Security Standard – Cloud Computing (SS-023)

Chief Security Office

Date: 26/06/2025

This Cloud Computing Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

Government Publications Security Policies and Standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

(Important note for screen reader users.) Paragraphs that contain a **‘must’** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains ‘must’ activities.

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision history

Version	Author	Description	Date
1.0		First issue	20/03/2017
2.0		Full update in line with current best practices and standards; Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls Added NIST CSF references All security measures have been updated and document reformatted Split between CSP and SO responsibilities for easer of reference	21/11/2023
2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Audience – Authority data Intro – Ref added to NCSC principles; mitigate vendor lock-in; ISO/IEC TR 22678; ISO/IEC 27017; NIST SP 800-210; ISF Scope – Use of multiple cloud providers; code repositories; zero trust and entitlement mgmt.; contractual	26/06/2025

		agreement of responsibilities; added ref to Containerisation, Malware, Security Testing, Patching and Network Security Design standards 12.1.6 Support staff and agents; Least privilege and MFA 12.1.7 Access credentials in line with Access & Authentication standard 12.1.8 MFA; default credentials must be changed in line with Privileged User Access standard; No admin access via RDP or SSH in line with Remote Access standard 12.3.1 Clarified applicability 13.2.1 AI tools; UK GDPR; IaaS and PaaS services 13.4.4 Agreed timeframe; backups and copies; Authority SO confirmation 13.6 Supply Chain Security 13.6.1 CSP profiles 14.3.1 CSP enabled data flows; Network security configuration 15.1.3 Virtualised CSP networks 15.2.5 Container hardening 16.1.4 DPIAs 17.1.1 SOs ensure CSPs follow the Patching Standard. 17.2.1 Continuously; Cloud-native security tools; (IaaS/PaaS/SaaS) and data sensitivity; events to be monitored; PII 17.2.2 SO confirm with CSP 17.4.3 Ref added to Security Incident Management standard; Incident communications 18.4.3 Confirm CSP access controls; privileged users	

		20.1.7 Access across all cloud service layers 21.1.4 UIs and APIs; error handling, input validation, rate limiting 21.1.6 File transfer malware scanning 22.1.1 SIEM tooling; external to the Authority 22.1.4 Added reference to the Authority's Information Management Policy Internal References – Added Remote Access standard; Security Incident standard; DWP Information Management Policy External References - ISO/IEC TR 22678; ISO/IEC 27017; NIST SP 800-210; ISF; ISO/IEC 27018	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	14/03/2017
2.0		Chief Security Officer	21/11/2023
2.1		Chief Security Officer	26/06/2025

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. D].
- independent external audit

Results of these will be fed back to the Authority.

5. Exceptions Process

(Important) this paragraph contains 'must' activities.

In this document the term **"must"** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications that utilise cloud computing for the purposes of delivering applications and services that handle Authority data.

7. Accessibility statement

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

(Important) this paragraph contains ‘must’ activities.

This Cloud Computing Security Standard defines the minimum technical security measures that **must** be implemented to secure Cloud based services to an Authority approved level of security.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e., guidance published by NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third-party providers, such as the CIS Critical Security Controls set. NCSC’s Cloud Security Principles should also be referenced for further information [see External References].

It also aligns with the principles and controls found in relevant international standards, such as the ISO/IEC 27000 series (including the cloud-specific guidance in ISO/IEC 27017 and ISO/IEC 27018), where applicable. This standard draws upon the cloud-specific implementation guidance provided in ISO/IEC 27017 and considers guidance from NIST SP 800-210, the CSA Controls Matrix and the Information Security Forum (ISF). (External References: ISO/IEC TR 22678, ISO/IEC 27017, NIST SP 800-210, ISF).

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question. This standard also supports the Authority 's strategic aim to mitigate vendor lock-in. Where feasible and aligned with security requirements, preference **must** be given during procurement and design to cloud services and configurations that support interoperability (e.g., through use of open standards) and provide well-defined data portability and service exit strategies. (External References: ISO/IEC TR 22678).

The aim of this standard is to:

- ensure security controls that are applicable to cloud computing requirements are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with cloud computing, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

A key objective of the assurance requirements within this standard is to build justifiable trust in the security of cloud services through demonstrable Cloud Service Provider (CSP) transparency regarding their operations, data handling, and security posture. (External References: ISO/IEC TR 22678)

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and are enabled by the implementation of controls from the CIS Critical Security Controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure systems and services utilising cloud computing for Authority data are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

(Important) this paragraph contains ‘must’ activities.

