DXC Secure Cloud for UK Government and supporting organisations

Response to the Cloud Security Alliance's Consensus Assessments Initiative Questionnaire V3.1 (30.09.19)

22 June 2021

Important notice

The Cloud Security Alliance® (CSA®) is a global not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.

The Cloud Security Alliance Cloud Consensus Assessments Initiative Questionnaire (CAIQ V3.1) is a set of questions with *Yes/No/Not applicable* answers that may be used by a cloud service provider, cloud customers or auditors to determine the level of compliance of a cloud service with the CSA Cloud Controls Matrix, and to guide cloud service providers to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The content in columns 1 to 6 of the tables in the following pages are taken from the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire (CAIQ) Version 3.1" at http://www.cloudsecurityalliance.org © Copyright 2019 Cloud Security Alliance, and the content in column 7 is DXC Secure Cloud's response to the questions.

DXC has prepared this document in good faith and reserves the right to make amendments and correct any errors that are identified after its submission. Neither DXC nor its representatives make any representations or warranties as to the accuracy or completeness of the information provided in here and neither DXC nor its representatives shall have any liability resulting from use of the information provided. The term "solution" in the context of this document means products and services but does not imply that those products or services are guaranteed to, or will, meet a customer's requirements. The use of the term "partner" in this document does not imply a formal, legal, or contractual partnership, but rather a mutually beneficial relationship arising from the teamwork between DXC and its vendors.

If there are any concerns, questions, or issues regarding this document, please contact the DXC Frameworks team by email at ukitenders@dxc.com

© 2021 DXC Technology Company. All rights reserved.

Table of Contents

Introduction 4
Application & Interface Security: AIS-01 to AIS-04 5
Audit, Assurance & Compliance: AAC-01 to AAC-03 8
Business Continuity Management & Operational Resilience: BCR-01 to BCR-11 11
Change Control and Configuration Management: CCC-01 to CCC-05 20
Data Security & Information Lifecycle Management: DSI-01 to DSI-07 24
Datacenter Security: DCS-01 to DCS-09 28
Encryption & Key Management: EKM-01 to EKM-04 32
Governance and Risk Management: GRM-01 to GRM-11 35
Human Resources: HRS-01 to HRS-11 42
Identity & Access Management: IAM-01 to IAM-13 49
Infrastructure & Virtualization Security: IVS-01 to IVS-13 62
Interoperability & Portability: IPY-01 to IPY-05 72
Mobile Security: MOS-01 to MOS-20 76
Security Incident Management, E-Discovery, & Cloud Forensics: SEF-01 to SEF-05 84
Supply Chain Management, Transparency, and Accountability: STA-01 to STA-09 89
Threat and Vulnerability Management: TVM-01 to TVM-03 98
Glossary of terms 102

Introduction

DXC Secure Cloud is an ISO/IEC 27001 certified and ISO/IEC 27017 and PSN compliant set of enterprise private and hybrid cloud solutions and services for UK Government and supporting organisations required to meet UK Government requirements. It was one of the first in the UK to gain the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) certification.

Secure Cloud offers its clients the following core service:

- DXC Technology Managed Services for Multicloud for Government – Private/Hybrid Cloud

for Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) options, operating at Official classification.

Additional services include:

- Workplace - delivering an enhanced desktop and mobile support experience, including integration with Microsoft 365®
- Mobility - a management service for mobile device and application management
- Collaboration - providing an environment based on Microsoft SharePoint®
- Real-Time Collaboration - providing highly available multi-platform voice and video communication services
- Network Management Service - delivering a scalable solution for monitoring and managing data and voice networks
- Enterprise Service Management - operating across all Secure Cloud services, based on the ITIL framework and using dedicated tools and processes, including a Secure Cloud service management instance for use with the ServiceNow® platform

Secure Cloud systems management infrastructure and tools, a Security Operations Centre and a Network Operations Centre underpin these services.

Secure Cloud Services delivers enterprise desktop, infrastructure, software and network services to its clients without them incurring the high cost of owning and managing their own equipment or data centres. It supports the quick deployment of high-end applications in secure, multi-tenant or single-tenant cloud environments and allows self-provisioning to match clients' business needs as they change and evolve.

For more information on DXC Secure Cloud Services and solutions, visit the Digital Marketplace for Government Cloud Services.

DXC Secure Cloud is managed under DXC's Information Security Management System (ISMS) that is certified to ISO 27001:2013, and the cloud services attained CSA's STAR Level 2 certification Silver Award during the period October 2013 to September 2018. The services are also compliant to ISO 27017:2015 and to the Public Services Network security requirements, holding ISO 27017 compliance, PSN Connection compliance and PSN Service Provision certificates.

The responses in the following pages are to the questions concerning the controls in place across the sixteen security domains in Cloud Security Alliance's Consensus Assessments Initiative Questionnaire V3.1 (30-9-19).

Application & Interface Security: AIS-01 to AIS-04

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AIS-01 Application Security	*Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.*	AIS-01.1 Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?			N/A	Secure Cloud does not undertake software development but integrates Commercial Off-The-Shelf (COTS) products.
		AIS-01.2 Do you use an automated source code analysis tool to detect security defects in code prior to production?			N/A	
		AIS-01.3 Do you use manual source-code analysis to detect security defects in code prior to production?			N/A	
		AIS-01.4 Do you verify that all your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		No		COTS components were selected according to their capability and reputation for effectiveness within the marketplace, and compliance of a product to an industry security standard influenced selection.
		AIS-01.5 (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes			Applications are tested for vulnerabilities, and issues are resolved before the system is deployed into production.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AIS-02 Customer Access Requirements	*Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.*	AIS-02.1 Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes			Customer networks connecting to and accessing the Secure Cloud network and data must hold a Public Services Network (PSN) compliance certificate, or equivalent, and must formally agree to the Secure Cloud Code of Connection.
		AIS-02.2 Are all requirements and trust levels for customers' access defined and documented?	Yes			
AIS-03 Data Integrity	*Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.*	AIS-03.1 Does your data management policies and procedures require audits to verify data input and output integrity routines?	Yes			DXC policies and processes require data input and output validation during the application/system integration and testing process, reinforced by security testing at key stages of the system development life cycle.
		AIS-03.2 Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AIS-04 Data Security / Integrity	*Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.*	AIS-04.1 Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	Yes			The cloud data security architecture is consistent with the National Cyber Security Centre (NCSC) security design principles and cloud security guidance, referred to as the NCSC 14 Cloud Principles.

Audit, Assurance & Compliance: AAC-01 to AAC-03

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AAC-01 Audit Planning	*Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.*	AAC-01.1 Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources, etc.) for reviewing the efficiency and effectiveness of implemented security controls?	Yes			Audit plans cover the information security management system and sampling the implementation of controls and security processes, assessing their efficiency and effectiveness across the different industry standard control areas.
		AAC-01.2 Does your audit program take into account effectiveness of implementation of security operations?	Yes			The DXC audit process considers the efficiency and effectiveness of security operations.
AAC-02 Independent Audits	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	AAC-02.1 Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes			The option of purchasing SOC 2 reports, subject to NDA, is available to customers/tenants.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AAC-02 Independent Audits	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	AAC-02.2 Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes			An independent CHECK-qualified security testing team performs network and application penetration testing of the Secure Cloud systems as prescribed by industry standards and guidance, at annual or higher frequency.
		AAC-02.3 Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes			
		AAC-02.4 Do you conduct internal audits at least annually?		No		Internal audits of Secure Cloud are conducted periodically to comply with the requirements of corporate policy and standards, and to ensure continued adherence to the maintenance requirements of industry standard certifications.
		AAC-02.5 Do you conduct independent audits at least annually?	Yes			Independent audits of Secure Cloud services are conducted at least annually by a UKAS-accredited certification body or by the PSN assessor. Data Centres hosting the Secure Cloud infrastructure undergo annual audits against the ISAE 3402/SSAE 18 standards.
		AAC-02.6 Are the results of the penetration tests available to tenants at their request?	Yes			Secure Cloud shares the headline results of penetration tests, internal and external audits at regular Customer Security Working Group meetings.
		AAC-02.7 Are the results of internal and external audits available to tenants at their request?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
AAC-03 Information System Regulatory Mapping	*Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.*	AAC-03.1 Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes			DXC monitors changes to the legal and regulatory requirements in relevant jurisdictions, to enable adjustment of its security programme to address changes to, and ensure ongoing compliance with, legal and regulatory requirements.

