information Security Policy Framework (ISPF).

This single 2018 framework therefore integrates the controls of ISO27001:2013, alongside the legal compliance requirements of NIS:2018 and GDPR:2018 thereby obviating the need for health boards to reference to all three standards. Although not a legal requirement, the 2018 ISPF controls additionally address the features of the Public Sector Action Plan (PSAP) and Cyber Essentials (CE) to which health boards need to comply with independent assurance verification of the CE critical controls.

3. Structure of the 2018 Framework

To lessen the change impact on health boards, the overall structure of the 2015 ISPF, that was aligned to ISO 27001, has been retained.

Some controls have been augmented with additional requirements (as shown by the CAF and ICO cross-references) while additional control categories have been incorporated into the framework to explicitly address NIS compliance (Table 3.1).

In addition, the narrative-based requirements of the 2015 ISPF and ISO27001 have been integrated into the new control framework (Table 3.2). This approach provides a consistency of approach and simplifies the operational deployment of the framework.

Finally, the guidance from the ICO regarding cyber risk aspects of GDPR has been included with cross-references into the controls.

---

[1] Statutory Instruments, 2018 No. 506, Electronic Communications. The Network and Information Systems Regulations 2018, April 2 018, 36pp. http://www.legislation.gov.uk/id/uksi/2018/506

[2] GDPR Security Outcomes. https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes#quicktabs-guidances_tabs1, May 2018.

[3] NHSScotland Information Security Policy Framework, July 2015, 9pp.

[4] NHSScotland Information Security Policy Framework: ANNEX NHSS Reference Control Objectives and Controls, July 2015, 24pp.

[5] NIS Directive - Cyber Assessment Framework, https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework, April 2018.

This Document Has Been Superseded

4. NIS Audit and Assurance

The Competent Authority is required by Article 15 of the NIS regulations to conduct formal assessments and audits of health boards to obtain compliance assurance.

The 2018 NHSS ISPF shall be adopted as the basis for these compliance assessments and audits.

TABLE 3.1 New additional category controls in the 2018 Framework

Additional controls added to the 2018 ISPF	
1) Governance	7) Organisation of information security: device management
2) Risk Management	13) Asset Management: Information & data storage & protection

TABLE 3.2 Narrative aspects of the 2015 ISPF incorporated into the 2018 Framework controls

Narrative in 2015 ISPF	Incorporation into 2018 ISPF Controls
1) Leadership and commitment	1) Governance
2) Information Security Objectives	1) Governance
3) Information Security Policy	3) Information Security Policy
4) Information Security Management System (ISMS)	4) Information Security Management System (ISMS)
5) Information Risk Assessment	2) Risk Management
6) Information Security Risk Treatment	2) Risk Management
7) Performance evaluation	41) Compliance: information security reviews
8) Internal audit	41) Compliance: information security reviews
9) Management review and improvement	4) Information Security Management System

5. ISPF mapping to the Cyber Resilience Framework (CRF)

The Scottish Government Cyber Resilience Framework applies to all public bodies in Scotland, including health boards and Local Authorities. This will have the benefit of a uniform set of criteria for cyber security across all public bodies and for health will have the added benefit of better enabling the integration of health and care between the NHS and Local Authorities in a manner consistent with the Digital Health and Care Strategy[6].

As noted, NIS Audits and Reviews shall be performed using the ISPF controls, but to aid the familiarisation and migration of health boards to the CRF, the findings shall be reported under the categories of the CRF.

[6] Scottish Government, Scotland's Digital Health & Care Strategy, April 2018, 20pp.

This Document Has Been Superseded

As a guide to the relationship between the ISPF and CRF, Annex 1 shows a mapping of the ISPF controls to the CRF categories.

This Document Has Been Superseded

6. Controls

1) Governance

Objective
The Board and Chief Executive shall demonstrate leadership and commitment with respect to information security management by ensuring that the information security policy, security objectives and information security management system (ISMS) are established, supported at Board-level and deliver legal compliance.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Leadership & commitment (ISO: 5.1a) (CAF: A1a)	There is effective organisational security management led at board level and articulated clearly in corresponding policies. The approach and policy relating to the security of networks and information systems supporting the delivery of essential services are set and managed at board level. Regular board discussions on the security of network and information systems take place, based on timely and accurate information and informed by expert guidance. The importance of effective information security management and of conforming to the information security management system requirements is communicated
b) Policy & Direction (ISO: 5.1, 5.2) (CAF: A1c)	The board shall establish an information security policy and management system that integrates well into the other functions, processes and risk assessments of the organisation (e.g. Information Governance, eHealth and estates/physical security and Human Resources).
c) Operational performance (ISO: 5.1)	Direction is set at board level and is translated into effective organisational practices that direct and control the security of the networks and information systems. The performance on the ISMS is reported to the management board at regular intervals to ensure that the information security management system achieves its intended outcomes. The board promotes continual improvement.
d) Resources (ISO: 5.1)	The board shall ensure that resources needed for the effective operation of the ISMS are available and are supported by senior management.
e) Communication (ISO: 5.1)	The board shall ensure that all of the above is communicated to staff, business partners and the wider public to ensure that trust and confidence is maintained in health and care services.
f) Roles & responsibilities (ISO: 5.1) (CAF: A1b)	The board shall: • Appoint a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level. • Assign the role of senior information risk owner (SIRO) at executive level

This Document Has Been Superseded

	• Be clear that the roles in information security are part of a professional specialist discipline and career home and not a generalist NHS administration role. • Designate a permanent role of Board Information Security Officer/Manager that encompasses all information risks (not just 'IT Security') and is of appropriate grade and standing. • Assure the appointed person(s) shall be competent and have the necessary specialist training and experience. • Provide on-going training and support for information security personnel and for this to be documented. • Ensure that the personnel are able to participate fully in national-level communities (IG and ISO Fora) and governance structures (e.g. Public Benefit and Privacy Panel) and accreditation work (e.g. Scottish Wide Area Network and services used across Boards) so that national level information risks are addressed in an effective way.

2) Risk Management

Objective
The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Risk management process (CAF: A2.a)	Security risks to networks and information systems relevant to essential services are identified, analysed, prioritised and managed though a documented risk management policy and processes. Risk owners are identified.
b) Risk assessments (CAF A2.a)	Risk assessments shall be based on a clearly articulated set of threat assumptions, informed by an up-to-date understanding of relevant security threats and the vulnerabilities in the organisation's networks and information systems. Risk assessments shall be conducted when significant events potentially affect the essential service, such as replacing a system, technical changes to networks and information systems, change of use and new threat information. The output from the risk assessment shall be a set of security requirements that will address the risks in line with the organisational approach to security and risk appetite. The effectiveness of the risk management process is reviewed periodically and improvements made as required.
c) Risk treatment (ISO: A. 6.1.3) (CAF: A1.c) (ICO: A2)	Appropriate information security risk treatment options shall be identified to address the information risk assessment results. This shall include a determination of all the controls necessary to treat the information security risk treatment options.

