CAIQv3.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

UKCloud IntroductionThe Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) is a comprehensive framework of questions and responses which potential UK public sector customers can make reference to to assessand understand the information security, data governance and related privacy elements of consuming UKCloud Ltd services. This response is one element of UKCloud's available information security related documentation,which also includes G-Cloud "Evidence Packs", RMADS (Risk Management and Accreditation Documentation Set), and other accreditation and certification documents (e.g. ISO27001, ISO27017, ISO27018, Cyber Essentials, Cyber Essentials Plus, PSN etc.)

This response has been compiled and is provided for informational purposes only, and individual responses may change without notice. Potential UK public sector customers are encouraged to engage with UKCloud Ltd to seek clarity or confirm the ongoing accuracy of individual responses. Please note that this document does not confer any legal rights or intellectual property in any UKCloud Ltd service, although you may copy and use this document for your own internal purposes. The supply of UKCloud Ltd services are subject to the agreement of a separate, legally binding agreement. For further information on UKCloud accreditations and certifications, visit https://ukcloud.com/governance/, or contact the UKCloud Compliance Team.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	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.	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)?	X			UKCloud's Development Team fully adhere to the Open Web Application Security Project (OWASP) Standards to ensure high levels of security within our Systems/Software Development Lifecycle (SDLC). All production software deployments are done in accordance with the UKCloud Software Engineering Development Process and Change Management Process. UKCloud's Development Teams follows Test Driven Development (TDD) practices where applicable, with all code being peer reviewed prior to being committed to a source code repository where each change is linked to a requirement. Software is then packaged via a continuous integration process after which it is subject to manual or automated regression tests in a dedicated QA environment. Final acceptance, integration and regression testing is performed in a representative test environment. All test results are recorded in UKCloud's Jira and Confluence repositories. Code reviews are managed though Bitbucket using pull requests. Where changes to production code are made on separate short lived branches. All code changes need to be approved by two different team members, which includes a subject matter expert. Once the pull request has been approved, only authorised team members are able to merge code to the master branch. Key Development team members have GIAC Certified Web Application Defender (GWEB) certifications from SANS. They use static code analysis tools like SonarQube and OWASP dependency checker to identify potential security vulnerabilities in the code. This is integrated to UKCloud's Continuous Integration builds which are executed on every commit. The results for the master branch which represents production ready code is visible to all teams. OWASP ZAP is also used regularly by the UKCloud's QA Team to test for security vulnerabilities in the Portal application. This is done in accordance with UKCloud Software Engineering Development Process which includes a reference to the Secure Software Library Policy. Where a third party is recorded as being an essential element of the service, UKCloud will always engage an existing partner to minimise supplier engagement and provide the strongest controls for information within the supply chain. All UKCloud suppliers undergo a thorough selection process, and regular due diligence and audit checks are conducted during the lifecycle of the service. For software suppliers, this includes an assessment of their approach to Systems/Software Development Lifecycle (SDLC) security. Evidence of assessment of third party security capabilities been evidenced during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications, undertaken regularly by Lloyd's Register. UKCloud customers are advised of a pending significant feature release via notifications posted within the Customer Portal. Wherever possible, feature releases are undertaken during normal office hours, to ensure that maximum benefit from development and support resources are available to support customers, if required. All release activities are protected by rollback plans to a previous version.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	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?	X			The identification of all security, contractual and regulatory requirements for customers to access and use UKCloud services are documented and communicated, and require customer contractual approval, before customers are granted access to data, assets and information systems. This activity is overseen and enforced by the UKCloud Commercial Team. UKCloud has implemented and operates a number of technical controls to ensure only authorised individuals are able to authenticate to and access the UKCloud services for which they have an identified and approved business need - including the option for customers to enable a software token based multi-factor authentication (based upon RFC 6238). UKCloud has implemented and provides Role Based Access Control (RBAC) capabilities, allowing customer system administrators to determine the level of access and privileges that their users have. UKCloud only provides one system administrator account when the initial service is commissioned: beyond that the customer organisation is fully responsible for determining, creating, managing and deleting their own user accounts and their permissions. When administering the platform, UKCloud administrative personnel utilise a combination of device certificates (Microsoft Certificate Authority based) and RSA hardware tokens (SID700/SID800).
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	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.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Application and API inputs are validated to ensure integrity. Where possible services are developed to be independent. Where it is essential to ensure data is up-to-date and correct, for example within customer billing activities, UKCloud implements regular checks and has reconciliation tools in place to resolve any identified issues. The UKCloud Software Engineering Development Process explains how such implementations are to be undertaken.
		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?	X			
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	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.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			UKCloud's Platforms have been regularly reviewed in consultation with experts from the National Cyber Security Centre, including during the initial design and implementation phases which commenced in 2012. Until 2017, UKCloud was subject to regular formal assessments by Pan Government Accreditors. Alongside the framework of policies, procedures and controls which are required to meet the requirements of UKCloud's certifications to the ISO27001, ISO27017 and ISO27018 standards, being focused on the delivery of cloud services to the UK public sector has required UKCloud to demonstrate adherence to UK Government requirements, including IS1/2 risk assessments, various "Good Practice Guides" (GPG) and the incorporation of architectural patterns, recommended configurations and technical implementation requirements. Combined together, these reference points provide a comprehensive framework for data security, ensuring that confidentiality, integrity and availability are properly maintained.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	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.	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?	X			UKCloud maintains a framework of internal audit activities (Internal Audit Schedule, updated each month), which are undertaken by qualified auditors from the Compliance Team, which assess all activities, processes and function within UKCloud. The Compliance Team also co-ordinates the six-monthly surveillance audits of UKCloud's ISO-management systems, undertaken by Lloyd's Register. UKCloud declares its audit capabilities to customers via the G-Cloud Digital Marketplace, its response to the UK Government's (NCSC) 14 Cloud Security Principles, and a supporting comprehensive "G-Cloud Evidence Pack" which provides in-depth supporting information for each of the Digital Marketplace requirements to assist its Customers. The following documentation can be shared upon request to UKCloud's Compliance Team: (i) G-Cloud Assurance Information Portfolio "Evidence Pack" (ii) "How UKCloud Implements NCSC Cloud Security Principles"
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	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.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			UKCloud provides documentation to its customers which confirms that external, third party certifications and assessments take place, and this is available upon request from the UKCloud Compliance Team. For ISO27001, this includes certificates, scopes, detailed explanations within the UKCloud's G-Cloud Assurance Information Portfolio "Evidence Pack" and visibility of the supporting Statement of Applicability (automatically generated within the InfoSaaS Assure risk management solution). UKCloud's services are subject to regular tests, both internally by Network Security Analysts and also by comprehensive ITSHC/CHECK security tests undertaken by an independent testing organisation at least once a year. This is amongst the highest and most detailed level of technical validation available to cloud providers, and ensures that infrastructure, configurations and working practices are regularly being assessed against current best practice and the latest vulnerabilities and threats. Regular penetration tests of UKCloud's infrastructure are undertaken by qualified and experienced internal personnel, and also independent testers through the NCSC CHECK Test scheme. UKCloud conducts a rolling programme of internal audits, which are undertaken by Internal Auditors within the UKCloud Compliance Team. Such audits are a mandatory element of UKCloud's certifications for ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/27017/27018 (Information Security Management). The results of internal audits are submitted for Senior Management review, are also assessed by external auditors during their periodic visits. UKCloud's internal audits are planned, scoped and delivered to assess cross-departmental activities. UKCloud is subject to regular external assessment by Lloyd's Register. Government accreditors also regularly take up their right to assess UKCloud.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			
		AAC-02.4		Do you conduct internal audits at least annually?	X			
		AAC-02.5		Do you conduct independent audits at least annually?	X			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		X		
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?		X		

Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	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.	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?	x			Within UKCloud's Business Operations function, the Compliance, Commercial and Finance Teams work closely to ensure that the specific control frameworks within their respective areas combine to provide a comprehensive set of benchmarks for all UKCloud functions. This is most easily visible through the implementation of the controls detailed within Annex A of ISO27001:2013 (as supplemented by the additional controls from ISO27017 and ISO27018). These require for UKCloud to identify all legislative, regulatory and contractual requirements, which are clearly recorded and communicated within their own repositories (e.g. Register of Applicable Legislation). All such repositories are required to be formally reviewed on at least an annual basis, although the frequency of changes ensures that such reviews are carried out on a more regular basis. The results of such reviews, or the introduction of new requirements (e.g. the introduction of the UK Data Protection Act 2018 to deliver the requirements of the EU General Data Protection Regulation (GDPR) 2016/679, triggered a significant project involving all UKCloud functions and personnel to ensure UKCloud remained fully compliant.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	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	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			UKCloud has implemented and maintains a formal business continuity, service continuity and disaster recovery framework, which consists of three core documents: - Business and Service Continuity Management Policy - Business Continuity Framework - Availability and Service Continuity Framework The policy referenced above includes details of UKCloud's Leadership Team who have overall responsibility for the direction, effectiveness and implementation of the framework. This includes the Director of Compliance & Information Assurance, who is a certified Member of the Business Continuity Institute, who maintains overall responsibility for their availability, accuracy and communication to the appropriate UKCloud Teams. Business Continuity and Availability and Service Continuity Frameworks provide the detailed recovery procedures which are to be followed in the event of invocation for whatever reason, and include agreed approaches to customer and public facing communications, as appropriate. UKCloud's customers have full control over where they host their services and data (from single-site development environments to multi-site active-active configuration), and options to implement load balancing technologies or use disaster recovery services to other external locations outside of the UKCloud platform. This will be dependent on them having suitable resilient network access, connectivity and capacity, as not all customer services are connected to the internet and may instead be connected to closed networks such as PSN, PNN, HSCN, JANET or RLI.