Business Continuity Management & Operational Resilience: BCR-01 to BCR-11

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-01 Business Continuity Planning	*A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:* *• Defined purpose and scope, aligned with relevant dependencies* *• Accessible to and understood by those who will use them* *• Owned by a named person(s) who is responsible for their review, update, and approval* *• Defined lines of communication, roles, and responsibilities* *• Detailed recovery procedures, manual work-around, and reference information* *• Method for plan invocation.*	BCR-01.1 Does your organization have a plan or framework for business continuity management or disaster recovery management?	Yes			DXC has established a corporate business resilience framework, including policies, processes and a programme which addresses emergency response, crisis management, business continuity management and disaster recovery management in order to meet business, legal, regulatory and contractual requirements.
		BCR-01.2 Do you have more than one provider for each service you depend on?	Yes			Secure Cloud has multiple suppliers for critical services, as determined through business impact analysis.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-01 Business Continuity Planning	*A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:* *• Defined purpose and scope, aligned with relevant dependencies* *• Accessible to and understood by those who will use them* *• Owned by a named person(s) who is responsible for their review, update, and approval* *• Defined lines of communication, roles, and responsibilities* *• Detailed recovery procedures, manual work-around, and reference information* *• Method for plan invocation.*	BCR-01.3 Do you provide a disaster recovery capability?	Yes			Secure Cloud offers tiered options for disaster recovery, depending on a customer's/tenant's business requirements, and on their recovery point and recovery time objectives.
		BCR-01.4 Do you monitor service continuity with upstream providers in the event of provider failure?	Yes			DXC's operational processes monitor the status of critical services provided by upstream providers to ensure a prompt response in the event of a critical incident.
		BCR-01.5 Do you provide access to operational redundancy reports, including the services you rely on?	Yes			DXC regularly tests the redundancy of critical equipment, and the test reports are shared with and assessed by internal and external auditors during the audit cycle.
		BCR-01.6 Do you provide a tenant-triggered failover option?	Yes			Secure Cloud offers tiered recovery services options to its customers/tenants, including a tenant-triggered failover option, subject to contractual and service agreements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-01 Business Continuity Planning	*A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:* *• Defined purpose and scope, aligned with relevant dependencies* *• Accessible to and understood by those who will use them* *• Owned by a named person(s) who is responsible for their review, update, and approval* *• Defined lines of communication, roles, and responsibilities* *• Detailed recovery procedures, manual work-around, and reference information* *• Method for plan invocation.*	BCR-01.7 Do you share your business continuity and redundancy plans with your tenants?	Yes			Depending on a customer's/tenant's business and recovery requirements and the Secure Cloud recovery services agreed between the parties, DXC will work with the customer/tenant to jointly establish IT service continuity and disaster recovery plans and procedures to ensure that the customer's/tenant's recovery point objectives and recovery time objectives are achieved.
BCR-02 Business Continuity Testing	*Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.*	BCR-02.1 Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes			Business continuity plans are reviewed and tested periodically or upon significant organisational and environmental changes.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-03 Power / Telecommunications	*Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.*	BCR-03.1 Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	Yes			DXC Data Centres hosting the Secure Cloud infrastructure are certified to ISO 9001, ISO 14001, ISO 27001, ISO 27017, ISO 22301, ISO 50001, and conform to the ISAE 3402/SSAE 18 standards.
		BCR-03.2 Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	Yes			Secure Cloud systems are hosted in facilities that have implemented appropriate environmental and physical security controls, resilience and redundancy measures, including automated fail-over mechanisms, to safeguard against failures in supporting utilities or environmental conditions, supported by a preventative maintenance programme, monitoring tools and incident response procedures.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-04 Documentation	*Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:* *• Configuring, installing, and operating the information system* *• Effectively using the system's security features*	BCR-04.1 Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes			Comprehensive information system documentation and artefacts are available; these are made available to authorised administration and support staff.
BCR-05 Environmental risks	*Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.*	BCR-05.1 Is physical damage anticipated and are countermeasures included in the design of physical protections?	Yes			Secure Cloud systems are hosted in facilities which have been designed to include physical protection measures which protect the systems from damage from diverse threats, including disasters occurring through natural causes and man-made threats.
BCR-06 Equipment location	*To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.*	BCR-06.1 Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		No		DXC data centres are based at locations that have low risk from external environmental and man-made threats, validated by an annual threat assessment.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-07 Equipment Maintenance	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.*	BCR-07.1 Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	Yes			Environmental systems and IT systems at Secure Cloud data centres and support locations are managed by documented policies, procedures and business processes. They are maintained under the vendors' (or approved alternative) hardware support and maintenance plans, and a preventative maintenance programme is in place for Data Centre equipment and systems.
		BCR-07.2 Do you have an equipment and datacenter maintenance routine or plan?	Yes			
BCR-08 Equipment Power Failures	*Protection measures shall be put into place to react to natural and man-made threats based upon a geographically specific business impact assessment.*	BCR-08.1 Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes			Geographically specific threat and impact assessments have been conducted at the Secure Cloud data centres to consider diverse natural and man-made threats. To reduce the impact of failures in utilities, the Secure Cloud data centres have implemented redundancies for all critical equipment.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-09 Impact Analysis	*There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:* *• Identify critical products and services* *• Identify all dependencies, including processes, applications, business partners, and third party service providers* *• Understand threats to critical products and services* *• Determine impacts resulting from planned or unplanned disruptions and how these vary over time* *• Establish the maximum tolerable period for disruption* *• Establish priorities for recovery* *• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption* *• Estimate the resources required for resumption*	BCR-09.1 Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc)?	Yes			The DXC Business Resilience framework, which is used to conduct business impact analysis, is aligned to ISO 22301 and ISO 27001.
		BCR-09.2 Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	Yes			A business impact analysis (BIA) is conducted as a key step in the development of a business continuity plan. BIAs consider disruptions to the Secure Cloud services and they are performed for the main delivery sites.
BCR-10 Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.*	BCR-10.1 Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes			Secure Cloud makes available DXC policies, standards and processes for governance and service management to support staff. These incorporate industry standards such as ISO 9001, ISO 27001, ISO 22301 and codes of practice ISO 27002 and ISO 27017, enhanced to meet customer requirements, including Public Services Network compliance. DXC utilises the ITIL framework for service management processes, supported by specialised training.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-11 Retention Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	BCR-11.1 Do you have technical capabilities to enforce tenant data retention policies?	Yes			Secure Cloud has the technical and management capabilities to offer its customers/tenants a number of options for backup and recovery, which are captured in the contractual and service agreements with the customer/tenant and take into account the type and frequency of backups, storage options, retention periods for data, and ensure that applicable legal, statutory, regulatory requirements are addressed. The backup and recovery designs are documented and associated policies, service descriptions, processes, procedures and tooling are in place.
		BCR-11.2 Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	Yes			
		BCR-11.3 Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes			
		BCR-11.4 If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Yes			The Secure Cloud backup solution treats virtual machines as physical servers and is not dependent on the hypervisor. The backup of a virtual machine can be independently restored and recovered to DXC-provided or customer-provided hardware, subject to contractual and service agreements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
BCR-11 Retention Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	BCR-11.5 If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?		No		Virtual machines are backed up in accordance with the backup policy, and tenants are not provided with the capability to restore the backups; customers/tenants may request restores, which are fulfiled by DXC.
		BCR-11.6 Does your cloud solution include software/provider independent restore and recovery capabilities?	Yes			The Secure Cloud backup solution offers a tape backup option that can be used with any independent industry standard IT Service Continuity provider.
		BCR-11.7 Do you test your backup or redundancy mechanisms at least annually?	Yes			Data recovery is regularly performed by DXC staff as part of its service to customers/tenants. DXC may also support disaster recovery testing, depending on a customer's/tenant's requirements and subject to contractual and service agreements. Redundancy testing is performed at various levels, including testing of the Data Centre critical infrastructure, and failover testing in accordance with a tenant's requirements.

Change Control and Configuration Management: CCC-01 to CCC-05

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
CCC-01 New Development / Acquisition	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.*	CCC-01.1 Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes			DXC policies and processes are followed for procurement of IT hardware or software or third-party services for Secure Cloud. This requires pre-approval by the appropriate level of authority in DXC's business leadership. Business and architecture governance processes are in place for acquisitions, changes to Secure Cloud architecture or provision of new cloud services; a change management process is in place for operational changes in the Secure Cloud environment.
CCC-02 Outsourced Development	*External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).*	CCC-02.1 Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	Yes			An ITIL-based change management process is communicated to all customers and business partners, and applies to all changes, including new releases, in the Secure Cloud environment, whether initiated by DXC or a third party. The change management process applies to all the cloud environments and is strictly enforced.
		CCC-02.2 Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
CCC-03 Quality Testing	*Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.*	CCC-03.1 Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	Yes			Secure Cloud has a process in the system development life cycle (SDLC) for onboarding a customer onto a Secure Cloud service. Change management and quality testing are integral to this process before a product or service is implemented and used in the Production environment. Changes are reviewed by the Security team to ensure that confidentiality, integrity and availability of information systems and services are in accordance with policies and standards.
		CCC-03.2 Is documentation describing known issues with certain products/services available?	Yes			Issues with products and services are logged through the incident and problem management processes. Security testing of the cloud system is conducted on a regular basis, and all issues or vulnerabilities affecting the products or services are reported to management, technical and/or delivery teams for resolution. Their status is monitored; where necessary, projects are initiated to resolve the issues or vulnerabilities through patching or upgrading the software to a secure version or choosing an alternative product.
		CCC-03.3 Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes			
		CCC-03.4 Do you have controls in place to ensure that standards of quality are being met for all software development?			N/A	Secure Cloud does not undertake software development activity, nor does it outsource such activity.
		CCC-03.5 Do you have controls in place to detect source code security defects for any outsourced software development activities?			N/A	

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
CCC-03 Quality Testing	*Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.*	CCC-03.6 Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?			N/A	Secure Cloud does not develop code but integrates COTS applications. Secure Cloud's change management processes require all changes into the live cloud environment and for new releases of software to undergo quality and security reviews to ensure that software is production-ready and does not contain debugging and test code elements.
CCC-04 Unauthorized Software Installations	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	CCC-04.1 Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes			Configuration and change management processes and procedures are in place to track the status of configuration items. DXC managed IT components are locked down through technical measures and monitored to prevent unauthorised changes.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
CCC-05 Production changes	*Policies and procedures shall be established for managing the risks associated with applying changes to:* *• Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.* *• Infrastructure network and systems components.* *Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.*	CCC-05.1 Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Yes			Tenants are provided with documentation describing the change management process and procedures, and the roles and responsibilities of all parties involved in the process.
		CCC-05.2 Do you have policies and procedures established for managing risks with respect to change management in production environments?	Yes			The change management process and procedures in the production environments include the identification of risks, and their management; these are reviewed by the change board and must be authorised before the change can proceed.
		CCC-05.3 Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	Yes			Technical measures are in place to ensure that changes in production environments are registered, authorised and adhere to SLAs.

Data Security & Information Lifecycle Management: DSI-01 to DSI-07

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DSI-01 Classification	*Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.*	DSI-01.1 Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Yes			Secure Cloud is hosted in the UK, approved for information classified as UK Government OFFICIAL, and supported by teams based in the UK. The Policy tags are not used, but administrative metadata of the cloud systems is maintained as part of the asset and configuration management processes.
		DSI-01.2 Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Yes			Secure Cloud hardware is tagged and managed in accordance with asset management policies and procedures. Secure Cloud holds administrative metadata in its asset inventories.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DSI-02 Data Inventory / Flows	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.*	DSI-02.1 Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?		No		Data flows within the Secure Cloud environment are documented as part of the design. Data flows are not inventoried, but changes are documented, reviewed and approved as part of change management.
		DSI-02.2 Can you ensure that data does not migrate beyond a defined geographical residency?	Yes			All Secure Cloud DXC managed data is stored within the UK border.
DSI-03 E-commerce Transactions	*Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.*	DSI-03.1 Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes			Secure Cloud does not provide electronic commerce services, but it offers the use of standardised non-proprietary encryption algorithms to protect tenant data in transit if it is to be moved through public networks.
		DSI-03.2 Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes			Secure Cloud uses open encryption methodologies when infrastructure components need to communicate with each other via public networks.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DSI-04 Handling / Labeling / Security Policy	*Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.*	DSI-04.1 Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	Yes			DXC has comprehensive policies, standards and procedures for labelling, handling and protecting data and objects containing data.
		DSI-04.2 Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes			DXC policies and procedures address data that is classified in accordance with DXC commercial requirements, as well as data classified using Cabinet Office Government Security Classification policy and procedures.
		DSI-04.3 Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes			Data aggregation is considered during business impact analysis and risk assessment, and the resulting data classification assigned to data and objects containing data is reflected in policies and procedures.
DSI-05 Nonproduction Data	*Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.*	DSI-05.1 Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes			Secure Cloud does not use live or personal data of tenants for testing unless necessary and explicitly pre-approved by the tenant's Senior Information Risk Owner (SIRO) or Information Asset Owner.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DSI-06 Ownership / Stewardship	*All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.*	DSI-06.1 Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	Yes			The responsibilities regarding data stewardship are defined, assigned, documented, and communicated in contract and service agreements, and DXC policies and processes.
DSI-07 Secure Disposal	*Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.*	DSI-07.1 Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	Yes			The responsibilities regarding data stewardship are defined, assigned, documented, and communicated in contract and service agreements, and DXC policies and processes.
		DSI-07.2 Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes			The DXC G-Cloud service definitions describe the procedure for exiting a Secure Cloud service arrangement, including secure deletion of tenant data. This can be further supplemented, if required, in contractual and service agreements between DXC and the tenant organisation.

Datacenter Security: DCS-01 to DCS-09

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DCS-01 Asset Management	*Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.*	DCS-01.1 Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	Yes			Secure Cloud assets are categorised and classified as part of the risk assessment process, which assigns the assets' loss impacts based on several considerations, including their significance to service levels, operational continuity, and business criticality.
		DCS-01.2 Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes			Secure Cloud maintains an inventory of physical assets used to deliver the services, storing key information about the asset, including its business criticality, location, and ownership.
DCS-02 Controlled Access Points	*Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.*	DCS-02.1 Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Yes			Secure Cloud services are provided from locations with defined physical security perimeters and controls commensurate with their security categorisation.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DCS-03 Equipment Identification	*Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.*	DCS-03.1 Do you have a capability to use system geographic location as an authentication factor?		No		Automatic identification of equipment based on location-aware technologies is not used as a method of connection authentication in general, as there are alternative security mechanisms in place.
		DCS-03.2 Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?		No		
DCS-04 Offsite Authorization	*Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.*	DCS-04.1 Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	Yes			All hardware (containing software and/or data) that provides the cloud services has a fixed location and may only be removed in accordance with change management procedures that require explicit authorisation.
DCS-05 Offsite Equipment	*Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.*	DCS-05.1 Can you provide tenants with your asset management policies and procedures?		No		Whilst DXC will not provide tenants its internal policies and procedures for asset management, it can provide tenants information about the standards followed for secure sanitisation and disposal of assets, as this is in accordance with the NCSC guidelines.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DCS-06 Policy	*Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.*	DCS-06.1 Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	Yes			Evidence of policies, standards and procedures for maintaining a safe and secure working environment is provided during internal/external audits, and is in scope of external certification audits, including ISO 27001 and ISAE 3402/SSAE 18.
		DCS-06.2 Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	Yes			Evidence of staff security awareness training is provided during internal/external audits, and is in scope of external certification audits, including ISO 27001 and ISO 27017.
DCS-07 Secure Area Authorization	*Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.*	DCS-07.1 Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	Yes			Comprehensive physical access control mechanisms are in place to secure, constrain and monitor egress and ingress points.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
DCS-08 Unauthorized Persons Entry	*Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.*	DCS-08.1 Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Yes			At the Secure Cloud locations, ingress and egress points, including service and loading areas are secured and monitored, and separated from data processing facilities.
DCS-09 User Access	*Physical access to information assets and functions by users and support personnel shall be restricted.*	DCS-09.1 Do you restrict physical access to information assets and functions by users and support personnel?	Yes			Secure Cloud restricts physical access to information assets and functions to the minimum required by a functional role.