This Document Has Been Superseded

	The risk treatment options shall be developed into an information security risk treatment plan communicated to risk owners. Produce a statement of applicability that contains the necessary controls and justification for inclusions, exclusions and whether actually implemented.
d) Communication (CAF A2.a)	Significant conclusions reached in the course of the risk management process are communicated to key security decision-makers and accountable individuals.

3) Information Security Policy

Objective
To provide management direction and support for information security objectives and service protection in accordance with the business requirements and relevant laws and regulations.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Policies for information security (ISO: A.5.1.1) (CAF: B1.a)	The senior management shall define information security objectives for the organisation. These will be delivered by a set of practical, usable and appropriate policies that shall be defined, approved by management, published and communicated to employees and other relevant parties. These should include the overarching security governance and risk management approach, technical security practices and processes that mitigate the risk of service disruption.
b) Review of the policies for information security (ISO: A.5.1.2) (CAF: B1.a, B1.b)	To be reviewed and evaluated at planned intervals, or if significant changes occur, to ensure their continuing suitability, adequacy and effectiveness.
c) Policy integration (ISO: 4.1) (CAF: B1.b)	Security policies and processes are integrated with other organisational policies and processes, including personnel security screening and assessments and the Digital Health & Care Strategy 2018.

This Document Has Been Superseded

4) Information Security Management System

Objective
As an integral aspect of organisational information security governance, the organisation shall establish, implement, maintain and continually improve an information security management system.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Scope (ISO: 4.3)	Each board shall determine the boundaries and scope of its ISMS and associated policy. The board ISMS and associated policy should be defined to cover all the operations of the health board, this shall include interfaces and dependencies between activities performed by the board and those that are performed by other organisations.
b) Planning (ISO: 6.1.1)	The board shall: • Establish the risks that may prevent the ISMS from being established, working as intended and being able to achieve continual improvement. • Consider how far the ISMS needs to work beyond the current information security function but requires interaction with resource elsewhere (information governance, records management etc.) • Take action to address these risks at executive level.
c) Resources (ISO: 5.1c; 7.1)	The board shall determine and provide the resources needed for the establishment and continual improvement of the ISMS.
d) Staff awareness and communications (ISO: 7.4)	The Board shall put in place the means to conduct internal and external communications and awareness relevant to its information security management system. The outcome should be: • The information security management policy and associated security objectives should be freely available to all employees, interested parties and the wider public. • Board level policies and guidance should be available to all staff and interested parties digitally (e.g. via the Intranet). • There is a form of mandatory induction for all new personnel in regard to board information security policy and that this is followed. • There is a process to enable information security updates, advice and other content to be available in a timely manner.

This Document Has Been Superseded

e) Documentation (ISO: 7.5)	The board shall hold documented information relating to the design and effective running of its ISMS. • To be held in the board-approved corporate records management system. • For information relating to the ISMS to be held as one or more discrete functions within a file plan/business classification scheme and managed according to Board records disposal and retention schedules. • To be easily accessible to persons requiring them to support the smooth running of the ISMS, kept up to date and subject to the security and access permissions commensurate with the sensitivity.
f) Review (ISO: 9.1, 9.2 9.3)	The SIRO in conjunction with the executive management team should review the Board's information security management system at planned intervals to ensure its continuing suitability and effectiveness. Such review will include consideration of: • Status of actions from previous management reviews. • Changes in external and internal issues which are relevant. • Non-conformities in the ISMS and preventative/corrective actions. • Monitoring and measurement of results. • Audit results. • Results of high-level or significant risk assessment and risk treatment plans. • Feed-back from interested parties incl. patients. • Significant security incident reports at board and national level.
g) Improvement (ISO: 10.1,10.2) (CAF: A1.a)	The outputs of the management review shall include decisions related to continual improvement, opportunities and any changes needed to the information security management system. The Board, acting through the CEO, SIRO and senior management team will react when nonconformity occurs - over and above any regular audit and management review - and take action to deal with it including change to the information security management system. The Board recognises the circular nature of the ISMS: to plan, action, check and plan again so as to make continual improvement.

This Document Has Been Superseded

5) Organisation of Information Security

Objective
To establish a management framework and initiate and control the implementation and operation of information security within the organisation.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information security roles and responsibilities (ISO: A.6.1.1)	All information security responsibilities shall be defined and allocated.
b) Segregation of duties (ISO: A.6.1.2)	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets
c) Contact with authorities (ISO: A.6.1.3)	Appropriate contacts with the authorities shall be maintained.
d) Contact with special interest groups (ISO: A.6.1.4)	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
e) Information security in project management (ISO: A.6.1.5)	Information security shall be addressed in project management, regardless of the type of the project.

6) Organisation of information security: mobile devices and teleworking

Objective
To ensure the security of teleworking and mobile devices.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Mobile device & media policy (ISO: A.6.2.1) (CAF: B3.a)	A policy and supporting security measures and user behaviour shall be adopted to manage the risks introduced by using mobile devices and storage media.
b) Mobile device management (CAF: B3.d)	Mobile devices that hold data are catalogued, controlled by the organisation and configured according to best practice for the platform, with appropriate technical and procedural policies in place. Only the minimum amount of data required is stored on mobile devices.
c) Remote wipe capability (CAF: B3.d)	The organisation can remotely wipe all mobile devices of corporate data and information. Some data may be automatically deleted off mobile devices after a certain period.
d) Teleworking (ISO: A.6.2.2) (CAF: B3.a)	A policy and supporting measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

This Document Has Been Superseded

7) Organisation of information security: device management

Objective
To ensure only trusted devices, networks and services are permitted to access networks, information systems and data.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Dedicated devices (CAF: B2.b)	Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.
b) Third party networks and devices (CAF: B2.b)	There is independent or professional assurance of the security of third-party networks. Only third-party devices / networks dedicated to supporting organisational systems are permitted to connect.
c) Device identity management (CAF: B2.b)	Device identity management, which is cryptographically backed, is performed to only allow known devices to access systems.
d) Device discovery and scanning (CAF: B2.b)	Regular discovery scans are performed to detect unknown devices and investigate any findings.