This standard applies to all use of cloud computing within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

Throughout this document, the terms Authority System or Service Owner (SO) and Cloud Service Provider (CSP) are used extensively. Where security measures are split between the SO and CSP, these are described alongside each other to clearly show differing responsibilities. Agreements with CSPs **must** clearly define and document the allocation of information security responsibilities between the Authority and the CSP. This **must** cover all relevant control areas and be reviewed periodically. Appendix G provides guidance, but the specific responsibilities **must** be confirmed and agreed within the contractual agreement. (External References: ISO/IEC 27017)

A guiding principle for this document is that for any cloud deployment, the cloud services control plane, and the data plane of the Authority/SO **must** have strong separation.

It should also be noted that use of multiple cloud providers can complicate visibility and security controls, which is likely to make monitoring more difficult, especially as containerised environments may be resistant to establishing persistence due to their short-lived nature, but remain vulnerable to injection flaws, insecure dependencies and logic errors. Threat actors increasingly target vulnerabilities at the earliest stages of the lifecycle, such as in code repositories, as these are perceived as easier targets – sensitive data such as passwords, credentials and API keys **must never** be uploaded to code repositories.

Use of zero trust in multi-cloud platforms alongside cloud infrastructure entitlement management tools may help to increase visibility of unauthorised activities.

The following standards **must** be read in conjunction with SS-023 Cloud Computing.

- SS-001 pt.1 Access & Authentication
- SS-001 pt.2 Privileged User Access
- SS-003 Secure Software Development
- SS-006 Security Boundaries
- SS-007 Use of Cryptography
- SS-011 Containerisation
- SS-012 Protective Monitoring (SaaS)
- SS-015 Malware Protection
- SS-018 Network Security Design
- SS-025 Virtualisation
- SS-027 Security Testing
- SS-033 Security Patching
- SS-035 Backup and Recovery
- SS-036 Secure Sanitisation and Destruction

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains 'must' activities.

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

Please note that for ease of reference, the security measures below have been split to indicate which are the responsibility of the Cloud Service Provider (CSP) and those of the System Owner (SO).

12. Protection of Data in Transit

1.1. Encryption and authentication

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
12.1.1	The cloud service provider (CSP) **must** use Transport Layer Security (TLS) 1.2 or higher to provide data confidentiality and integrity for communications between the customer and the cloud, and internally between their own systems and data centres. The CSP should also deploy certificate pinning and HTTP Strict	(No additional security measures)	PR.DS-02

	Transport Security where possible. Please refer to SS-007 Use of Cryptography for approved Cryptographic controls [Ref. A].		
12.1.2	The CSP **must** provide assurances that data is protected in transit within their service, as well as when it is accessed via external interfaces. This includes where data is moved between physical data centres.	SOs **must** request assurances from the CSP that data is protected in transit within their service, as well as when it is accessed via external interfaces. This includes where data is moved between CSP physical data centres.	PR.DS-02
12.1.3	The CSP **must** not be able to access the data plane (i.e., customer-based resources). Only access to the control plane (management and orchestration to cloud environments) is permitted.	SOs **must** commission an ITHC along with a Controls Assessment to ensure that this requirement is satisfied.	PR.AA-05
12.1.4	(No additional security measures)	Bare metal cloud services **must** be avoided, and IaaS **must** be the preferred choice for utilising virtualisation.	PR.DS-10
12.1.5	(No additional security measures)	It **must** only be possible to connect to the KMS (Key management service) using an approved protocol with secure settings, in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-02

12.1.6	(No additional security measures)	All accesses made to a cloud service (by support staff, not citizens or agents) **must** follow the principle of least privilege and be authenticated utilising Multi Factor Authentication (MFA), and SOs **must** be confident that all data flows are authenticated and encrypted as described above. Please also refer to SS-001-1 Access & Authentication Security Standard [Ref. J] for more security measures.	PR.AA-05 PR.DS-02
12.1.7	(No additional security measures)	Access credentials for cloud services **must** be changed from defaults, and **must** be in line with SS-001-1 Access & Authentication Security Standard [Ref. J]	PR.AA-01
12.1.8	(No additional security measures)	Administrative access to cloud services **must** also utilise Multi Factor Authentication (MFA) in line with SS-001-2 Privileged User Access Security Standard [Ref. M]. Direct administrative access from a client/desktop via SSH and RDP is not permitted as per SS-016 Remote Access Security Standard [Ref. N].	PR.AA-03 PR.AA-05

1.2. Cryptographic Controls

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
12.2.1	Cryptographic controls implemented by the CSP **must** be in line with SS-007 Use of Cryptography Security Standard [Ref. A].	SOs **must** implement cryptographic controls in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-01 PR.DS-02 PR.DS-10

1.3. PKI & Key Management

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
12.3.1	If the CSP provides PKI & Key Management services, it **must** be responsible for the encryption and key management used to protect data in transit. This also includes backup of keys, rotation of keys, deletion and revocation of keys, and monitoring and logging access to encryption keys.	SOs **must** use the Authority's Enterprise Key Management solution where possible and not implement their own, and **must** prohibit the CSP from storing and managing the cryptographic keys from the Authority's Enterprise Key Management solution. Please refer to SS-002 PKI & Key Management Security Standard [Ref. B] for the minimum security measures.	PR.DS-02