Encryption & Key Management: EKM-01 to EKM-04

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
EKM-01 Entitlement	*Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.*	EKM-01.1 Do you have key management policies binding keys to identifiable owners?	Yes			Keys in use for the Secure Cloud services are managed in accordance with established policies and assigned responsibilities and can be attributed to a single user.
EKM-02 Key Generation	*Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.*	EKM-02.1 Do you have a capability to allow creation of unique encryption keys per tenant?	Yes			Secure Cloud has the capability to create and manage unique encryption keys for tenants, if required, subject to contractual and service agreements. In practice, Secure Cloud creates, maintains and manages encryption keys for its standard services.
		EKM-02.2 Do you have a capability to manage encryption keys on behalf of tenants?	Yes			
		EKM-02.3 Do you maintain key management procedures?	Yes			Secure Cloud has documented procedures for managing encryption keys, associated tools and devices which are used in its standard services.
		EKM-02.4 Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes			The Secure Cloud has documented procedures describing the lifecycle for encryption keys and the associated roles and responsibilities.
		EKM-02.5 Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes			Secure Cloud uses certified proprietary cryptographic products, supporting industry standard protocols and open source encryption algorithms to manage encryption keys.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
EKM-03 Encryption	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.*	EKM-03.1 Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes			Secure Cloud encrypts data on mobile devices provided as part of its services. Some, but not all data residing on storage devices within the environment is encrypted by default; Secure Cloud has the capability to encrypt data at rest, if a customer/tenant requires it, subject to contractual and service agreements.
		EKM-03.2 Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes			Encryption is used to protect data in transit across untrusted networks and under Secure Cloud management or within scope of a Secure Cloud service. Secure Cloud will assist customers/tenants during data migrations to ensure that data is protected with industry standard encryption, in accordance with customer/tenant requirements, and subject to contractual and service agreements.
		EKM-03.3 Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Yes			Secure Cloud has encryption management policies, standards and associated procedures in place.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
EKM-04 Storage and Access	*Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.*	EKM-04.1 Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes			Secure Cloud uses industry-standard encryption and algorithms in open/validated formats on its cloud platforms and applications.
		EKM-04.2 Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		No		Secure Cloud maintains its own encryption keys. Tenants have full control over their cryptographic keys which they may wish to use to encrypt their own data, under their management.
		EKM-04.3 Do you store encryption keys in the cloud?	Yes			Secure Cloud stores its keys securely in a managed and segregated environment. Specialised software and hardware products are used which meet the compliance requirements of various standards such as NIST SP 800-131A, CC EAL4+ and FIPS 140-2.
		EKM-04.4 Do you have separate key management and key usage duties?	Yes			The Secure Cloud policies and procedures specify segregation of duties for key management and usage activities.

Governance and Risk Management: GRM-01 to GRM-11

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-01 Baseline Requirements	*Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.*	GRM-01.1 Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?		No		DXC has documented information security baselines for most, but not all, components of the cloud infrastructure.
		GRM-01.2 Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		No		Continuous monitoring and reporting of compliance against the security baseline for all IT infrastructure components is not in place, but regular vulnerability scanning and security testing is performed to identify and address vulnerabilities in systems.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-02 Risk Assessments	*Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:* *• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure* *• Compliance with defined retention periods and end-of-life disposal requirements* *• Data classification and protection from unauthorized use, access, loss, destruction, and falsification*	GRM-02.1 Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	Yes			The risk assessment process considers diverse threats to data, including legal and regulatory requirements relating to residency, data retention, data classification and protection.
		GRM-02.2 Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes			Risk management is an ongoing activity, performed at least once a year, and considers threats related to data governance.
GRM-03 Management Oversight	*Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.*	GRM-03.1 Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes			All DXC employees are required to complete the annual corporate ethics, compliance and security training and there is an additional guide for managers to help them support their staff and ensure that they complete the training. In addition, there is specific annual security training for staff supporting cloud services, which is monitored and tracked, with the involvement of managers to ensure compliance of their staff.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-04 Management Program	*An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:* *• Risk management* *• Security policy* *• Organization of information security* *• Asset management* *• Human resources security* *• Physical and environmental security* *• Communications and operations management* *• Access control* *• Information systems acquisition, development, and maintenance*	GRM-04.1 Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		No		DXC does not, in general, provide tenants with documentation about its ISMP. Where contractual and service agreements are in place with a DXC tenant, relating to a specific ISMP, the relevant documentation will be shared, in accordance with the terms in these agreements.
		GRM-04.2 Do you review your Information Security Management Program (ISMP) at least once a year?	Yes			Activities that form part of an Information Security Management Programme are reviewed regularly, and at least once a year, as part of the ongoing security management and continuous improvement activities.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-05 Management Support / Involvement	*Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.*	GRM-05.1 Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	Yes			DXC executive management supports the information security activities within the corporation, through the Chief Risk Office and DXC IT Enterprise Security. This includes the creation of the policies, standards, procedures, guidelines and tooling for information security, and a cybersecurity awareness programme. A DXC Senior Information Risk Owner (SIRO) is in place, responsible for Information Assurance (IA) governance for the Secure Cloud services.
GRM-06 Policy	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	GRM-06.1 Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Yes			DXC information security policies and standards, implementation procedures, and guidelines are authorised by the business leadership and made available, as required, to staff supporting the services. These are supported by an IT security strategy and an Information Security Management Programme aligned to industry standards, with roles and responsibilities for information security documented and assigned.
		GRM-06.2 Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-06 Policy	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	GRM-06.3 Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes			Where external parties are required to provide services, DXC ensures that information security requirements are included in the third-party agreements.
		GRM-06.4 Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	Yes			A mapping of standards and/or regulatory requirements to the controls is in place, along with the relevant policies, processes and architectural artefacts.
		GRM-06.5 Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Yes			Secure Cloud controls and processes are aligned to HMG and PSN security requirements, and to industry standards such as ISO 27001, ISO 27017, CSA CCM, ISAE 3402/SSAE 18. These are externally and independently assessed by PSN assessors, UKAS-accredited certification bodies or AICPA-regulated audit companies. Customers may request copies of ISO certificates or purchase SOC reports.
GRM-07 Policy Enforcement	*A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.*	GRM-07.1 Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes			A DXC disciplinary policy and process is established for employees who have violated DXC security policies and procedures. All employees are made aware of their responsibilities to meet the security requirements and the consequences of not doing so.
		GRM-07.2 Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-08 Business / Policy Change Impacts	*Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.*	GRM-08.1 Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	Yes			Secure Cloud risk assessment results consider any updates which may be required to the security policies, procedures, standards and controls to ensure their continued effectiveness.
GRM-09 Policy Reviews	*The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.*	GRM-09.1 Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes			Material changes to information security policies and procedures which may affect Secure Cloud services are communicated to relevant parties, including tenant representatives who attend the regular Customer Security Working Group meetings.
		GRM-09.2 Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes			Secure Cloud follows information security policies which are reviewed at least annually to ensure that they are accurate, relevant, aligned to the corporate security strategy and include applicable legal, statutory, regulatory and contractual compliance obligations.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
GRM-10 Assessments	*Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).*	GRM-10.1 Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes			Formal risk assessments of Secure Cloud, aligned with the enterprise-wide framework, are performed at least annually. The methodology determines likelihoods and impacts of identified threats, using qualitative and quantitative methods to calculate inherent and residual risks.
		GRM-10.2 Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	Yes			The risk assessment process calculates the likelihood, impact and risk for inherent and emerging threats across multiple threat categories, and then independently calculates the residual risk for each threat, taking int account the controls implemented to mitigate the threat.
GRM-11 Program	*Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.*	GRM-11.1 Do you have a documented, organization-wide program in place to manage risk?	Yes			DXC has a documented, organization-wide program in place to manage risk.
		GRM-11.2 Do you make available documentation of your organization-wide risk management program?	Yes			The risk assessment process, results and associated documentation is made available to external auditors during ISO 27001, 27017 and CSA CCM certification and surveillance audits