8) Human Resource Security: prior to employment

Objective
To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Screening (ISO: A.7.1.1)	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
b) Terms and conditions of employment (ISO: A.7.1.2)	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.

This Document Has Been Superseded

9) Human Resource Security: during employment

Objective
To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Management responsibilities (ISO: A.7.2.1)	Management shall require all employees and contractors to apply information security in accordance with established policies and procedures of the organisation.
b) Information security awareness, education and training (ISO: A.7.2.2) (CAF: B1.b, B6.b)	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function. Staff security training and awareness activities are monitored, evaluated and updated at suitable intervals. Cyber security information and good practice guidance is easily and widely available.
c) Reporting incidents (CAF: B6.a)	Staff at all levels are encouraged to report incidents, are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored.
d) Disciplinary process (ISO: A.7.2.3)	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

10) Human Resource Security: termination and change of employment

Objective
To protect the organisation's interests as part of the process of changing or terminating employment.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Termination or change of employment responsibilities (ISO: A.7.3.1)	Information security management responsibilities and duties that remain valid after termination or change in employment shall be defined, communicated to the employee or contractor and enforced.

11) Asset Management: responsibility for assets

Objective
To identify organisational assets and define appropriate protection responsibilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Inventory of assets (ISO: A.8.1.1)	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
b) Ownership of assets (ISO: A.8.1.2)	Assets maintained in the inventory shall be owned.
c) Acceptable use of the assets (ISO: A.8.1.3)	Rules for the acceptable use of information and of the assets associated with information and information processing facilities shall be identified, documented and implemented.

This Document Has Been Superseded

d) Return of assets (ISO: A.8.1.4)	All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.

12) Asset Management: Information Classification & Lifecycle

Objective
To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Classification of information (ISO: A.8.2.1) (CAF: B3.a)	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
b) Labelling of information (ISO: A.8.2.2)	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme to be adopted by the organisation.
c) Handling of assets (ISO: A.8.2.3) (CAF: B3.a)	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation. User access to sensitive information is controlled.
d) Information and data lifecycle (CAF: B3.a)	Policies on the lifecycle management of information and data shall be developed from creation through retention and destruction. This will include documentation of retention times for data categories and evidence of audit procedures for information destruction.
e) Information asset register (CAF A3.a)	Key information assets and their owners shall be identified and documented in an Information Asset Register (IAR). Impact on assets needs to be assessed in terms of confidentiality, integrity and availability.

13) Asset Management: Information & data storage & protection

Objective
To ensure that information and data storage is managed and protected.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information and data protection (CAF: B3.c)	There is suitable physical or technical means in place to protect stored data from unauthorised access, modification or deletion. Necessary historic or archive data is suitably secured in storage.
b) Service resilience (CAF: B3.c, D1.b)	There are secured backups of data (electronic or hardcopy) that are available to allow service delivery continuity should the original data not be available.

This Document Has Been Superseded

t

14) Asset Management: media handling	
Objective Non stated.	
Sub-control (ISO 27001-CAF-ICO Ref. no.)	**Detail**
a) Management of removable media (ISO: A.8.3.1)	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.
b) Disposal of media (ISO: A.8.3.2)	Media shall be disposed of securely when no longer required, using formal procedures.
c) Physical media transfer (ISO: A.8.3.3)	Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.

15) Access control: business requirements of access control	
Objective To assure good management and maintenance of identity and access control of networks and information systems.	
Sub-control (ISO 27001 Reference no.)	**Detail**
a) Access control policy (ISO: A.9.1.1) (CAF: B2.d)	An access control policy shall be established, documented and reviewed based on the business and information security requirements.
b) Access to networks and network services (ISO: A.9.1.2) (CAF: B2.d)	Users shall only be provided with access to the networks and network services that they have been specifically authorised to use with permissions regularly reviewed. All access is logged and monitored.

This Document Has Been Superseded

16) Access control: user access management

Objective
To ensure authorised user access and to prevent unauthorised access to systems and services.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) User registration and de-registration (ISO: A.9.2.1) (CAF: B2.c)	A formal user registration, review and de-registration process shall be implemented to enable assignment of access rights.
b) User access provisioning (ISO: A.9.2.2) (CAF: B2.c, B2.d)	A formal user access provisioning and review process shall be implemented to assign or revoke access rights for all user types to all systems and services.
c) Management of privileged access rights (ISO: A.9.2.3) (CAF B2.a, B2.c, B2.d)	The allocation and use of privileged access rights shall be restricted and controlled and limited to the minimum necessary. Privileged user access is routinely monitored with sessions recorded for analysis and investigation as required.
d) Device access management (CAF: B2.c)	Privileged access is only granted on devices owned and managed by the organisation.
e) Management of secret authentication information of users (ISO: A.9.2.4)	The allocation of secret authentication information shall be controlled through a formal management process.
f) Review of user access rights (ISO: A.9.2.5) (CAF: B2.a, B2.c)	Asset owners shall review individual users' access rights to networks and systems supporting the essential service at regular intervals.
g) Removal or adjustment of access rights (ISO: A.9.2.6)	The access rights of all employees and external party users to the information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

17) Access control: user responsibilities

Objective
To make users accountable for safeguarding their authentication information.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Use of secret authentication information (ISO: A.9.3.1)	Users shall be required to follow the organisation's practices in the use of the secret authentication information.

This Document Has Been Superseded

18) Access control: system and application access control

Objective
To prevent unauthorised access to systems and applications.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information access restriction (ISO: A.9.4.1)	Access to information and application system functions shall be restricted in accordance with the access control policy.
b) Secure log-on procedures (ISO: A.9.4.2) (CAF: B2.a)	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure, utilising additional authentication mechanisms, such as two-factor or hardware-backed certificates.
c) Password management system (ISO: A.9.4.3)	Password management systems shall be interactive and shall ensure quality passwords.
d) Use of privileged utility programs (ISO: A.9.4.4)	The use of utility programs that might be capable of overriding systems and applications shall be restricted.
e) Access control to programme source code (ISO: A.9.4.5)	Access to program source code shall be restricted.
f) Remote access (CAF: B2.a)	Additional authentication mechanisms, such as two-factor or hardware-backed certificates, are deployed to individually authenticate and authorise all remote access to all networks and information systems that support your essential service.
g) Unauthorised access (CAF B2.d)	Attempts by unauthorised users to connect to systems are alerted, promptly assessed and investigated where relevant.