		BCR-01.2		Do you have more than one provider for each service you depend on?	X			
		BCR-01.3		Do you provide a disaster recovery capability?	X			
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?	X			
		BCR-01.6		Do you provide a tenant-triggered failover option?	X			
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?	X			
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	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.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Due to the resilient manner in which UKCloud delivers its services and manages its operations, many aspects of business continuity planning are routinely tested on a daily basis. This includes validating that all systems and services have fully operational resilient configurations, that UKCloud personnel can work seamlessly from different locations, and that availability is maintained with no single points of failure. On a periodic basis, scenario-based events are valuated with Ark Data Centres (UKCloud's provider of secure data centres), which provide realistic scenarios for different UKCloud Teams to engage within to ensure that services can be maintained and, if appropriate, recovered to alternate locations/systems. Details of such testing activities are strictly confidential. Regular failover tests within the UKCloud platform and between the two data centres are performed in order to ensure continuing service availability - this is part of UKCloud's routine business operations in providing its cloud services. Customers are also able to request failover tests of specific workloads or VDCs to ensure that their workload integrity is maintained in the event of an automatic failover, or request the migration of workloads to another host within the UKCloud platform. Records of such tests are retained within the appropriate ticketing repository.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	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.	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?	X			UKCloud's customers can request visibility of RMADS (Risk Management and Accreditation Documentation Sets) for each cloud service, which includes diagrams describing the diverse, encrypted transport routes which connect each of UKCloud's data centres. Records of Ark Data Centres utilities, services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) are secured, monitored, maintained - regular disclosure to UKCloud's Compliance Team takes place on a monthly basis, who use this information to ensure that appropriate security controls are being provided correctly and remain effective. If a UKCloud customer is utilising the internet as a means of connection, then their data can be transported via any country's service. However, If using a UK public sector secured network such as the Health and Social Care Network (HSCN) or the Public Services Network (PSN) then these networks may have resilience restrictions which are outside UKCloud's control.
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	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	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?	X			UKCloud maintains a full suite of technical documentation of every aspect of th design, configuration, operation, monitoring and mamagement of the technologies which underpin its cloud services provided to customers. These resources are securely located within the UKCloud Document Management System, with the technical elements housed within a secure internal Wiki instance. All document repositories are subject to encrypted daily backups.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	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.	Is physical damage anticipated and are countermeasures included in the design of physical protections?	x			UKCloud provides its cloud services from two secure data centre campuses, both owned and operated by Ark Data Centres (who additionally use the facilities for Crown Hosting). Each data centre maintains ISO27001 and ISO22301 certification, and additionally is externally validated by speficic UK government accreditors. The locations of Ark's data centre campuses have been assessed with consideration to: - the prevailing climatic conditions present in the south of England - no history of or consideration for earthquakes, volcanoes, tsunamis, mudslides or tectonic plate movements - secure ex-military campuses to which the general public has no access, significantly reducing civil unrest opportunities The physical security controls which are present on each site include: - 24x7 dedicated manned guarding, with secure internal control rooms and mobile patrols - Security fencing, vehicle blockers, full-height personnel turnstiles, perimeter detection beams - Extensive external and internal digital CCTV coverage with on-site and off-site recording - Solid construction of all walls and floor slabs. No windows in data rooms - Segregated loading and unloading areas, incorporating strategic airlocks - Triple authentication access control, incorporating ID cards, PIN validation and biometric authentication - Formalised "white list" access protocols, with robust procedures for visitor and emergency access requirements UKCloud also conducts internal audits as part of its ISO27001/17/18 certification within each of the Ark Data Centre campuses, validating that controls are in place and effective, and that the supplier's obligations are being delivered. Independent assessors from Lloyd's Register visit on at least an annual basis. UK Government accreditors also evaluate the physical security controls provided to protect UKCloud's operating environments: the last of these was undertaken by the Home Office (PASF) in April 2019.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	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.	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.)?		X		UKCloud conducts full site surveys and risk assessments of its data centres and operational facilities as part of its due diligence activities before selecting new sites. Such assessments include consideration of grographic, geological and meteorological considerations, including fire, flooding, proximity to water courses, weather extremes, activities of any neighbouring properties and proximity to airports/flight paths. Such risk assessments are conducted in accordance with the UKCloud Risk Assessment Methodology. UKCloud's core platforms and operational capabilities have been designed with no single points of failure in each platform or data centre campus by the use of redundant equipment configured as n+1 or 2n as a minimum.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	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.	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	x			UKCloud has dedicated backup technology which provides customers with restore and recovery capabilities. However, UKCloud does not allow third party companies to restore data from these backups. UKCloud has implemented a Business and Service Continuity Management Policy, Business Continuity Framework and Availability and Service Continuity Framework which direct and control business continuity arrangements and disaster recovery plans to ensure the continued availability of UKCloud's operations, platforms and cloud services. The UKCloud management domain has its configurations and data automatically backed up daily to the alternative data centre environment, offering high levels of security to the backed-up data set. This ensures that backed up data is securely stored remotely to the devices from which it originated, assisting in the continuity of service in the event of an outage at one data centre. Backed up data is subject to routine monitoring and testing to ensure that (a) the backup tasks are successfully completed as planned, and that (b) backed up data is recoverable and capable of being restored in the event of an emergency. UKCloud is responsible for ensuring the correct operation of the dedicated backup infrastructure which is used to backup data from customer environments, as applicable.
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?	x			

Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			The UKCloud management domain has its configurations and data automatically backed up daily to the alternative data centre environment, offering high levels of security to the backed-up data set. This ensures that backed up data is securely stored remotely to the devices from which it originated, assisting in the continuity of service in the event of an outage at one data centre. Backed up data is subject to routine monitoring and testing to ensure that (a) the backup tasks are successfully completed as planned, and that (b) backed up data is recoverable and capable of being restored in the event of an emergency. UKCloud is responsible for ensuring the correct operation of the dedicated backup infrastructure which is used to backup data from customer environments, as applicable. The UKCloud data centres are the physical locations where all service delivery infrastructure is located. UKCloud has two data centre campuses, and all infrastructure is mirrored within both. The two locations used by UKCloud are 100 km apart in different regions of the country. Both data centres are highly secure and resilient, and carry an extensive portfolio of security accreditations. Ark Data Centres, as the data centre provider, undertakes extensive tests on the security, connectivity, power and cooling functions of each site (as required by their own ISO22301 and ISO27001 certifications). In addition, the backup functions (for example, diesel generators, and UPS/rotary generators) are subject to periodic testing as required by their Planned Maintenance Schedule. Ark provides testing evidence to UKCloud as part of regular internal audit and security control validation sessions. Supporting evidential records of the activities mentioned above are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	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	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) ?	x			UKCloud's Service Definitions outline the SLAs, response times and other relevant options, which are also committed to within the Terms and Conditions of each cloud service. UKCloud provides 24/7 support for high priority incidents and extended support (08:00-20:00 Monday to Friday) for all other incidents. The "My Calls" function within the UKCloud Customer Portal provides access to Cloud Support Engineers who are trained to handle customer requests or queries in a timely and professional manner. Where a customer requires more interaction to talk about service provisioning, they also have access to a Service Delivery Managers (SDM) and a dedicated Senior Service Delivery Manager (Senior SDM). Each Senior SDM conducts regular service reviews with each customer, and formal service reports include analysis of UKCloud's performance against each agreed SLA. UKCloud customers can setup, manage and request assistance with their cloud services using the UKCloud Customer Portal. The Portal provides IT Service Management tools (ticketing system, knowledge centre, SLA reporting, service utilisation), reporting and self-provisioning tools, and secure access to the tools needed to manage IaaS services (for example VMware's vCloud Director for UKCloud for VMware and Red Hat's OpenStack Horizon for Cloud Native Infrastructure). It also provides visibility of SLA performance. UKCloud provides its customers with a range of information security metrics within the UKCloud Customer Portal, which includes details of security incidents, vulnerability advisories, protective monitoring alerts, change notifications and much more - this is documented in UKCloud's Support Portal - Customer Support Engagement.
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	x			
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	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	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			A comprehensive library of policies and supporting procedures is in place within the UKCloud Document Management System to ensure appropriate planning, delivery, and support of the UKCloud's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v3). The policies and procedures include defined roles and responsibilities supported by regular staff's training. Applicable documentation is regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	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.	Do you have technical capabilities to enforce tenant data retention policies?	x			UKCloud provides on-platform protection for customers to be able to use with their solutions: • snapshot protection: available for UKCloud for VMware, daily snapshot protection is available for VMs with either 14 or 28-day retention periods • journal protection: available for UKCloud for VMware, journal protection captures every change that takes place inside an application and is retained for a period of 14 days • cloud storage: available for all products, object storage is suitable for backing up data UKCloud's standard Terms and Conditions for each cloud service explain to Customers how it will respond to any lawful requests which it has received from governments or third parties. Should such a request be validated and required under English Law, UKCloud will inform and co-operate with the applicable customer/s to ensure that the request can be progressed in accordance with the required timelines. UKCloud backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Backup standards and policies, procedures and controls are documented (e.g. Backup Management Policy) and validated to ensure that they adhere to applicable regulatory, statutory, contractual or business requirements. Full resiliency and redundancy are designed and incorporated into all UKCloud services, which have no single points of failure. UKCloud backups are tested on a regular basis. Via the UKCloud Portal, Customers can select either 14 or 28-day retention periods. Customers are responsible for enforcing their own data retention policies and testing their own backups and redundancy controls. Backup management activities are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
		BCR-11.2		Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	x			
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	x			
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	x			
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	x			
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	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.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			UKCloud operates the following policies and procedures are to control the authorisation, design, implementation, operation and ongoing management of new facilities, infrastructure, systems, operations and assets within UKCloud: - Supplier Approval Process - Supplier Capability Assessment - Supplier & Partner Relationship Management Process - Product Management Process - New Product Approval Process - Change Management Policy - Change Management Process - Release Management Policy - Release Management Process These activities are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register. UKCloud makes available a framework of documentation to help customers understand the configuration, standard builds, deployment, management and operation operations of their own cloud services, including (a) service definitions, (b) service RMADS, which include roles and responsibilities, and (c) knowledge articles, white papers and educational/training activities.
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	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).	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	x			Controls are in place to ensure standards of quality are met for software development - all production software deployments are done in accordance with the UKCloud Change Management Process. UKCloud's Development Teams follows Test Driven Development (TDD) practices where applicable. All code is peer reviewed prior to being committed to a source code repository where each change is linked to a requirement. Software is then packaged via a continuous integration process after which it is subject to manual or automated regression tests in a dedicated QA environment. Final acceptance, integration and regression testing is performed in a representative test environment. All test results are recorded in UKCloud's Jira and Confluence repositories. Code reviews are managed though Bitbucket using pull requests. All code changes need to be approved by two different team members, which includes a subject matter

		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	x			expert. Once the pull request has been approved, only authorised UKCloud team members are able to merge code to the master branch. Key Development team members have GIAC Certified Web Application Defender (GWEB) certifications from SANS. They use static code analysis tools like SonarQube and OWASP dependency checker to identify potential security vulnerabilities in the code. This is integrated to UKCloud's Continuous Integration builds which are executed on every commit. The results for the master branch which represents production ready code is visible to all teams. OWASP ZAP is also used regularly by the UKCloud's QA Team to test for security vulnerabilities in the Portal application. This is done in accordance with UKCloud Software Engineering Development Process which includes a reference to the Secure Software Library Policy. Where a third party is recorded as being an essential element of the service, UKCloud will always engage an existing partner to minimise supplier engagement and provide the strongest controls for information within the supply chain. All UKCloud suppliers undergo a thorough selection process, and regular due diligence and audit checks are conducted during the lifecycle of the service. - Supplier Relationship Management Policy - Supplier & Partner Relationship Management Process For software suppliers, this includes an assessment of their approach to Systems/Software Development Lifecycle (SDLC) security. Evidence of assessment of third party security capabilities been evidenced during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications, undertaken regularly by Lloyd's Register. The activities surrounding coding, testing and deployment have been independently validated by a NCSC Pan Government Accreditor scoped IT Security Health Checks (ITSHC CHECK) undertaken by an independent organisation.