Human Resources: HRS-01 to HRS-11

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-01 Asset Returns	*Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.*	HRS-01.1 Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Yes			DXC's asset management policy requires workforce personnel to return all organisation-owned assets upon termination of their employment, contract or agreement, and this is also covered in security awareness training.
		HRS-01.2 Do you have asset return procedures outlining how assets should be returned within an established period?	Yes			DXC policies and procedures require IT assets to be returned at the time of end of employment, end of need for use, or end of life of the IT asset.
HRS-02 Background Screening	*Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.*	HRS-02.1 Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	Yes			DXC performs pre-employment screening on prospective employees as part of the corporate new hire process and as permitted under local law. Additional screening, complying with HMG personnel security and national vetting policies, is performed in accordance with contractual requirements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-03 Employment Agreements	*Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.*	HRS-03.1 Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Yes			DXC staff are required to sign a confidentiality statement as part of the employee terms and conditions in their employment contract and must agree to comply with the security obligations in the DXC Code of Business Conduct during employee induction and annually thereafter. Staff working on contracts for Government or supporting organisations must comply with the requirements of the Official Secrets Act.
		HRS-03.2 Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-04 Employment Terminations	*Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.accessed, the business requirements, and acceptable risk.*	HRS-04.1 Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes			DXC has policies, standards and processes in place for changes in employment and/or termination, including the role and responsibilities of staff and their managers.
		HRS-04.2 Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes			The DXC policies and standards specify the required timeframes for revocation of system access for a change in or termination of employment.
HRS-05 Portable / Mobile Devices	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).*	HRS-05.1 Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization’s facilities)?	Yes			DXC has comprehensive policies, standards and procedures for managing the risks associated with the use of organizationally owned or personal mobile devices. The policies do not permit DXC staff to use mobile devices (phones and tablets) for administration of Secure Cloud systems, and such access is not technically enabled.
HRS-06 Non-Disclosure Agreements	*Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.*	HRS-06.1 Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	Yes			DXC has Confidential Information and Non-Disclosure Agreements policies that apply to all DXC staff and third parties that have access to DXC information. These policies specify the applicability, the responsibilities of staff for review and approval, and the requirements to protect DXC's confidential and proprietary information.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-07 Roles / Responsibilities	*Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.*	HRS-07.1 Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Yes			The contract for services between DXC and the tenant organisation subscribed to Secure Cloud services specifies the responsibilities of DXC and the tenant. A more detailed document describing the shared administrative responsibilities of DXC and the customer/tenant for the cloud services is also specified and communicated.
HRS-08 Acceptable Use	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.*	HRS-08.1 Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	Yes			DXC has comprehensive policies and procedures for the acceptable use of organizationally owned or personal (BYOD) end-point devices for business purposes and to access corporate resources. DXC staff are not permitted to use mobile phones or tablets for administration of Secure Cloud systems, and such access is not technically enabled. These policies are communicated through annual security awareness training.
		HRS-08.2 Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-09 Training / Awareness	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	HRS-09.1 Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?		No		DXC provides access to cloud-related technical and security training, but these are not mandatory for the administration teams that deliver the cloud services. However, formal mandatory annual security awareness training is provided covering the security requirements for UK Government.
		HRS-09.2 Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Yes			Tailored annual security training is mandatory for staff working on DXC UK Government accounts, including staff supporting Secure Cloud, and security induction training is provided to staff who gain a security clearance: these cover their specific role and associated controls that must be fulfilled to meet UK Government security requirements.
		HRS-09.3 Do you document employee acknowledgment of training they have completed?	Yes			All staff are required to acknowledge the training they have completed, and records are kept. Metrics for training completed are monitored by DXC.
		HRS-09.4 Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes			Successful and timed completion of the mandatory security training is a requirement for gaining and maintaining access to Secure Cloud systems.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-09 Training / Awareness	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	HRS-09.5 Are personnel trained and provided with awareness programs at least once a year?	Yes			DXC corporate security training and mandatory training for staff working on DXC UK Government accounts, including all staff supporting Secure Cloud, require completion on an annual basis. DXC Security provides regular cybersecurity awareness and communications on security matters.
		HRS-09.6 Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes			DXC staff, including those supporting Secure Cloud services were required to take GDPR training, which advised them of their responsibilities with respect to data protection requirements.
HRS-10 User Responsibility	*All personnel shall be made aware of their roles and responsibilities for:* *• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.* *• Maintaining a safe and secure working environment*	HRS-10.1 Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Yes			Awareness of their roles and responsibilities and requirement to follow security policies, standards, procedures, legal and regulatory requirements is communicated to users through annual DXC Code of Business Conduct and security training and annual security training for staff supporting UK Government accounts.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
HRS-10 User Responsibility	*All personnel shall be made aware of their roles and responsibilities for:* *• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.* *• Maintaining a safe and secure working environment*	HRS-10.2 Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	Yes			Staff are made aware of their roles and responsibilities for the safety and security measures that must be followed, either through annual training or specific site-based inductions.
		HRS-10.3 Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	Yes			The DXC corporate and UK Government account security training courses specify the responsibilities of staff in regard to securing equipment and ensuring appropriate safeguards are in place if equipment is to be left unattended.
HRS-11 Workspace	*Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.*	HRS-11.1 Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	Yes			Screen lock policies are automatically enforced on user access devices and virtual desktops after a certain period of inactivity.
		HRS-11.2 Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	Yes			DXC policies require clear desks and clear screens, using technical measures such as screen locks, and procedural measures which require documentation, removable media and other material with sensitive information to be locked away when not in use.

Identity & Access Management: IAM-01 to IAM-13

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-01 Audit Tools Access	*Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.*	IAM-01.1 Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes			Secure Cloud system audit tools are installed on systems with specific roles and usage and are subject to network and user access controls to restrict access to the relevant administrator group. Audit logs are accessible only to a specialised team which analyses and responds to audit events. Audit tools used for vulnerability scanning are accessible only to the dedicated team that performs the security testing.
		IAM-01.2 Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes			Privileged access to Secure Cloud platforms is logged using automated tools and monitored by a specialised team. Only this team has access to the collated logs, to analyse the events and assess whether these are security incidents that need further investigation.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-02 User Access Policy	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:* *• Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)*	IAM-02.1 Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?		No		DXC policies and standards require prompt removal of leavers' IT access to systems. Secure Cloud is dependent on initial action by a DXC leaver's manager to promptly submit the deprovisioning request as part of the exit process; there is also a compensating control to ensure that dormant accounts are regularly reviewed and disabled.
		IAM-02.2 Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	Yes			DXC access control policies and standards have been established to ensure compliance with legal, statutory, regulatory and contractual requirements. The Secure Cloud system is designed to store and process UK Government classified information and meets the requirements for PSN compliance. Relevant legislation is considered, such as the Official Secrets Act and Data Protection Act. Technical measures, processes and procedures enforce the requirements for DXC users, and tenants, where applicable.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-02 User Access Policy	• *Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)* • *Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)*	IAM-02.3 Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?		No		DXC policies require access to be provided on a least privilege basis. Role-based access is implemented where feasible, but not fully implemented across all systems and services. Processes and procedures are in place for requesting, authorising, granting and revoking access, including privileged access.
		IAM-02.4 Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	Yes			Data access within the Secure Cloud environment is segmented for different tenants; a tenant can access only their own data; this is enforced through a variety of technical and procedural measures.
		IAM-02.5 Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	Yes			Secure Cloud uses the principles of authentication, authorisation and accounting to manage access to data and system functions within the cloud environment.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-02 User Access Policy	• *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible* • *Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)* • *Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions* • *Adherence to applicable legal, statutory, or regulatory compliance requirements* **Requirements in bullet points 4 to 7 are covered in IAM-12 questions.*	IAM-02.6 Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	Yes			Where a higher level of assurance is required for critical business case considerations, DXC policies allow for customisation of security controls to include enhanced measures. Where additional measures and customisation is required to meet tenant-specific security requirements, such as multi-factor authentication, these are subject to contractual and service agreements.
		IAM-02.7 Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	Yes			Secure Cloud provides metrics for the KPI for emergency disablement of customer/tenant user IDs as part of monthly service level reporting to DXC customers that require this service.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-03 Diagnostic / Configuration Ports Access	*User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.*	IAM-03.1 Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	Yes			Logical and physical access to diagnostic and configuration ports is restricted to authorised staff, based on functional necessity, utilising the change management process and access control measures.
IAM-04 Policies and Procedures	*Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.*	IAM-04.1 Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?		No		Identity information and associated access entitlements of Secure Cloud support users and third parties and their associated accounts across the IT infrastructure is available; however the complete profile of users across the whole estate, including their level of access, is currently not automatically available, but may be manually created.
		IAM-04.2 Do you manage and store the user identity of all personnel who have network access, including their level of access?		No		
IAM-05 Segregation of Duties	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.*	IAM-05.1 Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?		No		Roles and responsibilities within Secure Cloud services are documented and shared between the provider and customers. Segregation of duties for the cloud services is implemented at various levels using dedicated teams providing defined services. Due to its sensitive nature, the details are not shared with the tenant through documentation, but segregation of duties is in scope of external audits, and Secure Cloud is able to respond to specific questions from tenants.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-06 Source Code Access Restriction	*Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.*	IAM-06.1 Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?			N/A	Secure Cloud does not develop software, and hence does not create application, program or object source code for the cloud environment.
		IAM-06.2 Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes			Controls are in place for administering and managing system and user accounts in a tenant's compartment, and access to data, applications and source code within the tenant's compartment is restricted to authorised users.
IAM-07 Third Party Access	*The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.*	IAM-07.1 Does your organization conduct third-party unauthorized access risk assessments?	Yes			Third party access requests to DXC managed Secure Cloud systems are evaluated for risk and only permitted if specific conditions are satisfied. Customers/tenants must agree to the contractual provisions and the Secure Cloud Code of Connection before gaining access to the cloud environment.
		IAM-07.2 Are preventive, detective and corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	Yes			Policies, standards and controls are in place to ensure that access to the Secure Cloud systems and services is secured, and a process is in place to formally request and gain authorisation of access to the environment before it is provisioned. Security events are logged and monitored, including attempts for unauthorised access to systems, which, if detected, would be addressed by the security incident management process.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-08 User Access Restriction / Authorization	*Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.*	IAM-08.1 Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	Yes			The granting, approval and enforcement of access privileges to tenant credentials depends on the consumed Secure Cloud service (IaaS, PaaS or SaaS). Least privilege for tenant credentials is enforced where tenants have identified specific tenant roles and the associated least privilege access entitlements; the roles and responsibilities of DXC staff for access management functions, including privileged access management for the different services are documented, and elevated privileges require explicit approval.
		IAM-08.2 Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	Yes			DXC access control policies and standards specify the rules for the permissible storage and access of identities used for authentication. Secure Cloud operating procedures require DXC Secure Cloud support staff to adhere to the "Need to know" principle, which stipulates that they must not attempt to access information for which they have no need-to-know or legal right to access.
		IAM-08.3 Do you limit identities' replication only to users explicitly defined as business necessary?	Yes			Replication of access for networks and platforms is not permitted; requesters must explicitly state the system, domain and level of access rights being requested in the access request and this must be explicitly approved before being provisioned by authorised security administrators.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-09 User Access Authorization	*Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.*	IAM-09.1 Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	Yes			A An access request and authorisation process and associated procedures are in place for DXC staff requiring access to Secure Cloud services. There are additional requirements and restrictions for third party staff requesting access. Depending on the cloud service consumed (IaaS, PaaS or SaaS), customers/tenants also have responsibilities for putting in place appropriate access request, authorisation and provisioning processes for their staff, including tenant organisation staff.
		IAM-09.2 Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-10 User Access Reviews	*User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.*	IAM-10.1 Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?		No		DXC policies and standards require formal reviews of access of Secure Cloud administration and support users to be conducted at least annually and validated in accordance with the principle of least privilege, but a formal annual review process is not yet fully in place across all systems.
		IAM-10.2 Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?		No		Evidence is retained when access reviews take place, however, this is not available for all systems at an annual frequency.
		IAM-10.3 Do you ensure that remediation actions for access violations follow user access policies?	Yes			When access violations within the Secure Cloud environment are identified, remediation is performed to address the primary non-compliance to access policy, based on risk assessment.
		IAM-10.4 Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes			If unauthorised access to tenant data or systems is identified, it is logged as a security incident, reported to the customer/tenant, as appropriate, and investigated.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-11 User Access Revocation	*Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	IAM-11.1 Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?		No		Timely deprovisioning is fully dependent on a manager's prompt deprovisioning request in advance of an employee's change in status, and there are no automated mechanisms in place to enforce this. A compensating control is in place to regularly review DXC staff user ID status, disabling and removing dormant User IDs from directory services.
		IAM-11.2 Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes			DXC treats termination of employment, contract or agreement, change of employment or transfer within the organization as a change in the user's status which requires return of DXC assets and revocation of access entitlements to Secure Cloud systems.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-12 User ID Credentials	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* *• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* *• Account credential lifecycle management from instantiation through revocation* *• Account credential and/or identity store minimization or re-use when feasible* *• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)*	IAM-12.1 Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes			Secure Cloud supports use of, or integration with, customer or tenant based SSO solutions for specific Secure Cloud services.
		IAM-12.2 Do you use open standards to delegate authentication capabilities to your tenants?	Yes			Secure Cloud supports the use of open standards o delegate authentication capabilities to tenants for specific Secure Cloud services.
		IAM-12.3 Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes			Secure Cloud supports identity federation standards, such as SAML, as a means of authenticating users for specific Secure Cloud services.
		IAM-12.4 Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	Yes			Secure Cloud is a UK-based service, but for specific services, it has a Policy Enforcement Point capability to enforce policy constraints on user access.
		IAM-12.5 Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?		No		Secure Cloud is approved to hold UK Government classified data, and Secure Cloud managed data resides in the UK, supported by UK- based staff. Role-based access functionality is enabled where supported by the underlying platform or application. Currently, Secure Cloud does not provide solutions to tenants for context-based access control to tenant data.
		IAM-12.6 Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	Yes			Secure Cloud provides strong authentication options to tenants for specified Secure Cloud services.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-12 User ID Credentials	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* *• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* *• Account credential lifecycle management from instantiation through revocation* *• Account credential and/or identity store minimization or re-use when feasible* *• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)*	IAM-12.7 Do you allow tenants to use third-party identity assurance services?	Yes			Secure Cloud offers tenants the ability to make use of third-party identity assurance services either within their own network compartment, or in conjunction with a Secure Cloud service, subject to meeting Secure Cloud security requirements and in accordance with contractual and service agreements.
		IAM-12.8 Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	Yes			DXC and Secure Cloud password policies specify the requirements for password length, age, history, complexity and account lockout parameters. These are technically enforced where supported by the underlying technology.
		IAM-12.9 Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes			Secure Cloud allows customers/tenants to specify password and account lockout policies for those systems that are directly under the control of the customer or tenant.
		IAM-12.10 Do you support the ability to force password changes upon first logon?	Yes			DXC policy requires password management systems to force a change in password at the time of the user's first logon, and this is enforced in Secure Cloud systems by technical measures, where supported by the underlying technology, or through procedures.
		IAM-12.11 Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes			Mechanisms are in place for unlocking Secure Cloud support user accounts following successful validation of the user. Customers/tenants also have responsibilities to unlock accounts using appropriate validation methods, depending on the services to which they have subscribed.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IAM-13 Utility Programs Access	*Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.*	IAM-13.1 Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	Yes			System utilities on Secure Cloud DXC managed IT systems are restricted to authorised DXC administrative staff. Access is controlled to limit the explicit privileges required to manage system components, such as virtualised partitions.

