Information Security Statement of Applicability (SoA)

Published Version	v36
Date of Publication	20 Aug 2024

BS ISO/IEC 27002:2022 Annex A

A5 Organisational Controls

Key	**Summary**	**Status**	**Basis for Inclusion/Exclusion**
STANDARD-1768	A5.02 Information security roles and responsibilities	In Scope	We need clearly defined roles & responsibilities to ensure full coverage and shared ownership of security related tasks.
STANDARD-1769	A5.03 Segregation of duties	In Scope	We have internal segregation of duties between areas of the customer services team and our engineers.
STANDARD-1770	A5.04 Management responsibilities	In Scope	Information Security is a critical aspect of our business and a focus of senior management. We require both policies and procedures for the review of those policies to ensure they are up to date and effective.
STANDARD-1771	A5.05 Contact with authorities	In Scope	We are a regulated business with obligations to the FCA and ICO.
STANDARD-1772	A5.06 Contact with special interest groups	In Scope	We are a highly specialised business with multiple technical specialisms.
STANDARD-1773	A5.07 Threat intelligence	In Scope	Threat intelligence and the sharing of information relating to it is a key control in keeping all our people security aware.
STANDARD-1774	A5.08 Information security in project management	In Scope	We are a delivery focused organisation running multiple projects in parallel with one another, with complex client and internal dependencies.
STANDARD-1775	A5.09 Inventory of information and other associated assets	In Scope	We hold information assets and their protection and maintenance is a key activity for the company.
STANDARD-1767	A5.1 Policies for information security	In Scope	Information Security is a critical aspect of our business and a focus of senior management. We require both policies and procedures for the review of those policies to ensure they are up to date and effective.

STANDARD-1776	A5.10 Acceptable use of information and other associated assets	In Scope	We hold information assets and controlling their acceptable use is a priority for the protection of our people and customers.
STANDARD-1777	A5.11 Return of assets	In Scope	We provide all our people with Information Assets which they need to return on leaving our employment.
STANDARD-1778	A5.12 Classification of information	In Scope	We hold information assets which need to be classified and labelled in order to be securely managed.
STANDARD-1779	A5.13 Labelling of information	In Scope	We hold information assets which need to be classified and labelled in order to be securely managed.
STANDARD-1780	A5.14 Information transfer	In Scope	We regularly share information with our people, customers and other external parties.
STANDARD-1781	A5.15 Access control	In Scope	Access control is key to ensuring data is only available to people who should have access to it.
STANDARD-1782	A5.16 Identity management	In Scope	Identity management is required to enable to control, track and audit access to information.
STANDARD-1783	A5.17 Authentication information	In Scope	We need to control authentication to ensure information is only available to those who need it.
STANDARD-1784	A5.18 Access rights	In Scope	Access rights need to be controlled in order to ensure information is only accessible to those who need it.
STANDARD-1785	A5.19 Information security in supplier relationships	In Scope	We manage a significant number of third party suppliers, some of whom process information on our behalf.
STANDARD-1786	A5.20 Addressing information security within supplier agreements	In Scope	We manage a significant number of third party suppliers, some of whom process information on our behalf.
STANDARD-1787	A5.21 Managing information security in the ICT supply chain	In Scope	We manage a significant number of third party suppliers, some of whom process information on our behalf.
STANDARD-1788	A5.22 Monitoring, review and change management of supplier services	In Scope	We manage a significant number of third party suppliers, some of whom process information on our behalf.
STANDARD-1789	A5.23 Information security for use of cloud services	In Scope	We utilise a number of cloud services to support business critical functions.
STANDARD-1790	A5.24 Information security incident management planning and preparation	In Scope	Incident management is a key corrective discipline and a requirement from all our customers.