Change Control & Configuration Management *Quality Testing*	CCC-03	CCC-03.1	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.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			UKCloud has fully adopted ITIL as its service management framework, and this has been independently validated by Lloyd's Register as the independent assessors of UKCloud's ISO20000 certification. This framework includes documentation, technical resources and personnel training to address quality assurance matters, communication of known issues, the triage and remediation of bugs and known issues and the quality of released software bundles. Supporting documentation made available to customers includes: - Quality Management Policy - Quality Manual - Software Engineering Development Process - QA Test Strategy - UKCloud Knowledge Centre (https://docs.ukcloud.com) - Incident Management Policy - Incident Management Process - Problem Management Policy - Problem Management Procedure - Security Incident Management Policy - Security Incident Management Process
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X			
		CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	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.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			UKCloud has implemented a range of policy and technical controls to identify, report and address the installation of any software which is not present on the UKCloud Approved Software List. Alongside clear communication to personnel via the Acceptable Use Policy, which in enforced through Terms & Conditions of Employment, and regular security briefings, UKCloud has in addition implemented specialised monitoring solutions including: - Cisco Advanced Malware Protection (AMP) - Netwrix (auditing and reporting) - Nessus (security and vulnerability scanning) - Cumulo Protective Monitoring Services
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	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	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			UKCloud has a formal Change Management Policy and supporting Procedure are in place, which clearly define the respective roles and responsibilities of UKCloud personnel and customers. Customers are made aware of this documentation via their "Welcome Pack" and it is available within the UKCloud Customer Portal. This documentation is regularly assessed as part of UKCloud's formal ISO20000 assessments, undertaken by Lloyd's Register.
		CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			
		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?	X			
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	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.	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)?	X			UKCloud customers can apply metadata to their virtual machines, networks, etc. Customers are then able to use their metadata tags to control how they handle their own data: details of how to undertake this are communicated within the UKCloud Knowledge Centre (https://docs.ukcloud.com). Whilst UKCloud does utilise hardware asset policy tagging as a core component of its ITSM activities and protective monitoring services, at this time UKCloud does not offer the ability for customers to identify hardware assets via policy tags. Via the Customer Portal, UKCloud permits customer administrators to enable and control multi-factor user authentication through IP address restrictions. Data centres used by UKCloud are solely within the UK. Two secure campuses are used near Farnborough in Hampshire and near Corsham in Wiltshire. Customers can select and configure the storage for their data in either or both locations, depending upon their own requirements, and its geographic location is visible within the UKCloud Customer Portal.
		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.)?	X			
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	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.	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?	X			UKCloud maintains a secure repository of technical documentation relating to the authorised data flows between the components and services present within the UKCloud platform. This is used by UKCloud developers, and is a primary sources for the configuration of UKCloud's GPG13 aligned protective monitoring service (Cumulo, provided to UKCloud by e2e-assure, see https://www.e2e-assure.com). UKCloud strongly recommends that its customers deploy an equivalent form of protective monitoring capability within their own virtual environments (to which UKCloud personnel and system have no visibility). UKCloud delivers its cloud services from two UK-based data centre campuses operated by Ark Data Centres (https://arkdatacentres.co.uk) (near Corsham in Wiltshire, and at Farnborough in Hampshire) and therefore customer data cannot be located in any other geographic location. Customers can select which data centre(s) and hence location(s) they wish to use within the UKCloud Customer Portal.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X			
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	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.	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)?	X			UKCloud customers accessing the UKCloud Customer Portal and cloud services are encrypted through SSL/TLS. Customers are able to utilise industry standard encryption (e.g. 3DES, AES) on the UKCloud provided edge gateway, to provide SSL or IPSec VPN services (details are recorded within the UKCloud Knowledge Centre at https://docs.ukcloud.com). UKCloud utilises industry standard protocols including TLS, IPSEC and MACsec between user devices and its data centres.
		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)?	X			
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	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.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	X			UKCloud maintains an Information Classification Policy which determines the manner in which information assets of different classifications are to be labelled, handled, stored, disposed of etc. All personnel receive formal training on this subject. By default, UKCloud assesses all data repositories to be OFFICIAL (as per the Government Security Classification Policy) although customers who may have aggregated data considerations are responsible for identifying their own aggregation thresholds (as per service RMADS and SyOPs).
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		X		
		DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		X		
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	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.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			UKCloud does not access or copy customer or production data other than for authorised purposes of the service chosen, for example enabling customer-configured backup activities to take place. It is strictly forbidden for any customer data to be copied for development purposes or into non-production environments. This requirement is formally communicated during security briefings, and noted within the UKCloud SyOPs.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			UKCloud has a formal Asset Management Policy and supporting Process that requires all assets used to provide services to Customers to be accounted for and have a designated asset owner. Asset Owners are recorded within the InfoSaaS Assure risk assessment solution. Asset Owners are responsible for maintaining up-to-date information regarding their assets, including performing formal risk assessments. Customers manage their own data for the duration it resides on the UKCloud platform. Related documentation is provided to UKCloud Customers on the UKCloud Customer Portal.

Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	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.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			The UKCloud Asset Management Policy requires that all equipment (including both hardware and software assets) no longer required or subject to replacement must be subject to (a) secure disposal, or (b) secure cleansing prior to re-use. The supporting Data Erasure Policy details all aspects of data sanitisation including specific cloud service approaches for redeployment of resources (e.g. when a customer leaves a service) with specific detail and responsibilities recorded within the specific second-tier RMADS. Physical data sanitisation is undertaken using an appropriate method or product in accordance with HMG IA Standard No. 5 (IASS). This includes the use of approved Blancco or Tabernus software for any failed hard drives prior to disposal outside of the UKCloud business. Assets that require physical destruction are securely processed on-site during a witnessed destruction event. All disposal activities are supported by confirmation certificates. Customers looking to exit UKCloud's services are provided with the "UKCloud Client Offboarding and Decommissioning Process" which clearly communicates the customer's obligations when retiring cloud services and removing their data. This is also communicated to customers within the UKCloud Customer Portal.
		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?	X			
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	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.	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			As per the UKCloud Asset Management Policy, all assets are required to be identified, recorded, classified and defined to a named, responsible owner. Formal Supplier Management activities are in place (as per Supplier Relationship Management Policy), which includes the maintenance of a list of suppliers and details of their relationships (and the products/services they provide) with UKCloud. This activity is regularly reviewed during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications.
		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?	X			
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	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.	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?	X			UKCloud provides its cloud services from two secure data centre campuses, both owned and operated by Ark Data Centres (who additionally use the facilities for Crown Hosting). Each data centre maintains ISO27001 and ISO22301 certification, and additionally is externally validated by specific UK government accreditors. The physical security controls which are present on each site include: - 24x7 dedicated manned guarding, with secure internal control rooms and mobile patrols - Security fencing, vehicle blockers, full-height personnel turnstiles, perimeter detection beams - Extensive external and internal digital CCTV coverage with on-site and off-site recording - Solid construction of all walls and floor slabs. No windows in data rooms - Segregated loading and unloading areas, incorporating strategic airlocks - Triple authentication access control, incorporating ID cards, PIN validation and biometric authentication - Formalised "white list" access protocols, with robust procedures for visitor and emergency access requirements UKCloud also conducts internal audits as part of its ISO27001/17/18 certification within each of the Ark Data Centre campuses, validating that controls are in place and effective, and that the supplier's obligations are being delivered. Independent assessors from Lloyd's Register visit on at least an annual basis.
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	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.	Do you have a capability to use system geographic location as an authentication factor?	X			For internal UKCloud management systems, automated equipment identification is used as a method of validating connection authenticity (recorded within secure design repositories). MAC based authentication backed by Active Directory validation is used as a standard means to identify UKCloud-managed end user devices. Within the UKCloud platforms, a policy of disabling all unauthorised and unused ports, which removes risks associated with unknown equipment. UKCloud's protective monitoring service (Cumulo, provided by e2e-assure) is also configured to identify and report any unknown equipment or attempts to connect unknown equipment.
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			During the normal delivery of cloud services, there is no requirements for UKCloud to relocate or transfer any hardware, software or data assets to any off-site premises. Should a customer require for such a movement to take place, this would only be progressed by UKCloud against a formal Service Request from an authorised and authenticated representative of the customer, which if required would also entail validation with the accreditor or SIRO associated with the customer workload.
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	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.	Can you provide tenants with your asset management policies and procedures?	X			The UKCloud Asset Management Policy requires that all equipment (including both hardware and software assets) no longer required or subject to replacement must be subject to (a) secure disposal, or (b) secure cleansing prior to re-use. The supporting Secure Data Erasure and Destruction Policy details all aspects of data sanitisation including specific cloud service approaches for redeployment of resources (e.g. when a customer leaves a service) with specific detail and responsibilities recorded within the specific second-tier RMADS. Physical data sanitisation is undertaken using an appropriate method or product in accordance with HMG IA Standard No. 5 (IASS). This includes the use of approved Blancco or Tabernus software for any failed hard drives prior to disposal outside of the UKCloud business. Assets that require physical destruction are securely processed on-site during a witnessed destruction event. All disposal activities are supported by confirmation certificates. Additional information is documented within UKCloud's RMADS for various services and in the G-Cloud 10 Assurance Information Portfolio "Evidence Pack".