13. Asset Security and Resilience

1.4. Encryption for Data at Rest

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.1.1	Data at rest **must** be adequately safeguarded against unauthorised access by parties with physical access to infrastructure, in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J].	SOs **must** implement cryptographic controls for data at rest in line with SS-007 Use of Cryptography Security Standard [Ref. A]. See minimum security requirements and 12.2 Cryptographic Controls within this standard for further guidance.	PR.DS-01

1.5. Physical Sites and Legal Authority

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.2.1	There **must** be assurances that the CSP or any third parties do not retain copies of sensitive data or PII for such purposes as machine learning (including training AI tools), marketing, and advertising.	Data sovereignty **must** be within the UK region for IaaS and PaaS services. SOs **must** obtain assurances from the CSP that if data is being stored, processed, and maintained within the UK, their actions **must** comply with contractual obligations and all applicable laws, such as the UK Data Protection Act (DPA) 2018 and Regulation (EU) 2016/679: The UK General Data Protection Regulation (UK GDPR). If for any reason, IaaS and PaaS services are located outside the UK region, exceptions **must** be raised through the correct procedures.	PR.DS-01
13.2.2	(No additional security measures)	Application software used within a PaaS or IaaS cloud computing platform will be owned by the SOs/ the Authority. The Authority’s Data Protection Policy and any relevant legal frameworks **must** be adhered to when transferring any data that contains personally identifiable information (PII) or any other sensitive information.	ID.AM-02

1.6. Data Centre Security

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.3.1	The CSP **must** provide evidence, such as a SOC 2 report, that their physical security measures to their data centres mitigate against unauthorised access, tampering, theft, or reconfiguration of systems.	SOs **must** have assurances that these security measures are in place.	PR.AA-06

1.7. Sanitisation of Data and Disposal of Equipment

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.4.1	The CSP **must** disclose information about the processes and techniques they (or their suppliers) use to sanitise data and destroy equipment prior to disposal.	SOs **must** request confirmation that the CSP has policies and procedures in place for secure disposal of resources in line with SS-036 Secure Sanitisation and Destruction [Ref. C].	PR.DS-01 PR.PS-03
13.4.2	Unauthorised access to the Authority's data **must not** occur during the provisioning, transferring, or de-provisioning of resources.	(No additional security measures)	PR.DS-01
13.4.3	When resources are transferred, re-provisioned, or	(No additional security measures)	PR.DS-01

	requested for data to be sanitised or securely destroyed, there **must** be assurances from the CSP that these actions have been completed successfully.		PR.PS-03
13.4.4	At the end of its life, or at the end of the contract, storage media (including any copies or backups of Authority data) **must** be sanitised or securely destroyed within an agreed timeframe (e.g. 30 days) in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. C], and assurances from the CSP **must** be provided when this has been achieved.	The Authority's SO **must** confirm that any copies or backups of Authority data are no longer required, and that the CSP has completed this activity.	PR.DS-01 PR.PS-03
13.4.5	The CSP **must** provide proof of a recognised standard for equipment disposal or the use of a third-party destruction service that has been assessed against a recognised standard, in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. C].	(No additional security measures)	PR.DS-01 PR.PS-03

1.8. Availability

(Important) this table contains ‘must’ activities.

For information on backups in cloud environments, please refer to SS-035 Secure Backup and Recovery Security Standard [Ref. D].

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.5.1	There **must** be assurances that the CSPs commitment to availability, particularly its capacity for outages, satisfies the Authority’s requirements as per commercial agreement.	(No additional security measures)	GV.SC-02 GV.SC-06
13.5.2	There **must** be service level agreements (SLAs) or contractual commitments from the CSP that will meet Authority availability requirements as per commercial agreement.	(No additional security measures)	GV.SC-02 GV.SC-06

1.9. Supply Chain Security

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.6.1	CSPs may utilise Authority approved cloud hosting profiles to process OFFICIAL-SENSITIVE data.	SOs **must**, as part of due diligence and ongoing assurance for cloud services processing Authority data rated up to OFFICIAL-SENSITIVE, confirm with the relevant Authority Contract Manager that the CSP has processes in place for managing security risks within their own supply chain (i.e., subcontractors or critical suppliers to the CSP).	GV.SC-01 GV.SC-03 GV.SC-05 GV.SC-07 GV.SC-09
13.6.2	(No additional security measures)	SOs **must** confirm with the relevant Authority Contract Manager that the CSP contractually requires its critical third-party suppliers or subcontractors (who access, process, or store Authority data, or could impact the security of the service provided to the Authority) to adhere to security standards commensurate with this standard.	GV.SC-05 GV.SC-07 GV.SC-09