19) Cryptographic controls

Objective
To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Policy on the use of cryptographic controls (ISO: A.10.1)	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
b) Key management (ISO: A.10.2)	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

This Document Has Been Superseded

20) Physical and environmental security: secure areas

Objective
To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Physical security perimeter (ISO: A.11.1.1)	Security perimeter shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
b) Physical entry controls (ISO: A.11.1.2)	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
c) Securing offices, rooms and facilities (ISO: A.11.1.3)	Physical security for offices, rooms and facilities shall be designed and applied.
d) Protecting against external and environmental threats (ISO: A.11.1.4)	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
e) Working in secure areas (ISO: A.11.1.5)	Procedures for working in secure areas shall be designed and applied.
f) Delivery and loading areas (ISO: A.11.1.6)	Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled, and if possible, isolated from information processing facilities to avoid unauthorised access.

This Document Has Been Superseded

21) Physical and environmental security: equipment

Objective
To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Equipment siting and protection (ISO: A.11.2.1)	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for un-authorised access.
b) Supporting utilities (ISO: A.11.2.2) (CAF: A3.a)	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
c) Cabling security (ISO: A.11.2.3)	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
d) Equipment maintenance (ISO: A.11.2.4)	Equipment shall be correctly maintained to ensure its continued availability and integrity.
e) Removal of assets (ISO: A.11.2.5)	Equipment, information or software shall not be taken off-site without prior authorisation.
f) Security of equipment and assets off-premises (ISO: A.11.2.6)	Security shall be applied to off-site assets taking into account the different risks of working outside of the organisation's premises.
g) Secure disposal or re-use of equipment (ISO: A.11.2.7)(CAF B3.e)	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
h) Unattended user equipment (ISO: A.11.2.8)	Users shall ensure that unattended equipment has appropriate protection.
i) Clear desk and clear screen policy (ISO: A.11.2.9)	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

22) Operations security: procedures and responsibilities

Objective
To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Documented operating procedures (ISO: A.12.1.1)	Operating procedures shall be documented and made available to all users who need them.
b) Change management (ISO: A.12.1.2) (CAF: C1.a)	Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled and the implications for information and data access considered. This includes the installation of new or updated systems.
c) Capacity management (ISO: A.12.1.3)	The use of network resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

This Document Has Been Superseded

d) Separation of development, testing and operational environments (ISO: A.12.1.4)	Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.

23) Operations security: protection from malware

Objective
To ensure that information and information processing facilities are protected against malware.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Controls against malware (ISO: A.12.2.1) (CAF: B4.c)	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
b) Threat intelligence (CAF C1.d)	Threat intelligence measures are in place. New signature updates and indicators of compromise for all protective technologies (e.g. AV, IDS) are deployed within a reasonable (risk-based) time of receipt.

24) Operations security: back up

Objective
To protect against loss of data and enable service recovery.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information back-up (ISO: A.12.3.1) (CAF B3.c, B5c, D1.b; ICO D.1)	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
b) Information recovery and restoration (CAF B5.c, D1.b; ICO D.1))	Backups are secured at centrally accessible or secondary sites to enable disaster recover from an extreme event.
c) Operational recovery roles (CAF: B5.c, D1b; ICO D.1)	Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service

25) Operations security: logging and monitoring

Objective
To record events and generate evidence.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Event logging (ISO: A.12.4.1) (CAF: B2.c, B2.d)	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
b) Protection of log information (ISO: A.12.4.2) (CAF: C1.b; ; ICO C.1)	Logging facilities and log information shall be protected against tampering and unauthorised access. All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.
c) Administrator and operator logs (ISO: A.12.4.3) (CAF: B2.c)	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

This Document Has Been Superseded

d) Access to logs (CAF C1.b)	Access to logging data is limited to those with business need and no others. Legitimate reasons for accessing logging data are given in use policies and users are trained on this.
e) Clock synchronisation (ISO: A.12.4.4)	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.

26) Operations security: control of operational software

Objective
To ensure the integrity of the operational systems.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Installation of software on operational systems (ISO: A.12.5.1) (CAF:B4.b)	Procedures shall be implemented to control the installation of software on operational systems.
b) Software configuration (CAF:B4.b)	Standard users cannot change software settings that would impact security or business operation.

27) Operations security: technical vulnerability management

Objective
To prevent the exploitation of technical vulnerabilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Management of technical vulnerabilities (ISO: A.12.6.1; CAF: B4.d)	Knowledge about the technical vulnerabilities of information systems being used shall be obtained in a timely fashion, or the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. NOTE: **PSAP** requires adoption of the National Cyber Security Centre's Active Cyber Defence (ACD) Programme.
b) Systems and software vulnerability remediation. (CAF: B4.d; ICO B.4)	Vulnerabilities for all software packages, network equipment and operating systems are tracked, prioritised and mitigated (e.g. by patching) promptly. Where practicable only supported software, firmware and hardware in networks and information systems shall be employed. NOTE: **Cyber Essentials & PSAP** require software up to date, licensed and supported, removed from devices when no longer supported, critical or high risk vulnerabilities patched within 14 days of an update being released.
c) Restrictions on software installation (ISO: A.12.6.2; B4.b)	Rules governing the installation of software by users shall be established and implemented.
d) Security testing and audit (CAF: B4.d)	The vulnerabilities of the networks and information systems that support your essential service are regularly tested (at least annually) and verified through third-party audits and penetration testing.

This Document Has Been Superseded

This Document Has Been Superseded

28) Operations security: incident identification procedures

Objective
To identify security events that might impact service delivery.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) User behaviour monitoring (CAF: C1.a; ; ICO C.1)	User activity is monitored in relation to essential services and personal data processing. Policy violations can be detected against an agreed list of suspicious or undesirable behaviour.
b) Information and data access (CAF: C1.a; ; ICO C.1)	Information and data monitoring can reliably detect security incidents.
c) Internal systems (CAF: C1.a)	Monitoring coverage includes internal and host-based monitoring.
d) Boundary monitoring (CAF: C1.a)	End point protection and network perimeter monitoring is in place and is capable of incident detection.
e) Alert management (CAF: C1.c; ; ICO C.1)	The monitoring systems in place have the capacity to distinguish alterations relating to networks, malware, data with associated incident management procedures. Genuine security incidents can be distinguished from false alarms.
f) Staff resources (CAF C1.e, D1.b)	Designated staff responsible for investigating and reporting monitoring alerts are in place with the necessary authority, skills and tools to identify, prioritise, determine action responses and investigate incidents.
g) Abnormal system behaviour (CAF: C2.a, C2b; ICO C.1)	Normal system communications and data flows activity are known, defined and recorded to permit abnormalities in system behaviour to be identified and used to detect malicious activity. Routine searches for such abnormalities are performed for alert generation.