Datacenter Security *Policy*	DCS-06	DCS-06.1	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.	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?	X			A comprehensive library of information security, premises security and health and safety policies and supporting procedures is in place within the UKCloud Document Management System to ensure that all UKCloud personnel can work within a safe and secure environment when working from one of UKCloud's locations or facilities. Key documentation includes the UKCloud Facility Security Operations Framework and the UKCloud Health and Safety Policy. All personnel (and any applicable third party personnel) are required to attend and complete formal induction training soon after commencing their employment, which includes policy and procedure adherence, secure working practices and acceptable methods of working. Records of such training are maintained. Safety and security requirements and supporting evidential records are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	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.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			Each UKCloud data centre has been designed and constructed to incorporate segregated zones, which ensures that unauthorised personnel have no access to the physical environment from which UKCloud's services are delivered. This includes segregated loading/unloading areas, and separate facilities corridors for the maintenance of protective infrastructure. All zones are monitored by CCTV and subject to triple-authentication access control systems (pass card, PIN and biometric scan). Personnel access control to Ark Data Centres is in accordance with Ark Access Protocols, which are an external document available from UKCloud's Compliance Team. UKCloud personnel shall at all times fully comply with Ark Data Centres access requirements. Only permanent member of UKCloud staff who are listed on the current Ark Data Centres White List can access data centres (and different zones of access are authorised based upon the individual's authorised activities): the White List is managed by UKCloud's Compliance Team and is reviewed and updated regularly.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	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.	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?	X			Each UKCloud data centre has been designed and constructed to incorporate segregated zones, which ensures that unauthorised personnel have no access to the physical environment from which UKCloud's services are delivered. This includes segregated loading/unloading areas with airlocks, and separate facilities corridors for the maintenance of protective infrastructure such as fire extinguishing systems. All zones are monitored by CCTV and subject to triple- authentication access control systems. Personnel access control to Ark Data Centres is in accordance with Ark Access Protocols, which are an external document available from UKCloud's Compliance Team. UKCloud personnel shall at all times fully comply with Ark Data Centres access requirements. Only permanent member of UKCloud staff who are listed on the current Ark Data Centres White List can access data centres (and different zones of access are authorised based upon the individual's authorised activities): the White List is managed by UKCloud's Compliance Team and is reviewed and updated regularly.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			Each UKCloud data centre has been designed and constructed to incorporate segregated zones, which ensures that unauthorised personnel have no access to the physical environment from which UKCloud's services are delivered. This includes segregated loading/unloading areas, and separate facilities corridors for the maintenance of protective infrastructure. All zones are monitored by CCTV and subject to triple-authentication access control systems (pass card, PIN and biometric scan). Personnel access control to Ark Data Centres is in accordance with Ark Access Protocols, which are an external document available from UKCloud's Compliance Team. UKCloud personnel shall at all times fully comply with Ark Data Centres access requirements. Only permanent member of UKCloud staff who are listed on the current Ark Data Centres White List can access data centres (and different zones of access are authorised based upon the individual's authorised activities): the White List is managed by UKCloud's Compliance Team and is reviewed and updated regularly.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			All encryption keys are owned and managed by each named Service Owner, in accordance with UKCloud's SSL certificate Policy and Encryption Policy.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	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.	Do you have a capability to allow creation of unique encryption keys per tenant?		X		Customers who make use of the UKCloud-provided edge gateway can establish their own encryption keys for the service. UKCloud does not provide key management services for its customers. They are encouraged to deploy their own key management systems (using specialist hardware encryption modules or off-cloud key management systems) to adequately protect the data and systems which are hosted on UKCloud platforms. Procedures are in place to manage encryption keys for UKCloud's own activities - the UKCloud SSL Certificate Policy and Encryption Policy. UKCloud uses extensive physical access controls to satisfy the protection of "data at rest". Storage media which may contain customer data is physically contained with the dedicated, secure data suites inside the data centres used by UKCloud. As such, there is no separate storage media (such as conventional back-up tapes) which need to be removed from the data suites. UKCloud does not engage with any third-party organisation for the management of encryption keys.
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?		X		
		EKM-02.3		Do you maintain key management procedures?	X			
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X		

Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	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.	Do you encrypt tenant data at rest (on disk/storage) within your environment?		X		The UKCloud Encryption Policy details the requirements for encrypting data within the UKCloud Platform. It includes, for example, the applicable encryption technologies (as appropriate to the environment) will be in place for the transfer of customer images between hypervisors). Whilst UKCloud does not automatically encrypt customer data, they are able to encrypt their own data in accordance with their own security requirements. Where data at rest encryption is available within a specific UKCloud Service this is detailed within the Service Descriptions, which can be viewed on the Digital Marketplace. Further information is available within the UKCloud Knowledge Centre (https://docs.ukcloud.com).
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	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.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			The UKCloud Encryption Policy and SSL Certificate Policy detail the requirements for encrypting data within the UKCloud Platform. UKCloud has adopted industrystandard algorithms (e.g. 3DES, AES). UKCloud manages its own encryption keys in relation to its cloud platforms and services. It is each customer's responsibility to manage their own encryption activities (including key management).
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			
		EKM-04.3		Do you store encryption keys in the cloud?		X		
		EKM-04.4		Do you have separate key management and key usage duties?	X			
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	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.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			UKCloud maintains a secure internal repository of technical documentation, which includes details of standard, configurations and security baselines for every component of its cloud infrastructure. These ensure that personnel are consistently able to implement and operate such components to acceptable standards. Such documentation is regularly reviewed during external assessments of UKCloud's ISO27001, ISO27017 and ISO27018 certifications. All UKCloud infrastructure and systems are continually monitored by (a) Nessus, a security vulnerability and baseline analysis tool, and (b) Cumulo, a GPG13 compliant protective monitoring service provided by e2e-assure. Both of these immediately alert any deviation from security baselines, as well as suspicious or unauthorised access or behaviour to UKCloud's 24x7 NOC. Customers may upload, or create, their own trusted virtual machine images, which satisfy their own internal standards, for use on the UKCloud platform.
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	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	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?	X			UKCloud provides visibility (or "showback") of platform-related protective monitoring data to each specific customer, in order that they can validate the status of UKCloud's cloud services on an ongoing basis. UKCloud undertakes comprehensive information security risk assessments (as required by ISO27001:2013) in accordance with the UKCloud Risk Assessment Methodology, with data protection, location and retention requirements assessed within activity-focused Data Protection Impact Assessments, undertaken as per the GDPR Evidence Pack. Supporting records from risk assessments and DPIAs are formally reviewed on an annual basis as a minimum, and are subject to external assessment during external accreditations provided by UK public sector organisation and during external assessments of UKCloud's ISO27001/17/18 certifications undertaken by independent assessors from Lloyd's Register.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	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?	X			All UKCloud personnel, including all executive, business and technical managers, have defined roles and responsibilities, formally published job descriptions (within the UKCloud Document Management Systems) and contractual clauses within their Terms and Conditions of Employment to ensure that they remain fully compliant with all UKCloud published policies and associated procedures. Such responsibility is also communicated during formal induction training and during periodic refresher training initiatives, of which training records are maintained.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	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	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			All UKCloud customers receive information about the Information Security Management Plan (ISMP) within the RMADS (Risk Management and Accreditation Documentation Sets) that are available to support each cloud service which is made available to customers. It is also documented within the G-Cloud 10 Assurance Information Portfolio "Evidence Pack" which is made available to customers. The UKCloud Information Security Management Plan (ISMP) is reviewed on a quarterly basis during formal management review meetings, in accordance with UKCloud's Management Review Policy. RMADS (Risk Management and Accreditation Documentation Sets), and supporting Residual Risk Statements which validate each cloud service are made available to customers on request to the UKCloud Compliance Team.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	X			
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	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.	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?	X			All UKCloud personnel, including all executive, business and technical managers, have defined roles and responsibilities, formally published job descriptions (within the UKCloud Document Management Systems) and contractual clauses within their Terms and Conditions of Employment to ensure that they remain fully compliant with all UKCloud published policies and associated procedures. UKCloud's Information Security Policy provides clear direction and commitment requirements. Formal information security management system's management reviews with the UKCloud Leadership Team are conducted on an annual basis, in accordance with the UKCloud Management Review Policy, which is supported by ongoing Leadership Team reviews during quarterly reviews every 90 days.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	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.	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)?	X			UKCloud's information security and data privacy policies align with a wide set of industry standards - this is assessed and validated during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register. UKCloud additionally maintains Cyber Essentials and Cyber Essentials Plus certifications, and has been certified as a PSN service provider and for PSN connectivity to each cloud service. UKCloud suppliers are contractually required (by formal agreement) to adhere to UKCloud's security policies and procedures - this is undertaken in accordance with the Supplier Relationship Management Policy and the Supplier Relationship Management Process. The risk management methodology which underpins the Information Security Management System (ISMS) and ISO27001/ISO27017/ISO27018 certifications clearly records how controls, processes, activities and documentation maps to individual threats and/or vulnerabilities to UKCloud information and supporting assets. UKCloud operates an ISMS Operational Framework which includes a formal Risk Assessment Methodology. A wide variety of assurance-related information is made available to customers on request from UKCloud's Compliance Team.
		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?	X			
		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	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.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			UKCloud has implemented and maintains a formal Disciplinary Policy and Procedure - the Terms & Conditions of Employment also communicating that disciplinary action to be taken if anyone fails to comply with published policies and processes. UKCloud staff are made aware of what actions could be taken in the event of a violation via induction and refresher training sessions and via Disciplinary Policy and Procedure which is communicate to and accessible to all via the UKCloud Document Management System.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			UKCloud maintains a formal risk assessment programme (using InfoSaaS Assure) which has been designed to assist in identifying whether security policies, procedures, standards and controls remain relevant and are providing an acceptable level of protection to assets. If any risks are identified as being unacceptable, the documentation and/or controls will be highlighted for formal update to ensure that they remain relevant and effective. The risk assessments are reviewed on at least an annual basis. This is documented in an ISMS Operational Framework including UKCloud Risk Assessment Methodology. Risk management activities are assessed and validated during external assessments of UKCloud's ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register, and during formal assessments undertaken by Government accreditors.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	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.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			All UKCloud documentation, including policies and procedures around privacy and security, are required to have a formal review on an annual basis as a minimum, although these often happen more frequently as documentation is updated to reflect developments and improvements in working practices - this is performed in accordance with UKCloud's Document Control and Record Management Policy and Process. All UKCloud customers are promptly informed (and in advance, where possible) of changes to information security and privacy policies, with such updates also being communicated via the UKCloud Customer Portal and their dedicated Service Delivery Manager as the business relationship owner. Formal management reviews with the UKCloud Leadership Team are conducted on an annual basis, in accordance with the UKCloud Management Review Policy, which is supported by ongoing Leadership Team reviews during quarterly reviews every 90 days.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			

Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	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).	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?	X			UKCloud maintains a formal risk assessment programme (using InfoSaaS Assure) which uses qualitative and quantitative methods to assess the probability and impact of a comprehensive selection of threats and vulnerabilities to different types of assets (including data), including audit findings, independent technical assessments (e.g. ITSHC CHECK Tests), security incidents, threat advisories and external regulatory and legislative requirements. The Risk Assessment Methodology includes requirements to identify a wide range of threats and vulneraries focused on each asset type, and for the formal assessment of the probability and impact of each occurring. Such analysis is evaluated against UKCloud's risk acceptance threshold, with any risk exceeding this limit progressed for one or more options for risk treatment (as required by Section 6 and 8 of ISO27001:2013). Risk management activities are assessed and validated during external assessments of UKCloud's ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register. Risk assessment activities and details of any residual risks are communicated to customers within formal RMADS and Residual Risk Statements for each cloud service.