13.6.3	CSPs **must** provide annual independent audit reports (e.g., SOC 2, ISO 27001) covering relevant controls, including those implemented by sub-processors involved in the delivery of the service to the Authority. Contracts **must** allow the Authority (or an appointed agent) the right to audit the Authority operated cloud tenants or request further evidence of compliance with this standard.	(No additional security measures)	GV.SC-02 GV.SC-05 GV.SC-07
13.6.4	CSPs **must** disclose all geographic locations (at country or continent level) where Authority data may be stored, processed, or accessed, including those used by sub-processors and third-party data centres.	Any processing or transfer of Authority data outside the UK **must** comply with the DWP Offshoring Policy [Ref. R], relevant Authority security policies, and utilise approved data transfer mechanisms.	GV.SC-02 GV.SC-04 GV.SC-07 GV.SC-09

14. Separation Between Users

1.10. Boundary Protection

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
14.1.1	The CSP **must** provide assurances that security boundaries implemented by themselves allow SOs control of who can access data and how, in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J], SS-001 pt.2 Privileged User Access Security Standard [Ref. M], and SS-006 Security Boundaries Standard [Ref. L].	(No additional security measures)	PR.AA-05 PR.IR-01
14.1.2	(No additional security measures)	Boundary controls **must** be implemented, (as per SS-006 Security Boundaries Standard [Ref. L]) as custom code can be executed within these services.	PR.IR-01
14.1.3	(No additional security measures)	SOs **must** be aware of the separation methods utilised for each service they employ, and suitability for their purposes.	PR.AA-05 PR.IR-01

1.11. Separation of Storage

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
14.2.1	Cloud services that are utilised **must** have a deny access to stored objects by default and **must** be integrated with role-based access controls in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J].	(No additional security measures)	PR.AA-05
14.2.2	Cloud services that are utilised **must** use encryption for stored data by default. See section 13.1 Encryption for Data at Rest for minimum security requirements.	(No additional security measures)	PR.DS-01

1.12. Separation Flow of Network

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
14.3.1	Cloud services that are utilised **must** allow greater control over data flows enabled by the CSP, as well as the ability to detect anomalous traffic more easily.	The SO **must** ensure that the security configuration of virtual networks within the cloud service are defined, implemented, and managed in line with SS-006 Security Boundaries [Ref. L] and SS-018 Network Security Design [Ref. Q] security standards, taking into account any specific guidance from the CSP.	ID.AM-03 PR.IR-01

15. Hypervisor and Virtualisation Security

(SS-023 Cloud Computing Standard **must** be read in conjunction with SS-009 Hypervisor Security Standard [Ref. G] and SS-025 Virtualisation Security Standard [Ref. H]).

1.13. Segregation in Virtual Computing Environments

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
15.1.1	The SOs virtual environment running on a cloud service **must** be protected from access by other cloud service customers and unauthorised persons.	(No additional security measures)	GV.SC-05

15.1.2	The CSP **must** prevent any co-tenants (i.e. other customers) from monopolising shared resources such as bandwidth or CPU.	(No additional security measures)	ID.AM-05 PR.IR-04
15.1.3	The CSP **must** apply information security controls where the cloud service involves multi-tenancy to ensure proper resource isolation between tenants, such as customer data, virtualised applications, operating systems, storage, and virtualised network infrastructure.	(No additional security measures)	GV.SC-05
15.1.4	The CSP **must** consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the CSP.	(No additional security measures)	GV.SC-05

1.14. Virtual & Physical Machine Hardening

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
15.2.1	When configuring virtual machines, SOs and CSPs **must** ensure that appropriate aspects are hardened (e.g. underlying hardware, BIOS, only necessary ports, protocols, and services are enabled etc.) and that appropriate technical measures (e.g., anti-malware, logging) are in place for each virtual machine used. (For minimum security controls please refer SS-025 Virtualisation Security Standard [Ref. H]).		PR.DS-10 PR.IR-01
15.2.2	Mechanisms and safeguards **must** be developed and implemented by SOs and CSPs, to prevent human		PR.AA-06

	interference from accidentally or intentionally erasing, shutting down virtual servers, or destroying virtual assets as stipulated in the standards scope (i.e. CSPs manage the control plane, SOs manage the data plane).		PR.IR-02
15.2.3	The CSP is responsible for all elements of physical security e.g. access to data centres and physical assets),	(No additional security measures)	PR.AA-06 PR.IR-02
15.2.4	(No additional security measures)	The SO **must** verify the CSP is providing all the agreed secure services/components, supported by a risk assessment or ITHC.	GV.SC-07 GV.SC-09
15.2.5	(No additional security measures)	Where they are utilised, the SO **must** ensure that containers are appropriately hardened in line with SS-011 Containerisation Security Standard [Ref. O]).	PR.DS-10 PR.IR-02

16. Governance Framework

(Important) this table contains ‘must’ activities.