29) Operations security: information systems audit considerations

Objective
To prevent the exploitation of technical vulnerabilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information systems audit controls (ISO: A.12.7.1)	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

This Document Has Been Superseded

30) Communications security: network security management	
Objective To ensure the protection of information in networks and its supporting information processing facilities.	
Sub-control (ISO 27001-CAF-ICO Ref. no.)	**Detail**
a) Network controls (ISO: A.13.1.1) (B4.c)	Networks shall be managed and controlled to protect information in systems and applications. Systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.
b) Security of network services (ISO: A.13.1.2)	Security mechanisms, service levels, and management requirements of all network services shall be identified and included in the network services agreements, whether these services are provided in-house or outsourced.
c) End point protection and network monitoring. (CAF: C1.a; ; ICO C.1)	Networks are monitored in order to detect potential security incidents that could affect the organisation's operations and delivery of essential services.
d) Network security reviews (CAF: B4.c)	There are regular reviews and updates to technical knowledge about networks and information systems, such as documentation and network diagrams, and these are securely stored.
e) Segregation in networks (ISO: A.13.1.3) (CAF: B4.a)	Groups of information services, data, users and information systems shall be segregated on networks into discrete security zones.
f) Network resilience (CAF: B5.b)	Operational systems are segregated from other business and external systems by appropriate technical and physical means. Internet services, such as browsing and email, are not accessible from essential service operational systems.

This Document Has Been Superseded

31) Information & data transfer

Objective
To maintain the security of information and data transferred, within an organisation and with any external entity.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information transfer policies and procedures (ISO: A.13.2.1) (CAF: B3.b)	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. This includes appropriate physical or technical means to protect data that travels over an untrusted carrier
b) Information & data flows (CAF: B3.d, B4a)	Information and data flows have been mapped; the associated network links have been identified and appropriate protection is in place.
c) Agreement on information transfers 9ISO: A.13.2.2)	Agreements shall address the secure transfer of business information between the organisation and external parties.
d) Electronic messaging (ISO: A.13.2.3)	Information involved in electronic messaging shall be appropriately protected. NOTE: **PSAP** requires adoption of the National Cyber Security Centre's Active Cyber Defence (ACD) Programme
e) Confidentiality or non-disclosure agreements (ISO: A.13.2.4)	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.

32) System acquisition, development and maintenance: security requirements of information systems

Objective
To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information security requirements analysis and specification (ISO: A.14.1.1)	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
b) Securing application services on public networks (ISO: A.14.1.2)	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.
c) Protecting application service transactions (ISO: A.14.1.3)	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

This Document Has Been Superseded

33) System acquisition, development and maintenance: security in development & support processes

Objective
To ensure that information security is designed and implemented within the development lifecycle of information systems.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Secure design and development policy (ISO: A.14.2.1) (CAF: B4.a, B4.b)	Rules for the development and secure configuration of software and systems shall be established and applied to developments within the organisation.
b) System change control procedures (ISO: A.14.2.2) (B4.b)	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures and documented.
c) Restriction on changes to software packages (ISO: A.14.2.4) (CAF:B4.b)	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
d) Secure system engineering principles (ISO: A.14.2.5) (CAF:B4.b)	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts. All platforms conform to a secure baseline build specification.
e) Secure development environment (ISO: A.14.2.6) (CAF: B4.a)	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle
f) Outsourced development (ISO: A.14.2.7)	The organisation shall supervise and monitor the activity of outsourced system development.
g) System security testing (ISO: A.14.2.8)	Testing of security functionality shall be carried out during development.
h) System acceptance testing (ISO: A.14.2.9)	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

34) System acquisition, development and maintenance: test data

Objective
To ensure the protection of data used for testing.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Protection of test data (ISO: A.14.3.1)	Test data shall be selected carefully, protected and controlled.

This Document Has Been Superseded

35) Supplier relationships: information security in supplier relationships

Objective
To ensure protection of the organisation's assets that is accessible by suppliers.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Information security policy for supplier relationships (ISO: A.15.1.1) (CAF: A4.a)	Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.
b) Addressing security within supplier agreements (ISO: A.15.1.2) (CAF: A4.a, B3,e)	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide ICT infrastructure components for, the organisation's information. This shall include sanitisation of third-party storage media.
c) Information and communications technology supplier chain (ISO: A.15.1.3) (CAF: A4.a)	Agreements with suppliers shall include assurance procedures and requirements to address the information security risks associated with information and communications technology services across the product supply chain, to include sub-contractors. Data and information flows with appropriate encryption shall be mapped and documented with associated risk assessments. NOTE: **PSAP** requires adoption of the Supply Chain Security guidance.

36) Supplier relationships: supplier service delivery management

Objective
To maintain an agreed level of security and service delivery in line with supplier agreements.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Monitoring and review of supplier services (ISO: A.15.2.1) (CAF: A4.a)	Organisations shall regularly monitor, review and audit supplier service delivery and associated security provisions.
b) Managing changes to supplier services (ISO: A.15.2.2) (CAF: A4.a)	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

This Document Has Been Superseded

37) Information security incident response, management and improvement

Objective
To ensure a consistent and effective approach to the management of information security incidents, including communications on security events and weaknesses.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Responsibilities and procedures (ISO: A.16.1.1) (CAF: B6.a, D1.a)	Management roles, responsibilities and procedures shall be established, communicated and documented in an incident response plan to ensure quick, effective and orderly response to information security incidents. The plan shall incorporate supply chain and third-party service response actions.
b) Reporting information security incidents (ISO: A.16.1.2; CAF: B6.a)	Information security events shall be reported through appropriate management channels as quickly as possible and staff members are encouraged to report incidents. Incidents should be reported following the Scottish Health Competent Authority process.
c) Reporting information security weaknesses (ISO: A.16.1.3; CAF: B6.a)	Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
d) Assessment of and decision on information security events (ISO: A.16.1.4)	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
e) Response to information security incidents (ISO: A.16.1.5; CAF: D1.b)	Information security incidents shall be responded to in accordance with documented procedures.
f) Learning from information security incidents (ISO: A.16.1.6; CAF: C1.d; ICO D.2)	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents and shared with the security community. Note: **PSAP** requires Scottish public bodies that are responsible for managing their own networks to become active participants in the Cyber Security Information Sharing Partnership (CiSP).
g) Collection of evidence (ISO: A.16.1.7)	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence.