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	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.	Do you have a documented, organization-wide program in place to manage risk?	X			UKCloud maintains a formal risk assessment programme which measures risk levels and compares these to an acceptance threshold determined by the UKCloud Leadership Team. Any risks that are above this threshold are required to be remediated using one of four approaches (reduce, transfer, stop, accept) and require Leadership Team approval for their mitigation. Details of the risk criteria and acceptance levels are documented in an ISMS Operational Framework including UKCloud Risk Assessment Methodology. Risk assessment activities and details of any residual risks are communicated to customers within formal RMADS and Residual Risk Statements for each cloud service.
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			UKCloud operates a formal starters and leavers framework (in accordance with the Employee Management Process, which ensures that upon termination of personnel or expiration of an external business relationship, all assets are promptly recovered and access to premises, systems and solutions is immediately revoked. Records of these activities are retained. This is in accordance with Leavers Form..
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	X			
Human Resources *Background Screening*	HRS-02	HRS-02.1	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.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			The UKCloud Security Clearance Policy details how all employees are required to obtain and maintain an appropriate level of security clearance for their role, which is recorded within their respective Job Description. All employees and any contractors (if applicable) are required to achieve formal basic check validation as a minimum, with higher SC (and above) and NPPV (Non-Police Personnel Vetting) Level 3 clearances being required for those who: - support the UKCloud platform and customer environments, including those who access monitoring and reporting tools - have access to the IT infrastructure which supports the UKCloud platform and customer environments - have access to the UKCloud data centres and data suites in which infrastructure is located - non-technical personnel who engage with customers on specific matters which specifically require a higher security clearance level Security clearance are processed by Warwickshire Police, the Home Office and UKSV. Certain operational roles may be subject to additional, sector specific clearance requirements.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	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.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			UKCloud personnel have formal job descriptions in place which define their roles and responsibilities, as required by the Employee Management Process. UKCloud has a formal Security Training Policy in place: the information security induction is mandatory and is delivered to new joiners by UKCloud's Compliance Team within 10 working days of the new starter joining the business. The training records are recorded and maintained in UKCloud's HR system (PeopleHR). All personnel sign formal Employment Terms and Conditions before they join. On the first day of employment, all staff are required to read and acknowledge UKCloud's Security Operating Procedures (SyOPs) - records of signed declarations are maintained by UKCloud's Compliance Team. UKCloud maintains an IT System Access Matrix where Asset Owners define appropriate level of access to premises, systems, assets and data sources - access is defined based on the requirements of the individual role, and defaults to zero. All the activities listed above are regularly assessed, both during internal audits and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
		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?	X			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			UKCloud operates a formal starters and leavers framework (in accordance with the Employee Management Process, which ensures that upon termination of personnel or expiration of an external business relationship, all assets are promptly recovered and access to premises, systems and solutions is immediately revoked. Records of these activities are retained. This is in accordance with Leavers Form.
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	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).	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)?	X			UKCloud had determined how sensitive data is to be accessed from portable and mobile devices in its Access Control Policy and its Encryption Policy. All UKCloud systems and services are subject to protective monitoring (using Cumulo, provided to UKCloud by e2e-assure), and personnel are made aware of accepted working practices, policy requirements and activity monitoring through their Terms and Conditions of Employment, formal policy documentation and regular security briefings (of which records are retained). Access management, asset management and access control activities are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	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.	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?	X			All personnel sign formal Employment Terms and Conditions before they join, which contains confidentiality and non-disclosure requirements. Additional declarations are also present within the various security clearance documentation which they are required to complete. Employment records are maintained by UKCloud's HR team, with the Compliance Team securing clearance-related records. They are subject to ongoing assessment for suitability, accuracy and legislative/regulatory compliance.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			For UKCloud personnel, each employee's job description clearly communicates their individual responsibilities for information security and the management and use of specific assets. For any contractors engaged by UKCloud, similar requirements are communicated within their Engagement Agreement. Third-party users are governed by the applicable Terms and Conditions for using UKCloud services, which include requirements related to information security, data protection, access to resources and acceptable activities. A number of different Terms and Conditions documents are in use, dependent upon which framework the customer/third-party user has used to engage with UKCloud.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	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.	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?	X			UKCloud does not have any access to its customers' data or the majority of metadata (except metadata which reports service consumption for billing purposes) hence UKCloud does not provide documentation regarding how we may or access tenant data and any other types of metadata. UKCloud does not collect or create metadata about tenant data usage through inspection technologies - UKCloud does not have any access to its customers' data or the majority of metadata (as above).
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	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.	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?	X			All personnel, contractors and any third-party users are provided with formal induction and periodic refresher training on adhering to UKCloud information security and data protection requirements - as per the Information Security Training Policy. The ISMS induction is mandatory to all new starters in the company. Refresher training sessions are delivered by the Compliance Team approximately every 3-4 months, encompassing any new security working practices, managing evolving threats, and communicating emerging best practice. All such training includes specific instruction on the security of mobile devices and protection against malware, and the acceptable use of mobile assets. Records of information security and data protection training are retained.
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			
		HRS-09.3		Do you document employee acknowledgment of training they have completed?	X			
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			
Human Resources *User Responsibility*	HRS-10	HRS-10.1	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	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			UKCloud has a formal Security Training Policy in place. The information security induction is mandatory and is delivered to new joiners by UKCloud's Compliance Team within 10 working days after new starters join the business. Refresher training sessions are delivered periodically - e.g. by Compliance Team sending a security update bulletins or by delivering refresher training sessions in person. The training records are logged and maintained in UKCloud's HR system PeopleHR. The employees' awareness and compliance with various security policies are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			

Human Resources *Workspace*	HRS-11	HRS-11.1	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.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	x			UKCloud ensures that validation and authentication of users is in place. Inactivity lock out times on the UKCloud Customer Portal prevent any onward dependent sessions into a specific customer's virtual environments. The respective roles of UKCloud and its customers are defined within the RMADS and supporting assurance documentation. UKCloud does not permit access to customer environments or their data. By exception, this is only permitted if (a) authority has been provided by an authorised representative of the customer, and (b) the request has then been reviewed and approved by the UKCloud Compliance Department. Internally, UKCloud has an Acceptable Use Policy and UKCloud's Security Operating Procedures (SyOps) - which all UKCloud staff are required to sign to and are required to comply with. UKCloud Acceptable Use Policy states that employees should lock their screens when leaving devices unattended (which is technically enforced by system settings). Employees are periodically reminded of this requirement through training and awareness initiatives. Additionally UKCloud devices are configured to automatically lock their screens after a 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?	x			
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	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.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			UKCloud has implemented and operates several technical controls to ensure only authorised individuals can authenticate to and access the UKCloud services for which they have an identified and approved business need. This is recorded within UKCloud's System Access Matrix. UKCloud personnel are required to use 2FA authentication tokens (RSA SID 700/800 hardware tokens, RFC 6238 compliant software tokens or device certificates). UKCloud's Access Control Policy places specific responsibilities on "super user" or administrative accounts, which are not to be used routinely for normal support or development tasks. Any accounts which are required to have "super user" permission are uniquely created in such a way that the activities of the individual will still be tracked and recorded, clearly identifying the access and actions undertaken using the privileged account. All authentication requests (as well as many other functions) are fully logged and analysed in near real-time via the UKCloud GPG13 aligned protective monitoring service (Cumulo, provided by e2e-assure) which is operated and alerts on a 24x7 basis. Customers are strongly advised to deploy their own protective monitoring service within their own virtual environment, as required by the UKCloud "System Interconnect Security Policy". An effectively implemented protective monitoring service, encompassing the controls PMC1-12 from GPG13, enable customers to autonomously generate a record of user activity and security events which specifically relate to their own environment and applications. UKCloud's protective monitoring service maintains its own external accreditations and certifications. For customer-facing online systems (e.g. UKCloud's Customer Portal & API interfaces), all users are required to have a unique username and password. In addition, they have the option to add a memorable word combination. UKCloud personnel are required to use 2FA authentication tokens.
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	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) • 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) • 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.*	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			The Employee Management Process requires the immediate return of all UKCloud assets (including information, documentation, hardware, software, tokens and ID cards), when these are (a) no longer required for ongoing business purposes, (b) from personnel who leave the employment of UKCloud, or (c) from third parties who cease to provide services to UKCloud. These are then updated within the UKCloud Inventory of Assets, and system access is revoked (or adjusted, as applicable) with immediate effect. These activities are performed in accordance with UKCloud's Employee Management Process. UKCloud ensure that communications are sent out regarding the requirement to remove access from a known leaver in advance, and the removal of systems access will be completed on the day of departure by various UKCloud teams (e.g. Internal IT, Development, Customer Service, Compliance etc). Similarly, for any unplanned personnel departures the request will be expedited and completed the same day, typically within 30 minutes. Removal of the Windows Active Directory account disables overall platform and remote access to all UKCloud services. (Note: customer permissions management is self-managed through the UKCloud Customer Portal)
		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?	x			
		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?	x			
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	x			
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	x			
		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?	x			
		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?	x			
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	x			UKCloud operates a segregated management network through which the UKCloud platform is administered. UKCloud maintains an IT System Access Matrix which defines personnel access to IT systems and networks based on their role. This also specifies which users have access to diagnostic and configuration ports. A formal Access Control Policy is in place - which is reviewed annually as a minimum.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	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.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			Policies and procedures are in place to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. UKCloud maintains an IT System Access Matrix which defines personnel access to various IT systems and information based on their role. A formal Access Control Policy has been implemented. UKCloud operates on a principle of "no access" until such time as appropriate authority for access has been provided. Active Directory Groups provide means for validating a user's identity against access to systems and data, and UKCloud's protective monitoring service (Cumulo, provided by e2e-assure) records and escalates any out-of-line activities. Access control activities and records are regularly assessed, both during internal audits and risk assessments undertaken by the UKCloud Compliance Team (as per Internal Audit Schedule and the current ISMS Statement of Applicability), and during external assessments of ISO20000 (IT Service Management) and ISO27001/17/18 (Information Security Management) certifications undertaken by independent assessors from Lloyd's Register.