Infrastructure & Virtualization Security: IVS-01 to IVS-13

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-01 Audit Logging / Intrusion Detection	*Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.*	IVS-01.1 Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?		No		Secure Cloud has implemented network-based tools to monitor and respond to a range of threats, including malware and network intrusion attempts, and host-based anti-malware tools, but not host-based file integrity tools.
		IVS-01.2 Is physical and logical user access to audit logs restricted to authorized personnel?	Yes			Segregation of duties and a change management process are in place, to ensure that logical and physical access to Secure Cloud audit logs is restricted to authorised staff.
		IVS-01.3 Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	Yes			A mapping of the control set to security policies, standards and regulations, DXC processes, architectural designs and procedures is maintained.
		IVS-01.4 Are audit logs centrally stored and retained?	Yes			Logs of audit events are collected from across the IT cloud environment and stored centrally.
		IVS-01.5 Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes			Audit logs are reviewed for security events in real time using automated tools.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-02 Change Detection	*The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).*	IVS-02.1 Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?		No		A change to be made to a virtual machine (VM) image in the Secure Cloud environment must follow the change management process, including security review. Access to the servers hosting the VM images is restricted to authorised DXC staff and monitored using automated tooling, but changes to the images are not logged or alerted.
		IVS-02.2 Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?		No		Secure Cloud's virtual machine management infrastructure does not have a tamper audit or software integrity function but access to the servers hosting the virtual machine management software is restricted to authorised DXC staff.
		IVS-02.3 Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	Yes			A request for a change to a virtual machine image or moving an image to a different hypervisor must be initiated by a customer/tenant through the customer portal or via a non-standard service request to Secure Cloud. This would be fully documented and managed by Secure Cloud Services through the change management process, undergoing impact and security assessment to ensure that the integrity of the image is safeguarded.
IVS-03 Clock Synchronization	*A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.*	IVS-03.1 Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes			DXC Secure Cloud implements a network time service which provides a time signal to all DXC managed components within the IT estate to synchronise system clocks, and automated tooling is in place to monitor and report status.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-04 Capacity / Resource Planning	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	IVS-04.1 Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances /scenarios?		No		Secure Cloud does not provide documentation to customers on memory oversubscription thresholds. Secure Cloud does not oversubscribe system or network resources. It delivers capacity reports to customers as per agreed contractual and service agreements to ensure that the services are provided with the capacities required to meet the agreed service levels.
		IVS-04.2 Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Yes			Secure Cloud ensures that configuration controls are in place to ensure that hypervisor resources are used appropriately for the different classes of virtual machines under management, and that memory oversubscription does not occur.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-04 Capacity / Resource Planning	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	IVS-04.3 Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	Yes			Secure Cloud monitors the use of system resources by IT systems and by DXC staff, in real time and aggregated over longer periods. This usage is monitored by various DXC teams to confirm that the behaviour of the system is within its designed parameters and to identify trends to anticipate any required changes in system capacity.
		IVS-04.4 Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	Yes			System performance is monitored by various teams to ensure it meets DXC's and customers'/tenants' business requirements, including billing customers/tenants for service use and providing capacity reports to customers/tenants as per agreed contractual and service agreements.
IVS-05 Management - Vulnerability Management	*Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).*	IVS-05.1 Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	Yes			Secure Cloud vulnerability assessment tools and processes accommodate the virtualisation technologies being used.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-06 Network Security	*Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.*	IVS-06.1 For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Yes			Secure Cloud will provide support and guidance to customers, subject to contractual and service agreements, to assist them in creating a layered security in the Secure Cloud IaaS offering. Tenants must agree to the Secure Cloud Code of Connection to acknowledge that the baseline security requirements are being met.
		IVS-06.2 Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes			The original network architecture documents are not updated unless there is a major change to the design. Changes, such as service enhancements or changes to data flows, are managed through the change management process which may produce additional technical documentation for security review and approval before deployment.
		IVS-06.3 Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes			IT Health Check testing conducted at least annually, includes review of controls between different security zones and network segments within the Secure Cloud infrastructure, such as firewall rules and security configuration of network devices.
		IVS-06.4 Are all firewall access control lists documented with business justification?		No		Firewall access lists are created based on business and security requirements, and are maintained and tuned as necessary, to ensure that the required rules are in place, and redundant rules are removed. Changes to firewall rules follow the formal change management process and require security review and approval.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-07 OS Hardening and Base Controls	*Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.*	IVS-07.1 Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Yes			DXC utilises cybersecurity standards for creating the secure build and configuration of platforms. DXC managed components are subject to lock-down, anti-virus and malware protection and real-time protective monitoring.
IVS-08 Production / Non-Production Environments	*Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.*	IVS-08.1 For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes			Secure Cloud will provide testing and production in separate and distinct environments, subject to contractual and service agreements.
		IVS-08.2 For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Yes			Secure Cloud tenants may implement Production and non-Production environments within their managed infrastructure. DXC can provide guidance to a customer/tenant on how to do this, based on their requirements, and subject to contractual and service agreements
		IVS-08.3 Do you logically and physically segregate production and non-production environments?	Yes			Secure Cloud can provide logical and/or physical segregation of Production and non-Production environments, based on a customer's/tenant's requirements, and subject to contractual and service agreements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-09 Segmentation	*Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:* *• Established policies and procedures* *• Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance* *• Compliance with legal, statutory, and regulatory compliance obligations*	IVS-09.1 Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes			Secure Cloud protects network environments using firewalls to ensure that DXC's and a customer's business and security requirements are met.
		IVS-09.2 Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	Yes			Secure Cloud protects network environments using firewalls to ensure compliance with legal, regulatory and contractual requirements.
		IVS-09.3 Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	Yes			Secure Cloud tenants can choose between a shared cloud infrastructure or a more dedicated one, based on their business and security requirements. Secure Cloud constrains data flows and access paths to ensure that each tenant cannot access another tenant's IT assets, in adherence with policies, legal, statutory and regulatory requirements. Secure Cloud services are PSN-compliant and must adhere to permitted traffic flows and boundary and interface control requirements.
		IVS-09.4 Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes			Secure cloud data storage is configured to ensure that each tenant cannot access another tenant's data. The Service Management application shared instance enforces tenant data segregation, and this is validated during security testing.
		IVS-09.5 Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes			Secure Cloud system and network environments are firewalled to ensure protection and isolation of sensitive data.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-10 VM Security - Data Protection	*Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.*	IVS-10.1 Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	Yes			Secure Cloud handles system installations, system and data migrations as formal changes, undergoing technical and security reviews, requiring detailed implementation plans and customer approval. The migration activity will consider the security of the information assets and put in place appropriate measures, as agreed with the customer, including encrypted communication channels, and a network segregated from a production environment.
		IVS-10.2 Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	Yes			
IVS-11 VM Security - Hypervisor Hardening	*Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).*	IVS-11.1 Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes			Access to hypervisors are secured in line with an approved benchmark, which considers layered procedural and technical security controls in several categories. Access to hypervisor management functions and administration consoles is restricted to those staff that have functional responsibilities for hypervisor administration. The hypervisors are in scope of vulnerability scanning which are regularly performed on the Secure Cloud systems.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-12 Wireless Security	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:* *• Perimeter firewalls implemented and configured to restrict unauthorized traffic* *• Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)* *• User access to wireless network devices restricted to authorized personnel* *• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network*	IVS-12.1 Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Yes			At DXC locations, DXC IT wireless network environments are protected in accordance with corporate security policies and standards, and associated procedures.
		IVS-12.2 Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	Yes			DXC network architecture and operation security standards require strong encryption for authentication and transmission, and default vendor settings to be replaced with secure settings.
		IVS-12.3 Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes			Secure Cloud does not permit direct wireless connections into the Cloud environment, and wireless interfaces are disabled. DXC conducts regular scans of the environment to ensure that unauthorised wireless devices and traffic are not present at the locations of the Secure Cloud infrastructure.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IVS-13 Network Architecture	*Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.*	IVS-13.1 Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?		No		All Secure Cloud managed cloud data, data flows and provided services reside within the UK. The Secure Cloud network architecture diagrams identify separate zones, including those connected to untrusted networks, which may be considered higher risk, but these are not explicitly identified.
		IVS-13.2 Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes			Preventative, detective and corrective defence-in-depth techniques and technical measures are in place to monitor network traffic, to detect and prevent network-based attacks associated with anomalous traffic patterns, suppressing a wide range of threats, including MAC spoofing, ARP poisoning and DDoS.

Interoperability & Portability: IPY-01 to IPY-05

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IPY-01 APIs	*The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.*	IPY-01.1 Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?		No		Secure Cloud integrates Commercial-Off-The-Shelf (COTS) products to enable interoperability between the components in a heterogeneous environment. Secure Cloud supports the use of published APIs for the COTS products specified in its offerings. DXC does not publish a list of all APIs used in the provided services, but where DXC has customised APIs, this information is made available to DXC customers/tenants on request.
IPY-02 Data Request	*All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).*	IPY-02.1 Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Yes			Secure Cloud can make available structured and un-structured data to customers/tenants in an industry standard format, such as .doc, .xls, .pdf, logs, and flat files, in accordance with pre-agreed contractual and service provisions. Tenants retain control of their own data.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IPY-03 Policy & Legal	*Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.*	IPY-03.1 Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Yes			Secure Cloud provides a set of standardised IaaS, PaaS and SaaS offerings using COTS products. Where customers/tenants require interoperability between their applications and Secure Cloud services, they are responsible for ensuring their applications use APIs compatible with the products used in the Secure Cloud services. All communications and data exchanges between applications in tenant Secure Cloud compartments and external systems must be mediated through Secure Cloud secure gateways.
		IPY-03.2 If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		No		The Secure Cloud standard offering does not enable customers/tenants to download virtual machine images for porting to a new service provider; this requires a non-standard service request from the customer/tenant, and is subject to a service agreement, depending on the customer's/tenant's requirements and migration path.
		IPY-03.3 Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Yes			Policies and processes are available for governing the migration of application data to and from Secure Cloud services.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IPY-04 Standardized Network Protocols	*The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.*	IPY-04.1 Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes			Secure Cloud uses standardised network and application protocols, with appropriate encryption and authentication between tenant end-point devices and the target systems in the tenant's compartments. Secure Cloud has a formal process for importing and exporting data into and out of the Secure Cloud environment required for service management purposes.
		IPY-04.2 Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes			The Secure Cloud service descriptions on the UK Government's Digital Marketplace provide general information on the use of some of the network protocols. More information is available on request, during the initial meetings with a prospective tenant, and subsequently after contractual and service agreement, during the transition and transformation phases of the process for onboarding a tenant onto a Secure Cloud service.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
IPY-05 Virtualization	*The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.*	IPY-05.1 Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Yes			Secure Cloud supports industry standard virtualisation platforms based on the Open Virtual Machine Format (OVF).
		IPY-05.2 If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		No		Secure Cloud makes virtual machine images available for provisioning only through the customer portal and these cannot be downloaded or exported.
		IPY-05.3 Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	Yes			Secure Cloud does not make changes to the hypervisors in the shared multi-tenanted environment, and the configuration is fully documented. A customer requiring a dedicated, customised hypervisor, can request custom changes to be made via a non-standard service request, but these will only be approved if suitable, and any changes would be fully documented through this process.