This Document Has Been Superseded

38) Information security aspects of business continuity management: information security continuity

Objective
Information security continuity shall be embedded in the organisation's business continuity management systems.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Planning information security continuity (ISO: A.17.1.1) (CAF: B5.a, B6.a)	The organisation shall determine its requirements for information security and the continuity of information security management in adverse conditions, e.g. during a crisis or disaster. Staff across the organisation participate in cyber security planning activities and improvements, building joint ownership and bringing knowledge of their area of expertise
b) Implementing information security continuity (ISO: A.17.1.2) (CAF: B5.a, D1.b)	The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
c) Information and data transfer resilience (CAF: B3.b)	The organisation shall have alternative networks, communication bearers and transmission paths to mitigate the risk of service disruption.
d) Verify, review and evaluate information security continuity (ISO: A.17.1.3) (CAF: B5.a, B5.b, D1.c)	The organisation shall test and verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. Exercise scenarios are composed, documented, regularly reviewed, and validated. Findings are documented and used to refine incident response plans and protective security, in line with the lessons learned.
e) Lessons learned (ISO: A.17.1.3; CAF: D2a, D2.b)	Post-incident investigations shall include a root cause analysis to ensure appropriate remediating action is taken to protect against future incidents and improve security measures. Security improvements identified shall be prioritised, with the highest priority improvements completed in a timely manner.

This Document Has Been Superseded

39) Information security aspects of business continuity management: redundancy & resilience

Objective
To ensure availability of information processing facilities.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Availability of information processing facilities (ISO: A.17.2.1) (CAF: B5.b, D1.b))	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
b) Resilient connectivity (CAF: B5.b)	Resource limitations on bandwidth have been identified and mitigated. Systems co-dependency have been identified and mitigated. Network connectivity has alternative bearers, physical paths and service providers with no common single point of failure.

40) Compliance: compliance with legal and contractual requirements

Objective
To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and or any security requirements.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Identification of applicable legislation and contractual requirements (ISO: A.18.1.1)	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.
b) Intellectual property rights (ISO: A.18.1.2)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
c) Protection of records (ISO: A.18.1.3)	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislation, regulatory, contractual or business requirements.
d) Privacy and identification of personally identifiable information (ISO: A.18.1.4)	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
e) Regulation of cryptographic controls (ISO: A.18.1.5)	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

This Document Has Been Superseded

41) Compliance: information security reviews

Objective
The Board shall conduct audits at planned intervals to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

Sub-control (ISO 27001-CAF-ICO Ref. no.)	Detail
a) Independent review of information security (ISO: A.18.2.1)	The organisation'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 occur.
b) Compliance with security policies and standards (ISO: A.18.2.2)	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
c) Technical compliance review (ISO: A.18.2.3)	Information systems shall be independently reviewed at an agreed frequency for compliance with the organisation's information security policies and standards. The audit shall be conducted to a defined scope and criteria and shall be carried out by persons that are qualified, objective and impartial.
d) Performance evaluation	There shall be routine evaluations of the information security performance and the effectiveness of the information security management system. This shall include the appropriateness of monitoring security processes, controls efficacy and analysis of incidents. The methodology shall be documented to enable a trend analysis through comparable and reproducible results. The results shall be communicated to the SIRO and other appropriate senior management.
e) Assurance (CAF A2.b)	The security measures that are in place to protect the networks and information systems shall be regularly validated by an independent third party through appropriate assurance methods to ensure remain effective for the lifetime over which they are needed. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

This Document Has Been Superseded

Annex 1: NHSS ISPF Controls Mapping to CRF

NHSS ISPF 2018	Cyber Resilience Framework (CRF)
1) Governance	
a) Leadership & commitment (ISO: 5.1a) (CAF: A1a)	1.1
b) Policy & Direction (ISO: 5.1, 5.2) (CAF: A1c)	1.1
c) Operational performance (ISO: 5.1)	1.2
d) Resources (ISO: 5.1)	1.2
e) Communication (ISO: 5.1)	1.1
f) Roles & responsibilities (ISO: 5.1) (CAF: A1b)	1,1. 1.2, 6.2
2) Risk Management	
a) Risk management process (CAF: A2.a)	2.1, 2.4
b) Risk assessments (CAF A2.a)	2.2
c) Risk treatment (ISO: A. 6.1.3) (CAF: A1.c) (ICO: A2)	2.3
d) Communication (CAF A2.a)	1.2
3) Information Security Policy	
a) Policies for information security (ISO: A.5.1.1) (CAF: B1.a)	1.1, 1.2, 2.1, 5.1
b) Review of the policies for information security (ISO: A.5.1.2) (CAF: B1.a, B1.b)	5.1
c) Policy integration (ISO: 4.1) (CAF: B1.b)	5.1
4) Information Security Management System	
a) Scope (ISO: 4.3)	5.1
b) Planning (ISO: 6.1.1)	2.2
c) Resources (ISO: 5.1c; 7.1)	1.2
d) Staff awareness and communications (ISO: 7.4)	1.1, 1.2, 6.2, 6.3, 16.3
e) Documentation (ISO: 7.5)	5.1, 5.2, 8.3
f) Review (ISO: 9.1, 9.2 9.3)	1.5, 5.1, 13.9
g) Improvement (ISO: 10.1,10.2) (CAF: A1.a)	1.5, 16.4
5) Organisation of Information Security	
a) Information security roles and responsibilities (ISO: A.6.1.1)	1.2, 3.2, 6.2
b) Segregation of duties (ISO: A.6.1.2)	6.2
c) Contact with authorities (ISO: A.6.1.3)	16.2
d) Contact with special interest groups (ISO: A.6.1.4)	16.2
e) Information security in project management (ISO: A.6.1.5)	5.1
6) Organisation of information security: mobile devices and teleworking	
a) Mobile device & media policy (ISO: A.6.2.1) (CAF: B3.a)	9.1, 9.2
b) Mobile device management (CAF: B3.d)	9.2
c) Remote wipe capability (CAF: B3.d)	9.4
d) Teleworking (ISO: A.6.2.2) (CAF: B3.a)	6.5
7) Organisation of information security: device management	
a) Dedicated devices (CAF: B2.b)	8.3, 8.4
b) Third party networks and devices (CAF: B2.b)	1.5, 3.3, 8.4
c) Device identity management (CAF: B2.b)	9.2
d) Device discovery and scanning (CAF: B2.b)	13.4
8) Human Resource Security: prior to employment	
a) Screening (ISO: A.7.1.1)	6.1