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	x			
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	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.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	x			UKCloud maintains an IT System Access Matrix which defines personnel access to all data sources, IT systems and networks based on their role. A formal Access Control Policy is in place - which is reviewed annually as a minimum.
Identity & Access Management *Source Code Access*	IAM-06	IAM-06.1	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	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?	x			UKCloud maintains an IT System Access Matrix which defines personnel access to various IT systems and information based on their role. A formal Access Control Policy is in place - which is reviewed annually as a minimum. UKCloud operate on a zero access principle, such that specific authority needs to be provided before an individual is approved to be able to access systems, services or datasets. UKCloud does not have any access to customer virtual environments, or the data that they may be hosting.

Restriction		IAM-06.2	the rule of least privilege based on job function as per established user access policies and procedures.	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?	X			
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	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.	Does your organization conduct third-party unauthorized access risk assessments?	X			UKCloud has designed and implemented its cloud services platforms so as not to have any single points of failure. As such, full resilience of the data centre environments, network connectivity, external networks, the Customer Portal and core functionality is provided from multiple data centres. UKCloud customers can select and implement different levels of cloud service, which should be chosen carefully to ensure that these provide a corresponding level of resilience to make the customer's own requirements (these are detailed within individual Service Definitions, available for viewing on the Digital Marketplace). UKCloud maintains real-time visibility of its data centre estates, its external protective monitoring service provider (e2e-assure), and uses Solarwinds to assist with monitoring the state of all networks/circuits from upstream providers. Geographically-diverse data centres allow for resilient separation within UKCloud systems and customer environments. For internet network connections, multiple links from multiple providers increase resiliency, performance and availability. BGP peering is used to provide continual monitoring of the availability and performance of upstream providers. UKCloud advises customers of the disaster recovery services available via the UKCloud Customer Portal and related assurance documentation. UKCloud ensures that full resilience is built into data centre environments, core platform functionality, protective monitoring and network connectivity. Customers may independently declare a disaster, which well then immediately assessed by UKCloud and progressed appropriately according to the situation. Customers may initiate failover mechanisms at their discretion. UKCloud provides summary information on its business continuity and disaster recovery plans to its customers. Detailed information may not be provided, if it is assessed that such a disclosure would place the security position of UKCloud at increased risk, would breach data protection requirements or inhibit UKCloud's ability to meet the security requirements of its customers within multi-tenancy environments.
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	X			
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	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.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			UKCloud maintains an IT System Access Matrix which defines personnel access to various IT systems and information based on their role. A formal Access Control Policy is in place - which is reviewed annually as a minimum. UKCloud operates on a principle of "no access" until such time as appropriate authority for access has been provided. Access to customer virtual environments and data is only permitted if (a) authority has been provided by an authorised representative of the customer, (b) the request has then been reviewed and approved by the UKCloud Compliance Department and (c) the customer has technically enabled the appropriate level of access for the assistance they have requested. There is no automatic means of aligning customer data classifications within UKCloud services. It remains each customer's responsibility to understand the security classifications applicable to their data, and for them to select and configure an appropriate cloud service which provides sufficient security protection in line with their data classifications.
		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?	X			
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	X			
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	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.	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?	X			All personnel are governed by the UKCloud ISO27001-certified Information Security Management System, which includes adherence to applicable security policies and related operational procedures. This ensures that user access provisioning is only undertaken after receiving formal authorisation, and then in accordance with the IT Systems Access Matrix which defines personnel access to various IT systems and information based on their role. A formal Access Control Policy is also in place. New customers are provided with a single account to their authorised representative when they commence using a UKCloud service. Thereafter, they are responsible for creating and configuring all other user accounts within their organisation. This is documented in more detail in G-Cloud 10 Assurance Information Portfolio "Evidence Pack". Access to physical locations, infrastructure, application systems and network components is limited to small number of personnel (as per the current Ark Data Centre's White List) to maintain the highest levels of security. Customers are able to access their own data and virtual applications through the UKCloud Customer Portal.
		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?	X			
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	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.	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?	X			The IT Systems Access Matrix is regularly reviewed to ensure that personal continue to have access appropriate to their current role. The IT Systems Access Matrix is also consulted during routine internal audit activities, and its accuracy is again validated during periodic (at least annually) reviews of the supporting risk assessment for each asset. UKCloud operates on a principle of "no access" until such time as appropriate authority for access has been provided. Any discrepancies identified are recorded and promptly progressed as formal security incidents in accordance with the Security Incident Management Policy and Security Incident Management Process. UKCloud confirms that it has no access to its customers' virtual environments nor any of their hosted data.
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X			
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	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.	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?	X			The 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 is done in accordance with the Employee Management Process. Employment Termination Records are obtained to demonstrate that all applicable actions have been completed in a timely manner. The record confirms the recovery of all assets and revocation of any system access.
		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?	X			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	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)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		X		UKCloud customers can manage their accounts by connecting to the Customer Portal over "https" or programmatically via a RESTful API with a combination of their unique username, password and 2FA combination. This provides the authenticated user with access to the interface in which they can manage their virtual environments. UKCloud customers are able to control or restrict access for their own users by specifying specific network/IP addresses. New UKCloud customers are provided with a single account to their authorised representative when they commence using a UKCloud service. Thereafter, they are responsible for creating, configuring and managing all other user accounts within their organisation. This is documented within the UKCloud Knowledge Centre (https://docs.ukcloud.com). Multi-factor authentication options are available to customers, which include one-time passwords (RFC 6238 compliant software tokens) and the provision of SSL-device digital certificates for the secure remote access service. Customers cannot use third party identity assurance solutions when authenticating to UKCloud services. However, they have complete autonomy and flexibility to implement and use third party assurance solutions within their applications and systems hosted on the UKCloud platform. Password complexity requirements are recorded within the UKCloud Password Management Policy and supported by aligned technical controls (e.g. Active Directory). Access to the Customer Portal requires the use of complex passwords as defined by UKCloud. Customers are responsible for configuring the complexity of passwords and for their management within their own virtual environments. Forced password change requirements are recorded within the UKCloud Password Management Policy, and supported by aligned technical controls (e.g. Active Directory). An administration portal is available which enables locked user accounts to be unlocked and passwords reset. This function is available to customers by raising a Service Request - information about how to raise a service request is available from the UKCloud Portal - Customer Support Engagement Guide.
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?		X		
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		X		
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X		
		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?		X		
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	X			
		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?	X			
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			
		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)?	X			
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			In support of the IT Systems Access Matrix, UKCloud operates RBAC (Role Based Access Control) to ensure utility programs are properly controlled. A protective monitoring solution (Cumulo, provided to UKCloud by e2e-assure) continuously monitors audit logs for suspicious activity which may indicate unauthorised usage of such utilities. UKCloud uses a combination of hardware and software controls to identify any attacks being targeted at the virtual infrastructure layer. The Cumulo protective monitoring solution continuously monitors SIEM (security information and event management) logs for any indications of suspicious activity. UKCloud use a robust set of hardware and software controls to identify and neutralise attacks targeted at the virtual infrastructure layer. For example, all inbound internet traffic is monitored for DDOS activity using Neustar technology.

Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	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.	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?	X			For "Assured" (internet-facing) solutions, UKCloud do not offer network IDS as part of our standard offering. Whilst UKCloud can address activity based threats (e.g. port scans, syn floods, etc.), it is less effective at addressing payload threats as the traffic is typically encrypted when it passes through our IDS solution. Hence UKCloud recommend that customers implement their own Application Firewall, Network IDS/IPS (within their virtual data centre) and/or host based IDS/IPS. In this way, customers have complete control over the policies and the resulting audit logs. Customers can also consider implementing a Content Delivery Network (CDN) in front of the UKCloud solution. All traffic will flow through the CDN which often provide IDS/IPS features and can deal with issues such Distributed Denial of Service attacks. For "Elevated" (PSN- facing) solutions, UKCloud operate network IDS at the perimeter firewall and all logs are actively monitored via a protective monitoring service. It should be noted that whilst the solution can address activity based threats (e.g. port scans, syn floods, etc.), it is less effective at addressing payload threats as the traffic is typically encrypted when it passes through our IDS solution. Hence, UKCloud recommend that customers implement additional IDS/IPS within their own cloud solution as appropriate. Access to audit logs is restricted to authorised users only, as defined within the IT Systems Access Matrix. UKCloud operates a comprehensive protective monitoring service which has been developed and implemented in accordance with established standards: ISO20000 for IT Service Management, ISO27001 for Information Security Management and NCSC guidance GPG13. These standards are regularly validated by external assessors from Lloyd's Register to provide formal certification, as well as Government accreditors and customer auditors. Logs relating to all operations of the UKCloud service are stored centrally. All authentication requests and many other functions of the UKCloud platforms are fully logged and analysed in near real-time by UKCloud's protective monitoring service which operates on a 24x7 basis. Customers are recommended to implement their own protective monitoring service within their own virtual environments, as required by the UKCloud SISP (System Interconnect Security Policy). An effectively implemented protective monitoring service, for example addressing the controls PMC1-12 from GPG13, enables customers to autonomously generate a record of user activity and security events which specifically relate to their own environment and applications.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			
		IVS-01.4		Are audit logs centrally stored and retained?	X			
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	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).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			The UKCloud platform logs (to the Centralised Log Store) all changes made by all users to the virtual machine configuration. All changes are formally requested, assessed, approved and executed under formal change management Policy and Process. Changes made within the customer's virtual machines (e.g. operating systems and applications) are the responsibility of the customer as they have exclusive control and autonomy at that layer. The UKCloud Customer Portal provides users with audit logging capabilities which capture any changes made to all virtual machines, regardless of their running state.