STANDARD-1791	A5.25 Assessment and decision on information security events	In Scope	Incident management is a key corrective discipline and a requirement from all our customers.
STANDARD-1792	A5.26 Response to information security incidents	In Scope	Incident management is a key corrective discipline and a requirement from all our customers.
STANDARD-1793	A5.27 Learning from information security incidents	In Scope	We aim to promote a culture of open, continuous improvement. Learning from incidents is a key aspect of this.
STANDARD-1794	A5.28 Collection of evidence	In Scope	Evidence forms a key basis for making informed, rational decisions in the wake of an event.
STANDARD-1795	A5.29 Information security during disruption	In Scope	Responding effectively to security incidents is a critical part of our approach to continuity and security.
STANDARD-1796	A5.30 ICT readiness for business continuity	In Scope	ICT is a key part of our business continuity planning.
STANDARD-1797	A5.31 Legal, statutory, regulatory and contractual requirements	In Scope	We are a regulated business subject to multiple legal and regulatory requirements.
STANDARD-1798	A5.32 Intellectual property rights	In Scope	We are in an innovation business, and the protection of our IP, and the integrity of that of our customers is essential.
STANDARD-1799	A5.33 Protection of records	In Scope	Protecting the records we hold is critical to our operations.
STANDARD-1800	A5.34 Privacy and protection of PII	In Scope	We hold and manage PII and sensitive PII.
STANDARD-1801	A5.35 Independent review of information security	In Scope	External review is a requirement for improvement and proof points with customers.
STANDARD-1802	A5.36 Compliance with policies, rules and standards for information security	In Scope	We need to verify compliance with the policies and other standards set out.
STANDARD-1803	A5.37 Documented operating procedures	In Scope	We need clearly documented procedures for processing information in order to do so safely and compliance.

37 issues

A6 People Controls

Key	**Summary**	**Status**	**Basis for Inclusion/Exclusion**

STANDARD-1804	A6.01 Screening	In Scope	We need to ensure all our people are screened to help ensure they will handle information safely and ethically.
STANDARD-1805	A6.02 Terms and conditions of employment	In Scope	Our contracts need to handle information security responsibilities clearly and robustly.
STANDARD-1806	A6.03 Information security awareness, education and training	In Scope	Awareness and education is a key part of our approach to ensuring or people are confident and capable about Information Security.
STANDARD-1807	A6.04 Disciplinary process	In Scope	We need a clear procedure should any of our people violate our policies on Information Security.
STANDARD-1808	A6.05 Responsibilities after termination or change of employment	In Scope	Our people regularly change roles, and we need robust procedures to safely handle the information security aspects of any such changes.
STANDARD-1809	A6.06 Confidentiality or non-disclosure agreements	In Scope	We need additional controls for our people and third parties where PII is handled.
STANDARD-1810	A6.07 Remote working	In Scope	Remote working is our default method of operating.
STANDARD-1811	A6.08 Information security event reporting	In Scope	Ensuring a culture of no-blame reporting of incidents and tools to support this are as essential part of our corrective response.

8 issues

A7 Physical Controls

Key	Summary	Status	Basis for Inclusion/Exclusion
STANDARD-1812	A7.01 Physical security perimeters	In Scope	Although we have only one office, we have some controls in place, and also need to ensure we have statements on the procedures in place for third parties.
STANDARD-1813	A7.02 Physical entry	In Scope	Although we have limited risks associated with our single office, we still need controls in place for security reasons.
STANDARD-1814	A7.03 Securing offices, rooms and facilities	In Scope	We have a single office, but still require procedures for securing this location.
STANDARD-1815	A7.04 Physical security monitoring	In Scope	We have a single office location which needs to be secure.
STANDARD-1816	A7.05 Protecting against physical and environmental threats	In Scope	These threats represent a real risk to the business.

STANDARD-1817	A7.06 Working in secure areas	In Scope	We process some limited sensitive information in our office location.
STANDARD-1818	A7.07 Clear desk and clear screen	In Scope	We still have an office and need procedures relating to clear desks as sensitive information is handled there.
STANDARD-1819	A7.08 Equipment siting and protection	In Scope	We have equipment in our office location.
STANDARD-1820	A7.09 Security of assets off-premises	In Scope	We frequently use off-site assets.
STANDARD-1821	A7.10 Storage media	In Scope	We make use of storage media in the form of laptops, fixed PCs and (in limited circumstances) removable media.
STANDARD-1822	A7.11 Supporting utilities	In Scope	We have utilities in use at our office location.
STANDARD-1823	A7.12 Cabling security	In Scope	We have some cabling in the office required for pproductivity.
STANDARD-1824	A7.13 Equipment maintenance	In Scope	We have personal and office based equipment used for information processing.
STANDARD-1825	A7.14 Secure disposal or re-use of equipment	In Scope	We have equipment which needs to be securely disposed of.