Mobile Security: MOS-01 to MOS-20

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-01 Anti-Malware	*Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.*	MOS-01.1 Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	Yes			Anti-malware training specific to mobile devices is included as part of DXC's information security awareness training.
MOS-02 Application Stores	*A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.*	MOS-02.1 Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	Yes			DXC policies require the use of a company-approved application store for installation of corporate applications.
MOS-03 Approved Applications	*The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.*	MOS-03.1 Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	Yes			For processing company data, DXC mobile policies, standards, and implementation procedures require the use of a pre-identified company-approved application store for installing approved applications which are secured by a policy enforcement capability on the registered device.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-04 Approved Software for BYOD	*The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.*	MOS-04.1 Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?		No		DXC's BYOD policy does not mandate approved application stores, applications, application extensions and plugins, but requires an approved mobile device management solution to be used for BYOD access to DXC resources, and this controls the company-approved applications, extensions and plugins to be used for accessing and processing company data.
MOS-05 Awareness and Training	*The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.*	MOS-05.1 Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	Yes			DXC mobile device policies and standards for use of mobile devices to access DXC resources are published on the Intranet, referenced in security awareness and communicated to staff.
MOS-06 Cloud Based Services	*All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.*	MOS-06.1 Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	Yes			DXC's policies specify the approved cloud-based service that may be used for the storage of company business data, and any information that has a Government Security Classification of OFFICIAL is not stored in any cloud-based service.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-07 Compatibility	*The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.*	MOS-07.1 Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	Yes			DXC mobile device policies and standards require the most current version of the mobile operating system (OS) to be installed on the registered device that is compatible with the mobile device management (MDM) software installed on the device. DXC IT can monitor the OS and MDM application versions on the registered device and address any application compatibility issues.
MOS-08 Device Eligibility	*The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.*	MOS-08.1 Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	Yes			DXC's policies and standards for mobile devices, including the BYOD policy define the device and eligibility requirements for BYOD usage for DXC staff, and they do not permit DXC staff to use mobile devices (phones and tablets) for administration of Secure Cloud systems, and such access is not technically enabled.
MOS-09 Device Inventory	*An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.*	MOS-09.1 Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	Yes			An inventory of registered mobile devices used to store company data is maintained by DXC, with relevant status information, required to ensure compliance with the mobile device policies and standards.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-10 Device Management	*A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.*	MOS-10.1 Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	Yes			DXC has a centralised mobile device management solution configured to company policies and standards, which is deployed to all registered mobile devices processing company data. .
MOS-11 Encryption	*The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.*	MOS-11.1 Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	Yes			DXC policies and standards for mobile devices require the use of encryption for registered devices in order to protect company data, and this is enforced through technology controls during the device registration process.
MOS-12 Jailbreaking and Rooting	*The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).*	MOS-12.1 Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Yes			DXC mobile device policies and standards prohibit the circumvention of built-in security controls, including jailbreaking or rooting, for registered devices which can be used to access company data.
		MOS-12.2 Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Yes			DXC implements detective and preventative controls on registered mobile devices used to access company data, which prohibit the circumvention of built-in security controls.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-13 Legal	*The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.*	MOS-13.1 Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	Yes			DXC's BYOD policy requires participants to acknowledge that they have no expectations for privacy of data on the registered mobile device, and to give consent to DXC to monitor, hold, intercept or review data on the device and to comply with DXC legal department, as required.
		MOS-13.2 Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			N/A	Loss of non-company data on a DXC participant's BYOD mobile device has no bearing on the performance of Secure Cloud services.
MOS-14 Lockout Screen	*BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.*	MOS-14.1 Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Yes			DXC policies and standards require registered mobile devices used to access company data to be configured with automatic lockout screens, and this is enforced during the device registration process.
MOS-15 Operating Systems	*Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.*	MOS-15.1 Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	Yes			Changes to DXC IT software or patch levels on registered mobile devices are in scope of the DXC IT and fall under the DXC IT change management process.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-16 Jailbreaking and Rooting	*Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.*	MOS-16.1 Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	Yes			DXC has policies and standards on passwords and authentication requirements which apply to registered mobile devices used to access company data.
		MOS-16.2 Are your password policies enforced through technical controls (i.e. MDM)?	Yes			DXC policies and standards on passwords and authentication requirements which apply to registered mobile devices used to access company data, are enforced through technical controls.
		MOS-16.3 Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Yes			DXC policies and standards prohibit the changing of authentication requirements such as password/PIN length rules, and this is strictly enforced during the device registration process.
MOS-17 Policy	*The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).*	MOS-17.1 Do you have a policy that requires BYOD users to perform backups of specified corporate data?			N/A	DXC company data accessible from a registered mobile device resides on a corporate IT system and is backed up by DXC IT in accordance with corporate IT policies and procedures.
		MOS-17.2 Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?		No		DXC does not have a policy prohibiting the usage of unapproved application stores for BYOD users, but all DXC registered mobile devices are configured to use applications from a pre-approved company portal, for securely accessing company data.
		MOS-17.3 Do you have a policy that requires BYOD users to use anti-malware software (where supported)?		No		DXC does not have a policy for BYOD users to use anti-malware software, but DXC registered mobile devices are configured to allow remote monitoring and detection of malicious applications; company data securely accessible from the registered mobile device is hosted on corporate IT systems which have active malware protection in accordance with DXC's policies and standards.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-18 Remote Wipe	*All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.*	MOS-18.1 Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	Yes			DXC registered mobile devices (company-owned or BYOD) are configured to allow a remote wipe of company data to be performed on the device by the DXC IT, if the device is lost.
		MOS-18.2 Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Yes			
MOS-19 Security Patches	*Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.*	MOS-19.1 Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Yes			DXC mobile device policies and standards require the most current version of the mobile operating system (OS) to be installed on the registered device that is compatible with the mobile device management (MDM) software installed on the device. DXC IT can monitor the OS and MDM application versions on the registered device, and the device is configured to periodically download MDM policy updates or application security patches.
		MOS-19.2 Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
MOS-20 Users	*The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.*	MOS-20.1 Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			N/A	DXC registered mobile devices are configured to allow only approved corporate applications to access company data, and these applications transparently access the relevant systems and servers. The DXC corporate IT environment is physically segregated from the DXC Secure Cloud environment, and DXC's policy does not permit DXC staff to use mobile devices (phones and tablets) for administration of Secure Cloud systems and servers, and such access is not technically enabled.
		MOS-20.2 Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	Yes			DXC's policy does not permit DXC staff to use mobile devices (phones and tablets) for administration of Secure Cloud systems, and such access is not technically enabled.

Security Incident Management, E-Discovery, & Cloud Forensics: SEF-01 to SEF-05

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
SEF-01 Contact / Authority Maintenance	*Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.*	SEF-01.1 Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes			DXC maintains liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
SEF-02 Incident Management	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.*	SEF-02.1 Do you have a documented security incident response plan?	Yes			Secure Cloud has a documented security incident response plan.
		SEF-02.2 Do you integrate customized tenant requirements into your security incident response plans?	Yes			Secure Cloud can incorporate customised tenant requirements into its security incident response plan, subject to contractual and service agreements.
		SEF-02.3 Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Yes			Secure Cloud publishes a roles and responsibilities document, specifying its responsibilities and those of its customers in the event of a security incident.
		SEF-02.4 Have you tested your security incident response plans in the last year?		No		The Secure Cloud security incident management plan has not been formally tested in the last year. However, security incidents are reviewed by management and communicated to customers and tenants, lessons are identified, and corrective and preventative actions taken.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
SEF-03 Incident Reporting	*Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.*	SEF-03.1 Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Yes			Awareness and staff responsibilities for incident reporting is included in the DXC Code of Business Conduct, corporate security awareness and security training directed towards DXC staff supporting UK government and supporting organisations and contracts. Contracts with suppliers and business partners include the requirements for reporting security incidents.
		SEF-03.2 Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	Yes			DXC security incident policies and procedures describe the communication channels for reporting security incidents, and the required timeframes to ensure compliance with legal, statutory, regulatory and contractual requirements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
SEF-04 Incident Response Legal Preparation	*Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.*	SEF-04.1 Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes			DXC has forensic readiness procedures that follow the guidance of the National Cyber Security Centre (NCSC) to support the gathering and presentation of evidence that will be legally admissible, and to support potential legal action, in the event a security incident.
		SEF-04.2 Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes			A specialist digital investigation team is available to support a forensic investigation.
		SEF-04.3 Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes			The Secure Cloud architecture segregates the data owned by different tenants. Each tenant is responsible for, and has full control of only their own data, including the ability to enforce a legal hold on that data. If a tenant requires assistance from DXC to perform a legal hold on the tenant's specified data, a non-standard service request should be submitted to Secure Cloud, which is subject to approval by the DXC legal team and the tenant's organisation before execution.
		SEF-04.4 Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes			Tenant data segregation is enforced in the Secure Cloud architecture and the DXC legal team would be involved when responding to a witness summons.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
SEF-05 Incident Response Metrics	*Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.*	SEF-05.1 Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Yes			Secure Cloud uses tooling to detect and report security incidents, which are categorised, logged and assigned for investigation. Security events and incidents are periodically reported at a high-level to customers / tenants, by type and volume. Costs of security incidents are not explicitly calculated unless required because of a material impact to a service level or key performance indicator; in this case, the cost may be estimated as part of the wider incident investigation and reporting.
		SEF-05.2 Will you share statistical information for security incident data with your tenants upon request?	Yes			Information relating to a security incident that impacts a tenant will be shared with the tenant as part of the Secure Cloud incident management process. Metrics relating to security events and incidents are presented at the Secure Cloud Customer Security Working Group meetings.