		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?	X			
		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)?	X			
Infrastructure & Virtualization Security *Clock*	IVS-03	IVS-03.1	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.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			All UKCloud infrastructure and standard-build cloud services utilise redundant time servers that constantly synchronise with external UK PSN time servers. UKCloud offers this time-source service for use by its customers.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	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.	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?	X			UKCloud provides customers with details of its networks, storage, memory etc. within customer infrastructure via published Service Definitions (as published in the Digital Marketplace), and knowledge articles/FAQs available in UKCloud's Knowledge Centre at https://docs.ukcloud.com. UKCloud customers are restricted from oversubscribing memory resources by the hypervisor, which only allocates as much memory as has been requested by the virtual machine when it is instantiated. Virtual machines cannot write to more memory than was initially allocated. UKCloud maintains formal capacity management activities, in accordance with ITIL v.3 best practice and its ISO20000 certification, to ensure sufficient capacity is available for customers based on current usage and planned growth - capacity management activities are performed in accordance with Capacity Management Policy and Process. UKCloud platforms are monitored centrally 24x7 by the UKCloud Network Operations Centre (NOC). Any performance or service anomalies are triaged by NOC personnel, resolved where possible, or promptly passed to the appropriate resolver group to address. Performance and capacity attributes of systems is the responsibility of defined system owners, being reviewed on an ongoing basis to ensure that contractual requirements are being met.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			
		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?	X			
		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?	X			
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			On an ongoing basis, UKCloud uses Nessus for performing regular vulnerability assessment scans of the UKCloud platform. UKCloud has comprehensive ITSHC/CHECK security tests undertaken by an independent testing organisation at least once a year.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	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.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			Customers are encouraged to refer to the UKCloud Knowledge Centre (https://docs.ukcloud.com) which presents a wide variety of information on all aspects of UKCloud's services. If required, customers can also engage with one of UKCloud's Pre-Sales Architects or Service Delivery Managers to ensure that their solutions are designed and implemented to meet their unique security requirements. All documentation is regularly reviewed by UKCloud, including network architecture, security domains and security zones. This ensures that the latest and most accurate information is being made available to customers. All firewall access and rules are regularly reviewed by the UKCloud Networks Team, as part of their daily checks. UKCloud provides a default configuration which restricts connections between trusted and untrusted connections. Customers have the ability to purposely modify the configuration to allow certain types of untrusted connectivity: in this scenario both customers must make a reciprocal change to allow certain types of traffic to flow between their respective cloud solutions. For less common traffic types, customers can request UKCloud to review their request, which is undertaken by the Security Operations Team using UKCloud's Change Management Process. For traffic between the UKCloud's "Assured" internet connected domain and the "Elevated" PSN- connected domain, customers are required to obtain formal cross-domain approval before being allowed to proceed. UKCloud also operates a comprehensive protective monitoring service which has been developed and implemented in accordance with established standards: ISO20000 for IT Service Management, ISO27001 for Information Security Management and NCSC guidance GPG13. These standards are regularly validated by external assessors from Lloyd's Register, to provide formal certification, as well as accreditors and customer auditors. Logs relating to the operation of the
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	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.	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?	X			All operating standards are hardened in accordance with current best practice - Standard Build documents are regularly reviewed and published in UKCloud's Document Management System (DMS) and the secure internal repository for technical documentation, which is made available to all UKCloud technical personnel.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	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.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Customers can select and configure separate environments (including separate authentication sources, hardware etc.) for test/development and production purposes. Customers have access to "Blueprints" and "Getting Started Guides" within UKCloud's Knowledge Centre (https://docs.ukcloud.com) to assist with creating their environments. All UKCloud environments are fully segregated, including production and non-production environments.
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	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	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Physical firewalls protect the UKCloud platform. Customers can choose to deploy and manage their own virtual firewalls, or use the UKCloud-provided Edge Gateway which has firewall capabilities - details are communicated within the UKCloud Knowledge Centre (https://docs.ukcloud.com) System and network environments are protected by software firewalls that are provisioned as standard for all customer environments. In addition, UKCloud also offer customers the option to implement other software based firewalls that we have confirmed are compatible with our infrastructure. UKCloud production and non-production environments are appropriately separated by firewalls. It remains the customer's responsibility as to how they deploy their virtual environments (and firewalls) to ensure compliance with legislative, contractual and regulatory requirements and appropriate protection and isolation of sensitive data.
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			
		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?	X			
		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?	X			
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	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.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			All UKCloud's cloud Services are exposed via SSL/TLS, this allows customers to migrate their physical and virtualised servers onto the platform. Customers are also able to establish SSL or IPSEC VPNs into their virtual data centres, to facilitate the migration of applications and data directly into operating systems within their virtual data centre. Migrations of physical and virtual servers via the UKCloud Customer Portal are performed via the UKCloud Administrative Networks, which are securely segregated from the customer data network.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			

Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	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).	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)?	x			UKCloud operates a robust IT Systems Access Matrix, which records the levels of authorised access to systems appropriate to the individual's role and valid business requirements. When administering the UKCloud platform, administrative personnel are required to authenticate utilising a combination of device certificates (Microsoft Certificate Authority based) and RSA hardware tokens (SID700/SID800). All management access (as well as other functions) is via SSL/TLS encrypted communications which are fully logged and analysed in near real-time via the UKCloud GPG13 aligned protective monitoring service (Cumulo, provided by e2e-assure) which is operated on a 24x7 basis. Customers are strongly recommended to deploy their own protective monitoring service within their own virtual environments, as noted within the UKCloud SISP (System Interconnect Security Policy). An effectively implemented protective monitoring service, encompassing the protective monitoring controls PMC1-12 from GPG13, will enable UKCloud customers to autonomously generate a record of user activity and security events which specifically relate to their own environments and applications. UKCloud's protective monitoring service maintains its own external accreditations and certifications.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	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	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	x			UKCloud regards all wireless networks to be insecure, and these are provided within its office environments only. Within UKCloud's offices, wireless connectivity is provided for the use of staff and visitors (UKCloud Wi-Fi Network Process). Wireless connectivity is configured for strong encryption settings, and allows general internet access only, with all such access protected through a combination of Cisco Umbrella and Cisco Sourcefire to reduce the risk of internet-related compromises occurring. Events from the wireless network, and associated products, are additionally analysed by the Cumulo protective monitoring service provided to UKCloud by e2e-assure. UKCloud staff utilising the wireless network for anything other than general internet browsing must establish a secure VPN connection to gain onward access to UKCloud data or administer the UKCloud Platform.
		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)?	x			
		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?	x			
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	x			UKCloud holds a secure internal repository of technical documentation that includes detailed network architecture diagrams. These diagrams clearly highlight hash-risk environments (for example customer/interface presented portals). These diagrams are used in combination with the Cumulo protective monitoring service provided to UKCloud by e2e-assure, which also includes performing packet analysis. All UKCloud internet connected environments, as well as customer internet environments are protected by volumetric DDoS detection and mitigation using Neustar technologies, using a combination of technologies located within each of UKCloud's data centres, as well as larger-scale "internet scrubbing centres" which can be activated to traffic throttle any larger scale or prolonged DDOS attacks.
		IVS-13.2	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.	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?	x			
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			The various UKCloud cloud services are exposed to customers via a number of APIs. Predominately these are common industry APIs (e.g. VMware vCloud Director, Openstack, etc) from commercially available products. A small number of APIs are UKCloud specific, these relate to Customer account management, monitoring showback, and ticketing. Further details on all APIs which are available to Customers can be located within the UKCloud Knowledge Centre (https://docs.ukcloud.com)
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	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).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	x			The UKCloud Customer Portal allows customers to download data in various industry-standard formats, including csv, json, xml, pdf. Customers are also able to download their own virtual machine images in an industry-standard format (e.g. OVA for VMware images). Where a request for further data is made, any data made available will be in the most appropriate industry-standard format determined by UKCloud according to where the data is held (typically doc, xls, csv, pdf).
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	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.	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?	x			The APIs relating to UKCloud services are included within the control plane SLAs corresponding to each service - this includes APIs to interacting with the services, as well as for migrating images to/from the service. These SLAs are detailed within the applicable Service Definition. Service Levels are managed through the UKCloud Service Level Management Process.
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	x			
		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?	x			
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	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.	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	x			All APIs for UKCloud Servers are exposed via SSL/TLS. Details on the APIs, including their interoperability, and accessibility are available on the UKCloud Knowledge Centre (https://docs.ukcloud.com).
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	x			
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	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.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	x			UKCloud's cloud services use industry recognised virtualization formats. The most appropriate format is used according to the service, for example OVF/OVA with the UKCloud VMware service. Details on the virtualization format are made available to customers on the UKCloud Knowledge Centre (https://docs.ukcloud.com). At the time of writing, no customisation of these formats has taken place.
		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?	x			
		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?	x			
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	x			All personnel are provided with formal induction and periodic refresher training on adhering to UKCloud information security requirements - as per the Information Security Training Policy. The ISMS induction is mandatory to all new starters. Refresher training sessions are delivered by the Compliance Team approximately every 3-4 months, encompassing any new security working practices, managing evolving threats, and communicating emerging best practice. All such training includes specific instruction on the security of mobile devices and protection against malware, and the acceptable use of mobile assets. Records of training are retained.
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	UKCloud does not permit UKCloud mobile access to the UKCloud customer or management platforms. Mobile access may only be used to consume internal UKCloud corporate resources and such mobile access is subject to policies and procedures that include a whitelist of approved application stores. Various requirements are documented in UKCloud's Acceptable Use Policy and Mobile Telephone Policy.
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	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.	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?			x	UKCloud does not permit the installation of non-approved applications or approved applications not obtained through a pre-identified application store. Detailed requirements are documented within and communicated by UKCloud's Acceptable Use Policy and Mobile Telephone Policy.
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	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.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	x			UKCloud maintains a formal BYOD Policy. All personnel are provided with formal induction and periodic refresher training on adhering to UKCloud information security requirements - as per the Information Security Training Policy. The ISMS induction is mandatory to all new starters in the company. Refresher training sessions are delivered by the Compliance Team approximately every 3-4 months, encompassing any new security working practices, managing evolving threats, and communicating emerging best practice. All such training includes specific instruction on the security of mobile devices and overview of approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. Records of training are retained.
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	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.	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?	x			UKCloud maintains an Acceptable Use Policy and Mobile Telephone Policy. All personnel are provided with formal induction and periodic refresher training on adhering to UKCloud information security requirements (which includes the management and use of mobile devices) - as per the Information Security Training Policy. The ISMS induction is mandatory to all new starters in the company. Refresher training sessions are delivered by the Compliance Team approximately every 3-4 months, encompassing any new security working practices, managing evolving threats, and communicating emerging best practice. All such training includes specific instruction on the security of mobile devices and protection against malware, and the acceptable use of mobile assets. Records of training are retained.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	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.	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?			x	UKCloud does not permit any mobile device access to the UKCloud customer or management platforms. Mobile access may only be used to consume internal UKCloud corporate resources and such mobile access is subject to policies and procedures that include a whitelist of approved application stores. Various requirements are documented in UKCloud's Acceptable Use Policy and Mobile Telephone Policy.
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			x	N/A - UKCloud does not prepare applications for mobile device use.