14 issues

A8 Technological Controls

Key	Summary	Status	Basis for Inclusion/Exclusion
STANDARD-1826	A8.01 User endpoint devices	In Scope	All our people have access to at least one endpoint device.
STANDARD-1827	A8.02 Privileged access rights	In Scope	We have users who have privileged access to confidential and restricted data.
STANDARD-1828	A8.03 Information access restriction	In Scope	We need to restrict access to data in line with our overarching policy.
STANDARD-1829	A8.04 Access to source code	In Scope	Code development is a core function of our business.
STANDARD-1830	A8.05 Secure authentication	In Scope	Up to date controls to ensure authentication of all users and apps is secure are an essential control in the context of our business.
STANDARD-1831	A8.06 Capacity management	In Scope	Managing capacity effectively is essential from an application performance and cost perspectives.
STANDARD-1832	A8.07 Protection against malware	In Scope	Malware is a key attack vector for bad actors.

STANDARD-1833	A8.08 Management of technical vulnerabilities	In Scope	We develop complex systems based on multiple third party libraries, and the management of technical vulnerabilities is essential to ensure the data we hold is safe.
STANDARD-1834	A8.09 Configuration management	In Scope	We deploy all of our applications as part of a CI/CD pipeline. Careful configuration management is required to ensure this is robust and repeatable.
STANDARD-1835	A8.10 Information deletion	In Scope	We have obligations to retain and delete information in line with our policies and those of our customers.
STANDARD-1836	A8.11 Data masking	In Scope	We hold sensitive PII and employ a number of simple techniques to mask this for reporting and research purposes. As such this element is in scope.
STANDARD-1837	A8.12 Data leakage prevention	In Scope	The loss of data is one of our key, existential risks and we have significant controls in place in this area.
STANDARD-1838	A8.13 Information backup	In Scope	We need to maintain a robust and secure level of back-up of all our key data.
STANDARD-1839	A8.14 Redundancy of information processing facilities	In Scope	We guarantee a level of service for all our customers which requires significant resilience for our applications and infrastructure.
STANDARD-1840	A8.15 Logging	In Scope	Tracking activity in a robust and reliable way is an essential element of our controlling our estate.
STANDARD-1841	A8.16 Monitoring activities	In Scope	Monitoring has been a significant area of investment in the past 12-18 months.
STANDARD-1842	A8.17 Clock synchronisation	In Scope	We synchronise all of our server clocks in accordance with our policy.
STANDARD-1843	A8.18 Use of privileged utility programs	In Scope	We have a number of console and system access systems which provide elevated access options to our systems and encrypted data.
STANDARD-1844	A8.19 Installation of software on operational systems	In Scope	Our containerised solutions still utilise their own os versions.
STANDARD-1845	A8.20 Networks security	In Scope	We make extensive use of network technology within our AWS instances and our office.
STANDARD-1846	A8.21 Security of network services	In Scope	We make extensive use of network technology within our AWS instances and our office.
STANDARD-1847	A8.22 Segregation of networks	In Scope	We make extensive use of network technology within our AWS instances and our office.
STANDARD-1848	A8.23 Web filtering	In Scope	We have controls to limit access to different web sites and external sources of information.

STANDARD-1849	A8.24 Use of cryptography	In Scope	Encryption controls are key elements of our approach to keeping our information secure.
STANDARD-1850	A8.25 Secure development life cycle	In Scope	Software development is a core discipline in our business.
STANDARD-1851	A8.26 Application security requirements	In Scope	Application development is at the heart of our business.
STANDARD-1852	A8.27 Secure system architecture and engineering principles	In Scope	Application development is at the core of our business.
STANDARD-1853	A8.28 Secure coding	In Scope	Secure coding is an essential discipline for all our engineers.
STANDARD-1854	A8.29 Security testing in development and acceptance	In Scope	Security testing is a key control given the nature of our business.
STANDARD-1855	A8.30 Outsourced development	In Scope	We have utilised third party developers in the past, and the model is under consideration again.
STANDARD-1856	A8.31 Separation of development, test and production environments	In Scope	We have test (proof) and production environments and need controls to ensure they function securely and separately from one another.
STANDARD-1857	A8.32 Change management	In Scope	Release management and version controls are key to secure deployment of our solutions.
STANDARD-1858	A8.33 Test information	In Scope	We need test data in order to quality assure our systems.
STANDARD-1859	A8.34 Protection of information systems during audit testing	In Scope	We audit our systems internally and externally and information needs to be protected during these activities.