It **must** be defined between SOs and the CSP which information security controls are managed by whom.

1.15. Co-ordination and Management of Cloud Services

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
16.1.1	(No additional security measures)	SOs **must** define or expand existing system-specific policies and procedures to reflect its use of cloud services and make cloud service users aware of their roles and responsibilities in the cloud service's use.	GV.PO-01 GV.PO-02
16.1.2	The management of the cloud service and the data it contains **must** be coordinated and directed by the CSPs security governance framework.	(No additional security measures)	GV.SC-02 GV.SC-09
16.1.3	The CSP **must** have a framework for security governance and risk management that is formalised, with regulations governing important information security issues that are pertinent to the service.	SO **must** understand the CSPs operating procedures in order to design Authority services that take account of these in order to meet Authority business requirements.	GV.SC-02 GV.SC-09

16.1.4	(No additional security measures)	For cloud services processing personal data, SOs **must** ensure Data Protection Impact Assessments (DPIAs) are conducted where required by UK GDPR/DPA 2018. Cloud service configurations **should** support data minimisation principles, and utilise techniques such as pseudonymisation or anonymisation where feasible and appropriate.	GV.OC-03

17. Operational Security

1.16. Vulnerability & Patch Management

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
17.1.1	The CSP **must** have a vulnerability management process in place to identify, triage and mitigate vulnerabilities in all components of the service that they are responsible for, in line with SS-033 Security Patching Standard [Ref. E].	SOs **must** ensure that CSPs are managing vulnerabilities in line with SS-033 Security Patching Standard [Ref. E] for minimum security requirements.	PR.PS-02

1.17. Protective Monitoring & Logging

(Important) this table contains 'must' activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
17.2.1	There **must** be assurances that the CSP continuously monitors the service to detect; • successful and unsuccessful attacks • changes to firewalls and boundary controls that are managed by the CSP • unauthorised configuration changes • changes to security groups • misuse and malfunctions • Cloud-native security tools and cloud security posture management may be utilised for this purpose.	SOs **must** define monitoring and event logging requirements appropriate to the service model (IaaS/PaaS/SaaS) and data sensitivity such as resource usage, container runtime, failed access attempts and PII, and ensure that the CSP meets those requirements. Please refer to SS-012 Protective Monitoring Security Standard [Ref. F].	DE.CM-01 DE.CM-09
17.2.2	SOs **must** be assured that the CSP generates enough audit events to enable effective detection of suspicious activity, that these events are analysed to uncover potential breaches or improper usage of the service, and that the CSP reacts to incidents in a prompt and appropriate manner.	Authority SOs **must** confirm that the CSP is meeting this requirement.	DE.CM-03 DE.CM-06
17.2.3	(No additional security measures)	SOs **must** be able to monitor specific aspects of the operation of the cloud services that they utilise.	DE.CM-06

17.2.4	To prevent information security incidents caused by resource shortages, the CSP **must** monitor total resource capacity, and generate alerts to SOs accordingly.	(No additional security measures)	PR.IR-04

1.18. Configuration and Change Management

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
17.3.1	In order to identify and manage changes that could affect the security of the service and mitigate known vulnerabilities, the CSP **must** be aware of the assets that comprise their service, as well as their configurations and dependencies.	(No additional security measures)	ID.AM-04 ID.RA-07 PR.PS-01
17.3.2	(No additional security measures)	SOs **must** be confident that CSP service changes are managed and monitored through to completion after being evaluated for potential security impacts.	ID.AM-04 ID.RA-07
17.3.3	(No additional security measures)	SOs **must** be confident that unauthorised CSP changes to deployed service components and their configuration will be detected and prevented.	ID.RA-07 PR.PS-01

17.3.4	The CSP **must** give SOs appropriate notice before making changes that could affect how they use the service, or their ability to use the service.	(No additional security measures)	ID.RA-07 PR.PS-01
17.3.5	CSPs **must** implement all technical changes automatically and consistently throughout their infrastructure.	(No additional security measures)	ID.RA-07 PR.PS-01

1.19. Incident Management

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
17.4.1	The CSP **must** have incident management processes in place in line with SS-014 Security Incident Management Standard [Ref. N], and supported by appropriate Service Level Agreements to ensure that effective and timely decisions are made when security incidents occur.	(No additional security measures)	GV.SC-08 ID.IM-04
17.4.2	(No additional security measures)	SOs and outside parties **must** have a clear method and contact point to report security issues and vulnerabilities to the CSP.	DE.AE-08 RS.CO-02