Supply Chain Management, Transparency, and Accountability: STA-01 to STA-09

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-01 Data Quality and Integrity	*Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.*	STA-01.1 Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Yes			Services provided at the DXC Secure Cloud locations comply with DXC quality policies and standards, are certified to ISO 9001 and in scope of external certification audits. Supply chain partners are required to work in adherence of DXC quality requirements and standards.
		STA-01.2 Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Yes			Secure Cloud controls are designed and implemented to address risks to data through a layered approach, including separation of duties, role-based access and management of privileges for all personnel within the supply chain, working at DXC Secure Cloud locations. All internal and external supply-chain partners working at Secure Cloud locations are required to adhere to DXC quality and security policies, standards and procedures for the systems and services in scope, and where external suppliers are used, they are required, through contractual provisions, to comply with DXC security requirements.
STA-02 Incident Reporting	*The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).*	STA-02.1 Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes			Metrics relating to security events and incidents are presented periodically to customers/tenants at the Secure Cloud Customer Security Working Group meetings.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-03 Network / Infrastructure Services	*Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.*	STA-03.1 Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes			Secure Cloud service levels and key performance indicators, including capacity and use data of relevant IT components across the cloud environment, are agreed with customers/tenants, measured and service level reports are created.
		STA-03.2 Do you provide tenants with capacity planning and use reports?	Yes			Secure Cloud IT service management policies, procedures and tools are based on the ITIL framework and provide service level reporting, including the key capacity elements. Where Secure Cloud is requested to customise the capacity reporting, as per customer/tenant requirements, these would form a part of the contract or service schedules and be reported accordingly.
STA-04 Provider Internal Assessments	*The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.*	STA-04.1 Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes			Internal assessments of conformance and effectiveness of Secure Cloud services against DXC policies, procedures and supporting measures and metrics are conducted annually.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-05 Third Party Agreements	*Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:* • *Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)*	STA-05.1 Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Yes			DXC applies a risk-based due diligence evaluation of a prospective third-party provider, and, if satisfactory, DXC will negotiate a contractual and service agreement. As DXC managed data within the Secure Cloud environment is hosted in the UK, the agreements consider the applicable (UK) legal requirements that must be met by the provider.
		STA-05.2 Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	Yes			DXC policy requires legal or statutory requirements to be addressed in the contract and service agreements, following selection of a third-party service provider. These are monitored by DXC and also in scope of internal and external audits.
		STA-05.3 Does legal counsel review all third-party agreements?	Yes			All third-party agreements are reviewed by the DXC legal team, which is responsible for final approval of the contract template terms and conditions.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-05 Third Party Agreements	• *Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships* • *Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts*	STA-05.4 Do third-party agreements include provision for the security and protection of information and assets?	Yes			DXC ensures that information security requirements are included in third party agreements.
		STA-05.5 Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes			Secure Cloud services offer customers various options for data backup and recovery services: a customer/tenant chooses a service that satisfies its business and security requirements. In the event of a data loss, Secure Cloud can recover data for a customer/tenant in accordance with the agreed contractual and service agreement.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-05 Third Party Agreements	• *Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)* • *Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed*	STA-05.6 Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes			The Secure Cloud infrastructure and tenants' data is hosted in the United Kingdom (UK) and Secure Cloud services are provided by cleared staff based in the UK.
		STA-05.7 Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes			
		STA-05.8 Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes			
		STA-05.9 Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	Yes			Data routing and resource instantiation occurs from within the tenant's compartment in the Secure Cloud infrastructure. Data exchanges from within the tenant's compartment to external systems are agreed as part of the service specification and design and/or through the change management process. The source location from where a tenant's staff may access data via the tenant's compartment, through use of an approved end-user device, is controlled by the tenant.
		STA-05.10 Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes			Secure Cloud monitors security events and has a process in place for security incident management; security incidents, including privacy breaches, are reported expeditiously to DXC customers/tenants.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-05 Third Party Agreements	• *Expiration of the business relationship and treatment of customer (tenant) data impacted* • *Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence*	STA-05.11 Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Yes			Secure Cloud does not, in general, use inspection technology which would allow Secure Cloud support staff access to the personal data of tenants. DXC tenants' data is processed by DXC as specified in contracts, for business purposes only, in order to provide the contracted Secure Cloud service. The tenant is the data controller; if access to specific metadata is a concern to a customer/tenant, Secure Cloud will work with the customer or tenant to provide assurance that the identified metadata is not collected or processed.
		STA-05.12 Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?			N/A	Secure Cloud does not engage sub-processors to process Secure Cloud data.
STA-06 Supply Chain Governance Reviews	*Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.*	STA-06.1 Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes			The risk management and governance processes of partners of Secure Cloud, is reviewed as part of the annual risk management process. DXC is a Defence Cyber Protection Partnership (DCPP) executive group member, seeking Cyber Essentials Scheme (CES) certification from its supply chain, and undertakes annual supply chain assurance reviews.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-07 Supply Chain Metrics	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.*	STA-07.1 Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Yes			DXC has contracts and service agreements in place with tenants. Secure Cloud has specified Service Level Agreements (SLAs) for its services and these are monitored, measured and reported. Review of contracts, service schedules and service levels between Secure Cloud and customers/tenants are included in DXC's governance and management review practices.
		STA-07.2 Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Yes			DXC has processes in place to manage the supply chain and address non-conformances of provisions.
		STA-07.3 Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes			Secure Cloud has a simple supply chain model, and the risks of service-level conflicts as a result of multiple supplier relationships is low.
		STA-07.4 Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes			Secure Cloud provides reports of service level performance to enable tenants to review compliance with contractual and service agreements.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-07 Supply Chain Metrics	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.*	STA-07.5 Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes			Secure Cloud includes security metrics in its ITIL standards-based SLA reporting to DXC customers.
		STA-07.6 Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes			Secure Cloud provides customers with monthly reports of service level performance.
		STA-07.7 Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes			Secure Cloud provides specified cloud services, with defined SLA key performance indicators for which it is accountable. Service management processes are in place to manage any shortfalls or inconsistencies.
		STA-07.8 Do you review all service level agreements at least annually?	Yes			Secure Cloud reviews service level agreements at least annually.
STA-08 Third Party Assessment	*Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.*	STA-08.1 Do you assure reasonable information security across your information supply chain by performing an annual review?	Yes			ISO 27001, ISO27017 and CSA CCM internal or external audits of service suppliers are conducted annually at certified locations such as data centres and delivery teams at Secure Cloud support sites. Third parties providing sub-contracted security services are included in both internal and external audits at certified locations. The Secure Cloud risk assessment process considers risks relating to the provision of services by third-party providers.
		STA-08.2 Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes			

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
STA-09 Third party Audits	*Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.*	STA-09.1 Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?		No		DXC third parties are contractually bound by the relevant security requirements in DXC's policies and procedures. The services provided are monitored through meetings with DXC and third-party representatives. These are audited periodically, not necessarily annually, as part of the internal and external audit regime. Many of the third parties that provide services to DXC Secure Cloud are COTS product providers, and they are managed through support and maintenance contracts under the standard security conditions, including non-disclosure and confidentiality requirements. The third parties providing services with a potential security impact to Secure Cloud and tenant information assets, work within the DXC environment; they are required to adhere to DXC security policies and standards and are in scope of internal and external audits.
		STA-09.2 Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?			N/A	Secure Cloud does not use external third-party providers to conduct vulnerability scans or penetration tests on its applications and networks; it obtains assurance through the extensive annual IT Health Check testing conducted by CHECK-qualified staff, independent to Secure Cloud, which is required to maintain PSN compliance, and which is reported to the PSN assessor. The review of the test process and reports by the PSN assessor has successfully demonstrated its independence from Secure Cloud.

Threat and Vulnerability Management: TVM-01 to TVM-03

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
TVM-01 Antivirus / Malicious Software	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	TVM-01.1 Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?		No		Malware protection software and intrusion protection systems are installed on most, but not all, Secure Cloud IT infrastructure network and system components. This is done in accordance with the risk profiles of the IT components, and the activities are carried out in line with National Cyber Security Centre (NCSC) guidance.
		TVM-01.2 Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	Yes			Secure Cloud threat detection and prevention systems are maintained and subject to a policy that ensures malware recognition signatures are updated in a timely fashion, and the systems respond defensively when anomalous behaviour is detected. These are included in 24 X 7 protective monitoring, in line with National Cyber Security Centre (NCSC) guidance.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
TVM-02 Vulnerability / Patch Management	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	TVM-02.1 Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			Network layer vulnerability scans of the DXC managed components of the cloud infrastructure are regularly performed using specialised tools, by CHECK-qualified staff, and in line with NCSC guidance.
		TVM-02.2 Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			Application layer vulnerability scans of the DXC managed components of the cloud infrastructure are regularly performed using specialised tools, by CHECK-qualified staff, and in line with NCSC guidance.
		TVM-02.3 Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			Operating system layer vulnerability scans of the DXC managed components of the cloud infrastructure are regularly performed using specialised tools, by CHECK-qualified staff, and in line with NCSC guidance.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
TVM-02 Vulnerability / Patch Management	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	TVM-02.4 Will you make the results of vulnerability scans available to tenants at their request?	Yes			Secure Cloud has regular Customer Security Working Group meetings during which the shared cloud infrastructure high-level vulnerability metrics are presented.
		TVM-02.5 Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Yes			DXC managed IT components of Secure Cloud are subject to technically supported vulnerability and patch management processes, implemented through change management.
		TVM-02.6 Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	Yes			Secure Cloud provides information on roles and responsibilities to customers/tenants, including a description of shared responsibility for implementation of controls. Policies, procedures or guidance is shared where required. Secure Cloud informs customers/tenants, as required, in the case of identified weaknesses or security incidents that may have or have had a material impact to customer/tenant data or to the services provided.

CCM Control ID	Control specification	Consensus Assessment Questions	Consensus Assessment Answers			DXC Secure Cloud Response
			Yes	No	N/A	
TVM-03 Mobile Code	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	TVM-03.1 Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes			Mobile code such as Active-X, Java-script and Java are employed within the Secure Cloud environment, as some COTS applications use browser-based GUIs employing these technologies. Mobile code used in the COTS applications is subject to testing prior to being used and is in scope of a programme of vulnerability scans and IT Health Checks.
		TVM-03.2 Is all unauthorized mobile code prevented from executing?	Yes			Unauthorised code from untrusted networks is not imported or used in the Secure Cloud environment; layered controls protecting the core infrastructure prevents such imports, and all data imported into the DXC-managed Secure Cloud environment must be authorised through an established process. The use of mobile code is constrained by the applications and by the lockdown of an administrator's desktop, including anti-malware software that prevents low-level access to execute unauthorised code.

Glossary of terms

Term	Definition	Description
AAC	Audit, Assurance & Compliance	A control domain in the Cloud Controls Matrix with 3 controls; the control objective is to ensure that an adequate controls framework is established to address technical, legal, regulatory and compliance risks within the cloud environment and ongoing governance is performed through regular audit and compliance activities to provide cloud customers assurance that their data is adequately protected and service levels are being met.
AES	Advanced Encryption Standard	A specification for the encryption of electronic data using a symmetric key algorithm.
AICPA	American Institute of Certified Public Accountants	The national professional organization of Certified Public Accountants in the United States, with more than 418,000 members in 143 countries in business, industry and the public sector.
AIS	Application & Interface Security	A control domain in the Cloud Controls Matrix with 4 controls; the control objective is to ensure that software user interfaces and application programming interfaces used to manage or interact with cloud services are designed to protect against both accidental and malicious attempts to circumvent policy.
API	Application Programming Interface	A set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service.
ARP	Address Resolution Protocol	A communication protocol in the link layer of the Internet protocol suite, used within the boundaries of a single network.
BCM	Business Continuity Management	Holistic management process that identifies threats to an organisation, impacts to business operations of those threats, if realised, and which provides a framework for building organisational resilience to protect the interests of key stakeholders, reputation and brand.
BCR	Business Continuity Management & Operational Resilience	A control domain in the Cloud Controls Matrix with 11 controls; the control objective is to implement business and operational resilience by implementing business continuity and IT service continuity good practices to guard against data loss and degradation or loss of services as a result of natural or man-made disasters, malicious or accidental events.

Term	Definition	Description
BIA	Business Impact Analysis	The process of analysing business activities and the effect a business disruption might have on them.
BYOD	Bring Your Own Device	The practice of allowing employees to use their own phones, tablets or computers for work purposes.
CAPS	Certified Assisted Products	A scheme to evaluate a product by the NCSC and its partners; evaluated products may be issued with a certificate and/or approval letter detailing the level of cryptographic protection they offer.
CC EAL 4+	Common Criteria Evaluation Assurance Level 4+	A framework in which computer system users can specify their security functional and assurance requirements for a specific product for evaluation, and a numerical rating describing the depth and rigour of an evaluation.
CCC	Change Control & Configuration Management	A control domain in the Cloud Controls Matrix with 5 controls; the control objective is to manage risks relating to all changes to the cloud environment to maintain the integrity and availability of the environment and ensure service levels are maintained.
CES	Cyber Essentials Scheme	A Government-backed, industry-supported scheme to help organisations protect themselves against common online threats, with the opportunity to be certified to demonstrate assurance to a specified level of cybersecurity.
CHECK	-	CHECK is the scheme under which NCSC approved companies can conduct authorised penetration tests of public sector and Critical National Infrastructure systems and networks.
CIO	Chief Information Officer	Responsible for several roles within the (DXC) organisation, including business enablement and IT services, enterprise architecture, IT enablement and information assurance services.
COBIT	Control Objectives for Information and Related Technologies	A good-practice framework which provides an implementable set of controls for information technology and organizes them around a logical framework of IT-related processes and enablers.