This Document Has Been Superseded

b) Terms and conditions of employment (ISO: A.7.1.2)	6.1
9) Human Resource Security: during employment	
a) Management responsibilities (ISO: A.7.2.1)	1.2
b) Information security awareness, education and training (ISO: A.7.2.2) (CAF: B1.b, B6.b)	1.2, 6.3, 16.3
c) Reporting incidents (CAF: B6.a)	16.2
d) Disciplinary process (ISO: A.7.2.3)	6.2, 6.3
10) Human Resource Security: termination and change of employment	
a) Termination or change of employment responsibilities (ISO: A.7.3.1)	6.2, 8.1
11) Asset Management: responsibility for assets	
a) Inventory of assets (ISO: A.8.1.1)	1.4
b) Ownership of assets (ISO: A.8.1.2)	1.4
c) Acceptable use of the assets (ISO: A.8.1.3)	5.1, 6.2, 6.3
d) Return of assets (ISO: A.8.1.4)	6.2
12) Asset Management: Information Classification & Lifecycle	
a) Classification of information (ISO: A.8.2.1) (CAF: B3.a)	5.4
b) Labelling of information (ISO: A.8.2.2)	5.4
c) Handling of assets (ISO: A.8.2.3) (CAF: B3.a)	5.4
d) Information and data lifecycle (CAF: B3.a)	5.2
e) Information asset register (CAF A3.a)	5.5
13) Asset Management: Information & data storage & protection	
a) Information and data protection (CAF: B3.c)	17.1
b) Service resilience (CAF: B3.c, D1.b)	17.2, 17.3
14) Asset Management: media handling	
a) Management of removable media (ISO: A.8.3.1)	5.2, 9.2
b) Disposal of media (ISO: A.8.3.2)	9.1
c) Physical media transfer (ISO: A.8.3.3)	9.2
15) Access control: business requirements of access control	
a) Access control policy (ISO: A.9.1.1) (CAF: B2.d)	8.1
b) Access to networks and network services (ISO: A.9.1.2) (CAF: B2.d)	8.2, 12.1, 13.9
16) Access control: user access management	
a) User registration and de-registration (ISO: A.9.2.1) (CAF: B2.c)	8.1
b) User access provisioning (ISO: A.9.2.2) (CAF: B2.c, B2.d)	8.1
c) Management of privileged access rights (ISO: A.9.2.3) (CAF B2.a, B2.c, B2.d)	8.3, 8.4, 14.7
d) Device access management (CAF: B2.c)	8.3, 14.2
e) Management of secret authentication information of users (ISO: A.9.2.4)	8.3
f) Review of user access rights (ISO: A.9.2.5) (CAF: B2.a, B2.c)	3.3, 8.1, 8.3, 8.4, 12.1, 14.7
g) Removal or adjustment of access rights (ISO: A.9.2.6)	3.3, 6.2, 8.1, 8.3, 8.4, 12.1
17) Access control: user responsibilities	
a) Use of secret authentication information (ISO: A.9.3.1)	6.2
18) Access control: system and application access control	
a) Information access restriction (ISO: A.9.4.1)	5.1, 8.1
b) Secure log-on procedures (ISO: A.9.4.2) (CAF: B2.a)	8.2, 8.3, 8.4
c) Password management system (ISO: A.9.4.3)	8.1, 12.1
d) Use of privileged utility programs (ISO: A.9.4.4)	8.3
e) Access control to programme source code (ISO: A.9.4.5)	8.3
f) Remote access (CAF: B2.a)	3.3, 5.1

This Document Has Been Superseded

g) Unauthorised access (CAF B2.d)	8.2
19) Cryptographic controls	
a) Policy on the use of cryptographic controls (ISO: A.10.1)	9.3
b) Key management (ISO: A.10.2)	9.3
20) Physical and environmental security: secure areas	
a) Physical security perimeter (ISO: A.11.1.1)	11.1
b) Physical entry controls (ISO: A.11.1.2)	11.1, 11.2
c) Securing offices, rooms and facilities (ISO: A.11.1.3)	11.1, 11.2
d) Protecting against external and environmental threats (ISO: A.11.1.4)	10.1, 10.2
e) Working in secure areas (ISO: A.11.1.5)	11.2
f) Delivery and loading areas (ISO: A.11.1.6)	11.1
21) Physical and environmental security: equipment	
a) Equipment siting and protection (ISO: A.11.2.1)	11.1
b) Supporting utilities (ISO: A.11.2.2) (CAF: A3.a)	4.3, 7.1, 11.2
c) Cabling security (ISO: A.11.2.3)	4.3
d) Equipment maintenance (ISO: A.11.2.4)	4.3
e) Removal of assets (ISO: A.11.2.5)	4.2
f) Security of equipment and assets off-premises (ISO: A.11.2.6)	4.2, 6.5
g) Secure disposal or re-use of equipment (ISO: A.11.2.7)(CAF B3.e)	4.1, 9.1, 9.2
h) Unattended user equipment (ISO: A.11.2.8)	6.2, 6.3
i) Clear desk and clear screen policy (ISO: A.11.2.9)	6.2, 6.3
22) Operations security: procedures and responsibilities	
a) Documented operating procedures (ISO: A.12.1.1)	5.1
b) Change management (ISO: A.12.1.2) (CAF: C1.a)	12.1, 12.3
c) Capacity management (ISO: A.12.1.3)	12.1
d) Separation of development, testing and operational environments (ISO: A.12.1.4)	7.1, 14.4
23) Operations security: protection from malware	
a) Controls against malware (ISO: A.12.2.1) (CAF: B4.c)	4.2, 13.1, 14.1
b) Threat intelligence (CAF C1.d)	4.2, 14.1, 15.1
24) Operations security: back up	
a) Information back-up (ISO: A.12.3.1) (CAF B3.c, B5c, D1.b; ICO D.1)	17.2
b) Information recovery and restoration (CAF B5.c, D1.b; ICO D.1))	17.1, 17.3, 17.4
c) Operational recovery roles (CAF: B5.c, D1b; ICO D.1)	17.3, 17.6
25) Operations security: logging and monitoring	
a) Event logging (ISO: A.12.4.1) (CAF: B2.c, B2.d)	8.3, 13.1, 13.9
b) Protection of log information (ISO: A.12.4.2) (CAF: C1.b; ; ICO C.1)	13.9
c) Administrator and operator logs (ISO: A.12.4.3) (CAF: B2.c)	8.3, 8.4
d) Access to logs (CAF C1.b)	8.3
e) Clock synchronisation (ISO: A.12.4.4)	15.2
26) Operations security: control of operational software	
a) Installation of software on operational systems (ISO: A.12.5.1) (CAF:B4.b)	4.2
b) Software configuration (CAF:B4.b)	12.1
27) Operations security: technical vulnerability management	
a) Management of technical vulnerabilities (ISO: A.12.6.1; CAF: B4.d)	13.4
b) Systems and software vulnerability remediation. (CAF: B4.d; ICO B.4)	4.2, 13.1, 13.2, 13.3, 13.4, 13.6
c) Restrictions on software installation (ISO: A.12.6.2; B4.b)	12.1
d) Security testing and audit (CAF: B4.d)	12.4