17.4.3	The CSP **must** inform SOs if they detect a security incident that affects their data in an acceptable agreed timescale in line with SS-014 Security Incident Management Standard [Ref. S] to enable the Authority to meet its regulatory obligations (e.g. to the ICO). The CSP **must** provide reasonable assistance to Authority in investigating and managing the breach.	SOs **must** establish and agree procedures with the CSP for the timely communication and coordinated management of information security events and incidents, covering detection, reporting, assessment, response, and learning lessons for both parties. Contact mechanisms and expected response times **must** also be defined.	DE.AE-08 RS.CO-02

18. Personnel Security

1.20. Employees

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
18.4.1	The CSP **must** conduct security screening and regular security training for employees that have the ability to modify the service and **must** all be commensurate to their position and privileges.	(No additional security measures)	PR.AT-01 PR.AT-02
18.4.2	CSP staff **must** not have access to Authority data.	(No additional security measures)	PR.AA-05

18.4.3	CSP **must** implement the necessary access & authorisation controls for change management purposes.	SOs **must** confirm with the Authority Contract Manager that the CSP has security controls in place for access and authorisation, especially for privileged user actions.	PR.AA-02 PR.AA-05

19. Secure Development

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
19.1.1	(No additional security measures)	The SO **must** request assurances from the CSP that their design, development, and deployment of their cloud services minimises and mitigates security vulnerabilities.	PR.PS-06

20. Secure User Management

1.21. Restriction of Permissions

(Important) this table contains 'must' activities.

Please refer to SS-001 pt.1 Access and Authentication Security Standard [Ref. J] for more detail on managing user access.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
20.1.1	The CSP **must** provide administration tools and access controls to enable SOs in maintaining the identities they use, limiting access to cloud services, cloud service features, and cloud service customers' data stored in those services.	(No additional security measures)	PR.AA-01 PR.AA-05
20.1.2	To avoid inconsistencies between various access controls, which may lead to confusion and unforeseen accesses, the CSP **must** have a single, cohesive access control system implemented.	(No additional security measures)	PR.AA-02 PR.AA-03
20.1.3	(No additional security measures)	SOs **must** be aware of all mechanisms by which the CSP accepts management or support requests from the Authority (telephone, web portal, etc.), and that only authorised personnel are permitted to use those mechanisms to affect the service.	PR.AA-02 PR.AA-03

20.1.4	CSPs **must** provide SOs the ability to apply time-bounded permissions for highly privileged accesses.	(No additional security measures)	PR.AA-05
20.1.5	Access to service interfaces **must** only be granted to those who have been authenticated and authorised.	(No additional security measures)	PR.AA-02 PR.AA-03
20.1.6	(No additional security measures)	Identity, authentication, and authorisation measures **must** provide SOs with the assurance that users have the right to access a given interface.	PR.AA-01 PR.AA-02 PR.AA-03 PR.AA-05

20.1.7	(No additional security measures)	SOs **must** be confident that: • they understand how access to external interfaces is authenticated. • Access controls are implemented and managed across all relevant cloud service layers (e.g., infrastructure, platform, application, data) and service models (IaaS, PaaS, SaaS). • the CSP enforces an up-to-date password policy and requires Authority users to employ multi-factor authentication (MFA) before they may access any resources. • the CSP performs equally robust authentication of Authority service identities as it does for users. • Authority user authentication will be integrated with Authority processes for managing joiners, movers, and leavers. • processes are in place for the management lifecycle of service credentials.	PR.AA-01 PR.AA-02 PR.AA-03 PR.AA-05

1. External Interface Protection

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
21.1.1	(No additional security measures)	All external (to the Authority) or untrusted service interfaces **must** be identified and protected.	ID.AM-04
21.1.2	(No additional security measures)	SOs **must** have confidence that they know what physical and logical interfaces allow for access to information and how that access is restricted.	ID.AM-04 PR.IR-01
21.1.3	(No additional security measures)	SOs **must** have confidence that the cloud service identifies and authenticates users at the appropriate level across those interfaces.	PR.AA-02 PR.AA-03
21.1.4	(No additional security measures)	SOs **must** have assurances that interfaces from the CSP such as Sensitive User Interfaces and Application Programming Interfaces are designed to be resistant to attacks (e.g. via robust error handling, input validation or rate limiting), especially interfaces exposed publicly (over the internet).	PR.DS-10 PR.IR-01
21.1.5	(No additional security measures)	SOs **must** be confident that the CSP has a continuous testing regime in place to ensure that CSP-owned external interfaces are secure.	PR.IR-01 DE.CM-06

21.1.6	(No additional security measures)	SOs **must** ensure that all files uploaded to or downloaded from the cloud application **must** be scanned for malware in line with SS-015 Malware Protection Security Standard [Ref. P].	DE.CM-06

2. Logging Information and Alerting

1.22. Audit Information

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
22.1.1	CSPs **must** enable the production and collection of log data for ingestion into the Authority’s SIEM tooling, to investigate incidents involving the use of a service and the data contained within it.	SO's **must** be confident that these have been onboarded and are actioned appropriately.	PR.PS-04 DE.AE-03
22.1.2	The log information that is made available **must** meet the needs for investigating misuse or security incidents.	(No additional security measures)	PR.PS-04
22.1.3	Log information **must** be made available by the CSP for any personnel actions that have an impact on the service in use (or the data held within it).	(No additional security measures)	PR.PS-04 DE.CM-03
22.1.4	Log information **must not** be deleted by SOs or the CSP during a defined retention period in line with the DWP Information Management Policy [Ref. T].		PR.PS-04

1.23. Security Alerts

Please note Protective Monitoring of SaaS platforms falls within this standard.