34 issues

ISO/IEC 27018:2019

Extended Controls

Key	**Summary**	**Status**	**Components**
STANDARD-1370	05.1.1 Policies for information security	In Scope	ISO/IEC 27018:2019
STANDARD-1371	06.1.1 Information security roles and responsibilities	In Scope	ISO/IEC 27018:2019
STANDARD-1372	07.2.2 Information security awareness, education and training	In Scope	ISO/IEC 27018:2019

STANDARD-1373	09.2 User access management	In Scope	ISO/IEC 27018:2019
STANDARD-1374	09.2.1 User registration and de-registration	In Scope	ISO/IEC 27018:2019
STANDARD-1375	09.4.2 Secure log-on procedures	In Scope	ISO/IEC 27018:2019
STANDARD-1376	10.1.1 Policy on the use of cryptographic controls	In Scope	ISO/IEC 27018:2019
STANDARD-1377	11.2.7 Secure disposal or re-use of equipment	In Scope	ISO/IEC 27018:2019
STANDARD-1378	12.1.4 Separation of development, testing and operational environments	Out of Scope	ISO/IEC 27018:2019
STANDARD-1379	12.3.1 Information backup	In Scope	ISO/IEC 27018:2019
STANDARD-1380	12.4.1 Event logging	In Scope	ISO/IEC 27018:2019
STANDARD-1381	12.4.2 Protection of log information	In Scope	ISO/IEC 27018:2019
STANDARD-1382	13.2.1 Information transfer policies and procedures	Out of Scope	ISO/IEC 27018:2019
STANDARD-1383	16.1 Management of information security incidents and improvements	In Scope	ISO/IEC 27018:2019
STANDARD-1384	16.1.1 Responsibilities and procedures	In Scope	ISO/IEC 27018:2019
STANDARD-1385	18.2.1 Independent review of information security	In Scope	ISO/IEC 27018:2019

16 issues

Annex A - Extended Control Set for PII Protection

Key	Summary	Status	Components
STANDARD-1386	A.02.1 Obligation to co-operate regarding PII principals' rights	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1387	A.03.1 Public cloud PII processor's purpose	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1388	A.03.2 Public cloud PII processor's commercial use	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1389	A.05.1 Secure erasure of temporary files	In Scope	ISO/IEC 27018:2019 Annex A

STANDARD-1390	A.06.1 PII disclosure notification	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1391	A.06.2 Recording of PII disclosures	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1392	A.08.1 Disclosure of sub-contracted PII processing	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1393	A.10.1 Notification of a data breach involving PII	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1394	A.10.2 Retention period for administrative security policies and guidelines	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1395	A.10.3 PII return, transfer and disposal	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1396	A.11.1 Confidentiality or non-disclosure agreements	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1405	A.11.10 User ID management	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1406	A.11.11 Contract measures	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1407	A.11.12 Sub-contracted PII processing	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1408	A.11.13 Access to data on pre-used data storage space	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1397	A.11.2 Restriction of the creation of hardcopy material	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1398	A.11.3 Control and logging of data restoration	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1399	A.11.4 Protecting data on storage media leaving the premises	Out of Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1400	A.11.5 Use of unencrypted portable storage media and devices	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1401	A.11.6 Encryption of PII transmitted over public data-transmission networks	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1402	A.11.7 Secure disposal of hardcopy materials	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1403	A.11.8 Unique use of user IDs	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1404	A.11.9 Records of authorised users	In Scope	ISO/IEC 27018:2019 Annex A
STANDARD-1409	A.12.1 Geographical location of PII	In Scope	ISO/IEC 27018:2019 Annex A

STANDARD-1410	A.12.2 Intended destination of PII	In Scope	ISO/IEC 27018:2019 Annex A

25 issues