This Document Has Been Superseded

28) Operations security: incident identification procedures	
a) User behaviour monitoring (CAF: C1.a; ; ICO C.1)	13.9
b) Information and data access (CAF: C1.a; ; ICO C.1)	13.1, 13.2
c) Internal systems (CAF: C1.a)	13.2
d) Boundary monitoring (CAF: C1.a)	13.2, 14.6
e) Alert management (CAF: C1.c; ; ICO C.1)	13.1, 13.2
f) Staff resources (CAF C1.e, D1.b)	13.2, 13.5, 16.3
g) Abnormal system behaviour (CAF: C2.a, C2b; ICO C.1)	13.5, 15.1, 15.2
29) Operations security: information systems audit considerations	
a) Information systems audit controls (ISO: A.12.7.1)	1.5
30) Communications security: network security management	
a) Network controls (ISO: A.13.1.1) (B4.c)	14.2
b) Security of network services (ISO: A.13.1.2)	3.1
c) End point protection and network monitoring. (CAF: C1.a; ; ICO C.1)	15.2
d) Network security reviews (CAF: B4.c)	12.1
e) Segregation in networks (ISO: A.13.1.3) (CAF: B4.a)	7.1, 8.3, 12.2, 14.2, 14.4, 14.5
f) Network resilience (CAF: B5.b)	7.1, 12.2
31) Information & data transfer	
a) Information transfer policies and procedures (ISO: A.13.2.1) (CAF: B3.b)	5.6
b) Information & data flows (CAF: B3.d)	5.3, 5.6, 12.2
c) Agreement on information transfers 9ISO: A.13.2.2)	5.6
d) Electronic messaging (ISO: A.13.2.3)	13.2
e) Confidentiality or non-disclosure agreements (ISO: A.13.2.4)	3.1
32) System acquisition, development and maintenance: security requirements of information systems	
a) Information security requirements analysis and specification (ISO: A.14.1.1)	12.2
b) Securing application services on public networks (ISO: A.14.1.2)	12.2, 12.4, 13.3
c) Protecting application service transactions (ISO: A.14.1.3)	5.6, 12.2
33) System acquisition, development and maintenance: security in development & support processes	
a) Secure design and development policy (ISO: A.14.2.1) (CAF: B4.a, B4.b)	12.1, 12.2
b) System change control procedures (ISO: A.14.2.2) (B4.b)	12.3
c) Restriction on changes to software packages (ISO: A.14.2.4) (CAF:B4.b)	12.4
d) Secure system engineering principles (ISO: A.14.2.5) (CAF:B4.b)	12.1, 12.2
e) Secure development environment (ISO: A.14.2.6) (CAF: B4.a)	12.2
f) Outsourced development (ISO: A.14.2.7)	12.2
g) System security testing (ISO: A.14.2.8)	12.4
h) System acceptance testing (ISO: A.14.2.9)	12.4
34) System acquisition, development and maintenance: test data	
a) Protection of test data (ISO: A.14.3.1)	12.4
35) Supplier relationships: information security in supplier relationships	
a) Information security policy for supplier relationships (ISO: A.15.1.1) (CAF: A4.a)	1.5, 3.3
b) Addressing security within supplier agreements (ISO: A.15.1.2) (CAF: A4.a, B3,e)	1.5, 3.1, 3.2
c) Information and communications technology supplier chain (ISO: A.15.1.3) (CAF: A4.a)	3.1, 3.3, 3.4
36) Supplier relationships: supplier service delivery management	
a) Monitoring and review of supplier services (ISO: A.15.2.1) (CAF: A4.a)	3.1, 3.4
b) Managing changes to supplier services (ISO: A.15.2.2) (CAF: A4.a)	3.1

This Document Has Been Superseded

37) Information security incident response, management and improvement	
a) Responsibilities and procedures (ISO: A.16.1.1) (CAF: B6.a, D1.a)	16.1
b) Reporting information security incidents (ISO: A.16.1.2; CAF: B6.a)	16.2
c) Reporting information security weaknesses (ISO: A.16.1.3; CAF: B6.a)	16.2
d) Assessment of and decision on information security events (ISO: A.16.1.4)	16.1
e) Response to information security incidents (ISO: A.16.1.5; CAF: D1.b)	16.1, 16.2
f) Learning from information security incidents (ISO: A.16.1.6; CAF: C1.d; ICO D.2)	16.4
g) Collection of evidence (ISO: A.16.1.7)	16.1
38) Information security aspects of business continuity management: information security continuity	
Sub-control (ISO 27001-CAF-ICO Ref. no.)	
a) Planning information security continuity (ISO: A.17.1.1) (CAF: B5.a, B6.a)	16.3, 17.6
b) Implementing information security continuity (ISO: A.17.1.2) (CAF: B5.a, D1.b)	17.1, 17.2, 17.3, 17.4
c) Information and data transfer resilience (CAF: B3.b)	7.1, 17.3
d) Verify, review and evaluate information security continuity (ISO: A.17.1.3) (CAF: B5.a, B5.b, D1.c)	17.3
e) Lessons learned (ISO: A.17.1.3; CAF: D2a, D2.b)	16.4
39) Information security aspects of business continuity management: redundancy & resilience	
a) Availability of information processing facilities (ISO: A.17.2.1) (CAF: B5.b, D1.b))	17.6
b) Resilient connectivity (CAF: B5.b)	7.1, 17.6
40) Compliance: compliance with legal and contractual requirements	
a) Identification of applicable legislation and contractual requirements (ISO: A.18.1.1)	5.1
b) Intellectual property rights (ISO: A.18.1.2)	5.1
c) Protection of records (ISO: A.18.1.3)	5.1, 5.2
d) Privacy and identification of personally identifiable information (ISO: A.18.1.4)	5.2, 17.5
e) Regulation of cryptographic controls (ISO: A.18.1.5)	9.3
41) Compliance: information security reviews	
a) Independent review of information security (ISO: A.18.2.1)	1.5, 14.9
b) Compliance with security policies and standards (ISO: A.18.2.2)	5.1
c) Technical compliance review (ISO: A.18.2.3)	1.3, 1.5, 14.9
d) Performance evaluation	5.1, 16.4
e) Assurance (CAF A2.b)	1.3, 1.5