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
22.2.1	The CSP **must** alert SOs when compromises, malicious activity or vulnerabilities in the CSP services have been identified.	(No additional security measures)	DE.AE-08
22.2.2	CSP **must** notify the Authority of any security events that may impact the service, in line with SS-014 Security Incident Management Standard [Ref. N], and supported by appropriate Service Level Agreements.	(No additional security measures)	DE.AE-08

3. Secure Use of the Service

1.24. Security by Design and by Default

(Important) this table contains ‘must’ activities.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
23.1.1	The CSP **must** make it simple for SOs to deliver their services in a secure manner that is resistant to common attacks.	SOs are responsible for ensuring their services in the cloud environment are designed securely.	GV.SC-05
23.1.2	(No additional security measures)	SOs **must** understand which of the above security measures in this standard are met by the service’s default configurations, and what **must** be done for those security measures that are not currently compliant.	PR.PS-01
23.1.3	(No additional security measures)	Authority staff **must** be appropriately trained in using and administering the service in accordance with the Authority’s information security policies and standards.	PR.AT-01 PR.AT-02
23.1.4	The CSP **must** be responsible for updating the default settings for their service to address new risks (this may include altering the configuration of existing customers, as well as changing the starting point for new customers).	(No additional security measures)	ID.RA-05 PR.PS-01

4. Appendices

Appendix A - Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related security measures
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	16.1.4
GV.PO-01	Policy for managing cybersecurity risks is established based on organisational context, cybersecurity strategy, and priorities and is communicated and enforced	16.1.1,
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organisational mission	16.1.1,
GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organisational stakeholders	13.6.1

GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	13.5.1, 13.5.2, 13.6.3, 13.6.4, 16.1.2, 16.1.3,
GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	13.6.1
GV.SC-04	Suppliers are known and prioritised by criticality	13.6.4
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	13.6.1, 13.6.2, 13.6.3, 15.1.1, 15.1.3, 15.1.4, 23.1.1,
GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	13.5.1, 13.5.2,
GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritised, assessed, responded to, and monitored over the course of the relationship	13.6.1, 13.6.2, 13.6.3, 13.6.4, 15.2.4,
GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	17.4.1,

GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	13.6.1, 13.6.2, 13.6.4, 15.2.4, 16.1.2, 16.1.3,
ID.AM-02	Inventories of software, services, and systems managed by the organisation are maintained	13.2.2,
ID.AM-03	Representations of the organisation's authorised network communication and internal and external network data flows are maintained	14.3.1,
ID.AM-04	Inventories of services provided by suppliers are maintained	17.3.1, 17.3.2, 21.1.1, 21.1.2,
ID.AM-05	Assets are prioritised based on classification, criticality, resources, and impact on the mission	15.1.2,
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritisation	23.1.4
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	17.3.1, 17.3.2, 17.3.3, 17.3.4, 17.3.5,
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	17.4.1,

PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	12.1.7, 20.1.1, 20.1.6, 20.1.7,
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	18.4.3, 20.1.2, 20.1.3, 20.1.5, 20.1.6, 20.1.7, 21.1.3,
PR.AA-03	Users, services, and hardware are authenticated	12.1.8, 20.1.2, 20.1.3, 20.1.5, 20.1.6, 20.1.7, 21.1.3,
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	12.1.3, 12.1.6, 12.1.8, 14.1.1, 14.1.3, 14.2.1, 18.4.2, 18.4.3, 20.1.1, 20.1.4, 20.1.6, 20.1.7,
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	13.3.1, 15.2.2, 15.2.3,
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	18.4.1, 23.1.3,
PR.AT-02	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	18.4.1, 23.1.3,

PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	12.2.1, 13.1.1, 13.2.1, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 14.2.2,
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	12.1.1, 12.1.2, 12.1.5, 12.1.6, 12.2.1, 12.3.1,
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	12.1.4, 12.2.1, 15.2.1, 15.2.5, 21.1.4,
PR.PS-01	Configuration management practices are established and applied	17.3.1, 17.3.3, 17.3.4, 17.3.5, 23.1.2, 23.1.4
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	17.1.1,
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	13.4.1, 13.4.3, 13.4.4, 13.4.5,
PR.PS-04	Log records are generated and made available for continuous monitoring	22.1.1, 22.1.2, 22.1.3, 22.1.4,
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	19.1.1,
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	14.1.1, 14.1.2, 14.1.3, 14.3.1, 15.2.1, 21.1.2, 21.1.4, 21.1.5,
PR.IR-02	The organisation's technology assets are protected from environmental threats	15.2.2, 15.2.3, 15.2.5
PR.IR-04	Adequate resource capacity to ensure availability is maintained	15.1.2, 17.2.4,

DE.CM-01	Networks and network services are monitored to find potentially adverse events	17.2.1,
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	17.2.2, 22.1.3,
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	17.2.2, 17.2.3, 21.1.5, 21.1.6,
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	17.2.1,
DE.AE-03	Information is correlated from multiple sources	22.1.1,
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	17.4.2, 17.4.3, 22.2.1, 22.2.2,
RS.CO-02	Internal and external stakeholders are notified of incidents	17.4.2, 17.4.3,

Appendix B - Internal references

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	SS-007 Use of Cryptography	Yes
B	SS-002 PKI & Key Management	Yes
C	SS-036 Secure Sanitisation and Destruction	Yes
D	SS-035 Secure Backup and Recovery	Yes
E	SS-033 Security Patching	Yes
F	SS-012 Protective Monitoring	Yes
G	SS-009 Hypervisor Security	Yes
H	SS-025 Virtualisation	Yes
I	Security Assurance Strategy	No
J	SS-001-1 Access & Authentication	Yes
K	DWP Data Protection Policy	No
L	SS-006 Security Boundaries	Yes
M	SS-001-2 Privileged User Access	Yes
N	SS-016 Remote Access Security Standard	Yes
O	SS-011 Containerisation Security Standard	Yes
P	SS-015 Malware Protection Security Standard	Yes
Q	SS-018 Network Security Design Security Standard	Yes
R	DWP Offshoring Policy	No
S	SS-014 Security Incident Management Standard	Yes
T	DWP Data Protection Policy	Yes

*Request to access to non-publicly available documents **should** be made to the Authority.

Appendix C External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

External Documents List
Cloud Security Alliance Cloud Controls Matrix
CIS Critical Security Controls set
UK General Data Protection Regulation (UK GDPR)
Data Protection Act 2018 (DPA)
NCSC 14 Cloud Security Principles
Operational Best Practices for NCSC Cloud Security Principles - AWS Config (amazon.com)
Azure UK Governments - 14 compliance controls.pdf (microsoft.com)
ISO/IEC TR 22678 – Cloud Computing
ISO/IEC 27017 - Code of practice for information security controls for cloud services
ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds
NIST SP 800-210 - General Access Control Guidance for Cloud Systems The Information Security Forum (ISF)

Appendix D Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
DWP	Department of Work and Pensions.	UK Government
NCSC	National Cyber Security Centre	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OWASP	Open Web Application Security Project	Open Source
SIEM	Security Incident Event Management	Industry term

Appendix E Glossary

Table 6 – Glossary

Term	Definition
Bare Metal	A bare-metal environment is a specific kind of virtualisation environment that does not rely on a host OS in order to function.
Burst/Surge processing	Processing that exceeds regular processing capacity for short periods of time
Control Plane	The control plane provides management and orchestration across an organisation's cloud environment.
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, nonrepudiation, and accountability; including, but not limited to devices, products, systems, key variables, and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).
Data Plane	The data plane houses and transports application and data traffic.
DDA	Digital Design Authority (part of Digital Group)
IaaS	Infrastructure as a Service - The supply of basic infrastructure, such as networks, processing, and storage, on which users can base their applications, CSP is responsible.
PaaS	Platform as a Service - The level of responsibility shared with the CSP varies greatly in PaaS services. At one end of the spectrum, the distinction between IaaS and PaaS is blurred because the provider helps manage the operating system. Customers submit the source code for their application, and the service handles the rest.

SaaS	Software as a Service - The SaaS model enables CSC to provide the CSP the greatest amount of responsibility while taking full advantage of the increased security provided by the provider's large-scale operation.

Appendix F - Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies

Appendix G – Cloud Responsibility Service Model

The responsibility allocation options for the four basic deployment methodologies are broken down in the table below. Please use the following table only as guidance and confirm responsibilities with the CSP.

	on premise	IaaS	PaaS	SaaS
Application configuration	■	■	■	■
Identity & access controls	■	■	◩	◩
Application data storage	■	■	◩	□
Application	■	■	■	□
Operating system	■	■	□	□
Network flow controls	■	◩	□	□
Host infrastructure	■	□	□	□
Physical security	■	□	□	□

■	Customer is predominantly responsible for security
◩	Both customer and cloud service have security responsibilities
□	Cloud service is fully responsible for security