Term	Definition	Description
DSI	Data Security & Information Lifecycle Management	A control domain in the Cloud Controls Matrix with 7 controls; the control objective is to ensure that information assets are assigned ownership, classified and protected in storage and in transit throughout their lifecycle.
EKM	Encryption & Key Management	A control domain in the Cloud Controls Matrix with 4 controls; the control objective is to ensure that appropriate controls are in place for the encryption of data and management of the keys used to encrypt data, to safeguard against unauthorised disclosure, modification or loss of information in storage or in transit.
ESM	Enterprise Service Management	A means to provide service management across the enterprise and across IT Service management processes.
FIPS 140-2	Federal Information Processing Standard 140-2	A United States government computer security standard used to approve cryptographic modules.
G-Cloud	Government Cloud	An initiative targeted at easing procurement by public-sector bodies of information technology services that use cloud computing.
GDPR	Global Data Protection Regulation	A regulation in law on data protection and privacy, applicable worldwide, that came into force in May 2018, and applicable to the processing of personal data of individuals ("data subjects") within the European Union and the European Economic Area.
GRM	Governance & Risk Management	A control domain in the Cloud Controls Matrix with 11 controls; the control objective is to ensure management commitment to information security by means of a comprehensive information security programme, with security policies, procedures and controls aligned to a risk management framework, and an effective governance structure.
HMG	Her Majesty's Government	Formal term referring to the UK Government.

Term	Definition	Description
CSA CCM	Cloud Security Alliance Cloud Controls Matrix	A security controls framework to guide cloud vendors and assist cloud customers in assessing the overall security risk of using a cloud provider.
CSA STAR	Cloud Security Alliance Security, Trust & Assurance Registry	A registry of those organisations that have provided a defined level of assurance for implementation of the controls in the CSA CCM.
CCTV	Closed Circuit Television	A system of remote monitoring using a network of cameras.
CoCo	Code of Connection	A mandatory set of requirements that must be demonstrated for connecting to networks (usually) used by government bodies.
COTS	Commercial Off The Shelf	COTS products are packaged IT solutions that may be adapted and integrated to satisfy the needs of a purchasing organisation.
CPA	Commercial Product Assurance	The Commercial Product Assurance scheme was set up by NCSC to help companies demonstrate that the security functions of their products met defined NCSC standards (known as Security Characteristics)
CPNI	Centre for the Protection of National Infrastructure	Government authority for providing protective security advice to organisations that are a part of the UK national infrastructure.
DCPP	Defence Cyber Protection Partnership	A joint Ministry of Defence and industry initiative to improve the protection of the defence supply chain from the cyber threat.
DCS	Data Centre Security	A control domain in the Cloud Controls Matrix with 9 controls; the control objective is to ensure that asset management and physical security controls are in place to safeguard cloud hardware assets containing provider and customer information, throughout their lifecycle.
DDoS	Distributed Denial of Service	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by flooding the target with superfluous requests originating from multiple sources and causing a disruption of services to legitimate users.

Term	Definition	Description
HRS	Human Resource Security	A control domain in the Cloud Controls Matrix with 11 controls; the control objective is to ensure that risks to information in the cloud environment as a result of human activities, whether malicious, accidental or due to error, are mitigated by security measures applied to people, throughout the employment life-cycle.
IaaS	Infrastructure as a Service	A cloud computing model which allows for automated deployment of servers, processing power, storage, and networking, giving IaaS clients more (remote) control over their infrastructure.
IAM	Identity & Access Management	A control domain in the Cloud Controls Matrix with 13 controls; the control objective is to ensure that access to information in the cloud environment is protected by implementing access control principles, policies, procedures and technical measures to guard against a range of threats from different threat actors.
ICT	Information and Communications Technology	This is the infrastructure and components that enable modern computing.
IEC	International Electrotechnical Commission	The International Electrotechnical Commission is the international standards and conformity assessment body for all fields of electrotechnology.
IPY	Interoperability & Portability	A control domain in the Cloud Controls Matrix with 5 controls; the control objective is to minimize service disruptions in the face of a change to cloud provider relationship in the face of a change in a cloud vendor relationship or expansion of services.
ISMS	Information Security Management System	A set of policies, procedures and processes for systematically managing an organisation's information assets by reducing risk and ensuring business continuity.
ISO	International Standards Organisation	An international standards-setting body that promotes standards world-wide.
ISO/IEC 27001:2013	International Standards Organisation /International Electrotechnical Commission standard 27001:2013	Information technology - Security techniques - Information security management systems – Requirements.
ISO/IEC 27002:2013	International Standards Organisation /International Electrotechnical Commission standard 27002:2013	Information technology – Security Techniques - Code of practice for information security controls.

Term	Definition	Description
ISO/IEC 27017:2015	International Standards Organisation /International Electrotechnical Commission standard 27017:2015	Information technology – Security Techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
ITHC	Information Technology Health Check	An IT security assessment of IT systems required and conducted as part of an accreditation process, usually for IT systems that need to meet Government security requirements.
ISAE 3402	International Standard on Assurance Engagements (ISAE) No. 3402	A global assurance standard for reporting on controls at a service organisation.
ITIL	Information Technology Infrastructure Library	A set of practices for IT Service Management that focuses aligning IT services with the needs of the business.
IVS	Infrastructure & Virtualisation Security	A control domain within the Cloud Controls Matrix with 13 controls; the control objective is to ensure that suitable technical measures are implemented on cloud platforms and networks to ensure effective segregation of different customers (tenants) and their data, and to reduce the risk of service disruptions and data breaches.
MAC	Media Access Control	A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment.
MDM	Mobile Device Management	Software for managing the security of mobile devices such as phones.
MOS	Mobile Security	A control domain in the Cloud Controls Matrix with 20 controls; the control objective is to address the risks of accessing cloud data through the expanding use of mobile device technology.
NCSC	National Cyber Security Centre	A UK Government organisation that provides advice to the public and private sector on how to protect information and services from cyber threats.

Term	Definition	Description
NIST SP 800-131A	National Institute of Standards and Technology Special Publication 800-131A	Physical science laboratories, part of the US Department of Commerce, promotes US innovation and industrial competitiveness and guidance such as 800-131A for cryptographic key management.
OSA	Official Secrets Act	An act of parliament whose purpose is to provide for the protection of state secrets and official information, mainly related to national security.
OVF	Open Virtualisation Format	An open standard for packaging and distributing virtual appliances or software to be run on virtual machines.
OWASP	Open Web Application Security Project	A worldwide not-for-profit charitable organization focused on improving the security of software.
PaaS	Platform as a Service	A cloud computing model that provides a computing platform for cloud customers to develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure.
PKI	Public Key Infrastructure	A set of processes and tools that binds a public key with its respective organisational identity, established through a process of registration and issuance of certificates at and by a certificate authority.
PSN	Public Services Network	The UK Government's high-performance network, which helps public sector organisations and their partners and suppliers to work together.
RPO	Recovery Point Objective	The maximum targeted period in which data might be lost from an IT service after a business disruption.
RTO	Recovery Time Objective	The targeted duration of time and a service level within which a business process must be restored after a business disruption.
SAL	Security Aspects Letter	A document detailing special contractual conditions, that defines the security requirements for protecting Government classified information.
SDLC	System Development Life Cycle	A process for planning, creating, testing and deploying an information system.

Term	Definition	Description
SEF	Security Incident Management, E-Discovery & Cloud Forensics	A control domain within the Cloud Controls Matrix with 5 controls; the control objective is to ensure processes and procedures are in place to identify, report and manage security incidents, including a forensics capability, in a multi-tenant cloud environment.
SIEM	Security Information and Event Management	An IT solution, used in security operations for monitoring and managing real-time security events and alerts generated by IT systems.
SIRO	Senior Information Risk Owner	The person, who is part of an organisation's internal governance framework, and ensures that information risk is managed effectively, and acts as advocate for information risk on the organisation's Board.
SNMP	Simple Network Management Protocol	An Internet Standard protocol for collecting and organizing information about managed devices on networks and for modifying that information to change device behaviour.
SOC	Security Operations Centre	A facility where information systems are monitored for security information and events, assessed for security threats and defended against attack.
SLA	Service Level Agreement	An SLA defines the level of service you expect from a vendor, specifying the metrics by which service is measured, as well as remedies or penalties should the agreed service levels not be achieved.
SSAE 18 SOC 2	Statement on Standards for Attestation Engagements (no. 18) Service Organisation Control 2	An auditing standard for service organisations. Overseen by AICPA, SSAE 18 governs the way organisations report on their various compliance controls. The SOC 2 report considers the design and effectiveness of a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.
SSO	Single Sign On	A property of access control of multiple related but independent systems, where a user logs in to one system and is then signed on to other applications automatically.
SaaS	Software as a Service	A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted and managed, typically in a cloud environment.

Term	Definition	Description
STA	Supply Chain Management, Transparency and Accountability	A control domain in the Cloud Controls Matrix with 9 controls; the control objective is to address the need for ensuring due care is taken in the cloud providers supply chain, as well as the risks associated with governing data within the cloud.
SyOPs	Security Operating Procedure	Procedures that define the security rules and behaviours required by people when accessing information systems.
TLS	Transport Layer Security	A protocol used to provide secure communications, usually over untrusted networks.
TVM	Threat & Vulnerability Management	A control domain in the Cloud Controls Matrix with 3 controls; the control objective is to manage the threats of malware, malicious code and technical vulnerabilities impacting cloud platforms, applications and data by implementing appropriate preventative, detective and responsive controls, including technical and procedural security measures.
UAD	User Access Device	A desktop or portable computer used to access an IT network.
UPS	Uninterruptible Power Supply	Electrical apparatus that provides emergency power when the mains power fails.
UKAS	United Kingdom Accreditation Service	The sole national accreditation body recognised by the British government to assess the competence of organisations that provide certification, testing, inspection and calibration services
VESDA	Very Early Smoke Detection Apparatus	Advanced smoke detection system used as early warning of fire detection in areas with critical IT infrastructure and systems, such as data centres.
VM	Virtual Machine	An emulation of a computer system which provides the functionality of a physical computer.
VPC	Virtual Private Cloud	An on-demand configurable pool of shared computing resources allocated within a cloud environment, providing a certain level of isolation between the different organizations using the resources.

About DXC Technology

DXC Technology helps our customers across the entire Enterprise Technology Stack with differentiated industry solutions. We modernize IT, optimize data architectures, and make everything secure, scalable and orchestrated across public, private and hybrid clouds.
DXC invests in three key drivers of growth: People, Customers and Operational Execution.
The company's global scale, talent and innovation platforms serve 6,000 private and public-sector customers in 70 countries.

For more information, visit **www.dxc.technology** and explore DXC perspectives at **Our Perspectives (dxc.com)**

© 2021 DXC Technology Company. All rights reserved.

Registered UK office

17 Royal Pavilion,
Wellesley Road,
Aldershot, Hampshire,
GU11 1P