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	x			UKCloud maintains a BYOD Policy in place which defines acceptable device(s) and eligibility requirements allowed for authorised BYOD usage.
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	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.	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)?	x			UKCloud maintains an full asset inventory, which contains details of all mobile devices which access or store UKCloud data - this includes details of the owner of each of UKCloud's mobile devices. Mobile devices are also added and maintained within the UKCloud Configuration Management Database. Each mobile device is assigned a unique asset tag number - this is done in accordance with UKCloud's Asset Management Policy and Asset Management Process. The capabilities of Microsoft Office 365 "Security and Compliance Center" provides visibility of the status of all UKCloud-owned mobile devices, and is accessible by authorised members of the UKCloud IT Team.
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			x	N/A - UKCloud does not use mobile devices to store, transmit or process customer data.
Mobile Security *Encryption*	MOS-11	MOS-11.1	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.	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?			x	N/A - UKCloud does not permit the use of mobile devices for accessing sensitive data. UKCloud-provided mobile devices are installed with appropriate encryption technology as part of their standard configuration (e.g. Windows BitLocker, Android encryption, Apple AES-256), as documented in UKCloud's Acceptable Use Policy and Mobile Telephone Policy.

Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	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).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	Whilst UKCloud does not operate a dedicated centralised device management capability, control of UKCloud-owned mobile devices and authorised BYOD devices is achieved using the features of Microsoft Office 365 "Security and Compliance Center" as well as vendor-specific asset location and remote wiping technologies. As recorded in UKCloud's Acceptable Use Policy and Mobile Telephone Policy, it is strictly prohibited for users to attempt to circumvent security controls on mobile devices (e.g. using jailbroken devices or downloading of unauthorised applications). This is communicated within security induction training, which is mandatory for all new starters in the company. Refresher training sessions are delivered by the Compliance Team approximately every 3-4 months, encompassing any new security working practices, managing evolving threats, and communicating emerging best practice. All such training includes specific instruction on the security of mobile devices. Records of training are retained.
		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?		x		
Mobile Security *Legal*	MOS-13	MOS-13.1	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.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	UKCloud does not permit mobile devices (including BYOD) access to any customer environments or UKCloud management platforms, in accordance with UKCloud's Acceptable Use Policy and Mobile Telephone Policy. Mobile access may only be used to consume internal UKCloud corporate resources and such mobile access is subject to policies and procedures that include an accepted acceptable use policy. UKCloud's BYOD Policy is in place which includes clarifications of the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy clearly states the expectations regarding no liability for the loss of non-company data in the case that a UKCloud-initiated wipe of the mobile device is 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?	x			
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	x			UKCloud-owned devices are configured to auto lock after a period of 5 minutes. Devices have password policies set via Active Directory Technical controls. These requirements are documented in the Acceptable Use Policy, Mobile Telephone Policy and BYOD Policy. Non-UKCloud BYOD mobile devices are required to be configured to auto-lock after a short period of activity, and BYOD users are formally made aware of this requirement within security induction training, which is mandatory for all new starters.
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	x			Due to the limited use of mobile devices by UKCloud, for general internet-based browsing and applications only, the Acceptable Use Policy and Mobile Telephone Policy require that all mobile device users are aware of upgrades and patches as soon as they become available, and that these are deployed to their devices without delay.
Mobile Security *Passwords*	MOS-16	MOS-16.1	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.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	x			UKCloud does not permit any mobile device access to the UKCloud customer or management platforms, systems or data, as per BYOD Policy. Mobile access may only be used to consume internal UKCloud corporate resources only via basic internet connectivity (web-based applications). All UKCloud personnel and contractors receive formal training on the requirements to identify the security features, update options, cloud-based backup capabilities etc relevant to any BYOD assets they may use, and reinforcing the web-based applications which can be used.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	x			
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	x			
Mobile Security *Policy*	MOS-17	MOS-17.1	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).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	UKCloud does not permit any mobile device access to the UKCloud customer or management platforms, systems or data, as per the Acceptable Use Policy and Mobile Telephone Policy. Mobile access may only be used to consume internal UKCloud corporate resources only via basic internet connectivity (web-based applications). All UKCloud personnel and contractors receive formal training on the requirements to identify the security features, update options, cloud-based backup capabilities etc relevant to any BYOD assets they may use, and reinforcing the web-based applications which can be used.
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	x			
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	x			
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	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.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	x			All mobile devices, whether company-owned and issued, or an authorised BYOD-asset, are required to authorise the administrative capabilities of Microsoft Office 365 "Security and Compliance Center". This allows for authorised UKCloud corporate IT administrators to initiate a remote wipe in the event of a device being reported as lost or stolen. Further details: https://docs.microsoft.com/en-us/office365/securitycompliance/
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	x			
Mobile Security *Security Patches*	MOS-19	MOS-19.1	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.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	x			UKCloud requires all users to update their software in line with applicable policies: UKCloud's Acceptable Use Policy, Mobile Telephone Policy and BYOD Policy.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	x			
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	x			UKCloud's BYOD Policy clearly communicates to personnel which systems and servers are permitted to be accessed and activities undertaken from a non-UKCloud owned asset. Access to any UKCloud core cloud platforms and customer environments is strictly prohibited from any BYOD asset. UKCloud maintains full records of individuals who are authorised to use BYOD assets for non-sensitive, non-critical internal business activities only.
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	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.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			Formal records of all applicable authorities, regulatory bodies, law enforcement agencies, data protection authorities and CERTs (Computer Emergency Response Teams) are maintained by UKCloud's Compliance and Commercial Teams. These are reviewed on at least an annual basis in order to ensure that they are current.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	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.	Do you have a documented security incident response plan?	x			UKCloud maintains a documented security incident response framework as part of its ISO27001-certified Information Security Management System. This is documented in the Security Incident Management Policy and Security Incident Management Process. Whilst the UKCloud security incident response plans have been designed and implemented to work with multi-tenancy platforms, customers can request UKCloud to follow specific communication and escalation plans. It is for each customer to design, implement and manage the configuration and operation of their own virtualised environments in a way which minimises or eliminates the effects of a security incident. UKCloud explains the applicable security incident roles and responsibilities for itself and its customers within the RMADS (Risk Management and Accreditation Documentation Set) for each service, and the SISP (System Interconnect Security Policy) which is referred to in each customer contract.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	x			
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	x			
		SEF-02.4		Have you tested your security incident response plans in the last year?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	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.	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?	x			UKCloud monitors its cloud platforms using an accredited external protective monitoring service (Cumulo, provided by e2-assure) which meets the requirements of (the former) NCSC Guide GPG13 for the protective monitoring of ICT systems, and identifies events and alerts against Protective Monitoring Controls (PMC) 1-12. The SIEM which feeds this activity merges data from multiple sources. UKCloud is responsible for the logging and protective monitoring of its core platforms, upon which all customer virtual environments are dependent, and can identify incoming and outgoing traffic and transactions to and from the perimeter of each customer's virtual environment. However, each customer remains responsible for providing an appropriate protective monitoring service to protect data and transactions within their own virtual data centre. This demarcation is outlined within the supporting RMADS (Risk Management and Accreditation Documentation Set) documentation which is provided for each individual UKCloud service.
		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?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	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.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	x			UKCloud operates a Customer Forensic Readiness Process. UKCloud regularly works alongside individual UK public sector customers to ensure that incident response plans and forensic investigation activities can be undertaken in a manner which can produce legally admissible data for legislative proceedings. UKCloud can assist its customers by extracting specific log and event records to support their own forensic investigations. As such, the methods of extraction and preservation are discussed and agreed with a customer on an individual case by case basis. In most cases, and subject to be notified of the need to freeze data within an acceptable timeframe, it will be possible to extract, duplicate and freeze data for a specific customer without there being any impact upon other cloud customers. UKCloud is able to demonstrate that there is robust separation between individual customers within its environments. This is regularly validated by comprehensive ITSHC/CHECK security tests undertaken by an independent testing organisation at least once a year.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	x			
		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?	x			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	x			UKCloud continually monitors, quantifies and analyses information on all security incidents, so that security controls can be updated, enhanced or implemented in a more secure way in order to prevent their recurrence. Each individual incident is comprehensively documented as either an internal security incident, or an external incident if it affects one or more UKCloud customers. All operational incidents are subject to the formal review by the UKCloud's FIRST (Focused Incident Response Security Team) and by Senior Management review as part of the ISO27001-certified Information Security Management System. This is documented in the Security Incident Management Policy and Security Incident Management Process. UKCloud confirms that statistical information about information security related incidents can be provided to customers upon request via their Service Delivery Manager.
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	x			
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	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.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	x			UKCloud conducts formal Supplier Management activities on a regular basis, which includes cloud-based services which are provided into UKCloud. Each is subject to a formal risk assessment (as required by UKCloud's ISO27001/17/18 certifications) and supplier management activities as required by Supplier Relationship Management Policy and the Supplier Relationship Management Process. Noting the use of off-site, encrypted Office 365 backups of UKCloud emails, no external organisations with logical access to either UKCloud or customer data using cloud services. UKCloud works with two specialised suppliers in the delivery of its secure cloud services - Ark Data Centres (for data centre provision) and e2e-assure (for the provision of protective monitoring services, aligning with GPG13). Al suppliers are subject to thorough selection, including security culture, personnel clearances, device management etc. and related compliance activities prior to and during their engagements. As per UKCloud personnel, full Role Based Access Control (RBAC) is implemented in accordance with the UKCloud Access Control Policy, Systems Access Matrix. Any authorised logical access to UKCloud or customer data is only permitted from UKCloud's secure premises.
		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?	x			

Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			The UKCloud Platform is protectively monitored by an independent organisation (e2e-assure). Security Incidents are managed through the UKCloud Security Incident Process, and where applicable communicated to customers through the UKCloud Customer portal, via their dedicated Service Delivery Manager, or by the other means as recorded in the UKCloud Security Incident Reporting Matrix.
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure*	STA-03	STA-03.1	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.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			UKCloud undertakes capacity management in accordance with Capacity Management Policy and Process. Customer usage reports are available via the UKCloud Customer Portal. Each customer has a Service Delivery Manager who maintains regular contact with them to review and discuss their future capacity requirements, along with customer capacity reports that are available upon request.
		STA-03.2		Do you provide tenants with capacity planning and use reports?	X			
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			A regular rolling program of internal audits is undertaken in accordance with UKCloud's Internal Audit Policy and Internal Audit Process. The UKCloud Compliance Team consists of certified Lead Auditors and Internal Auditors. Audit activities support UKCloud's certifications for: UKCloud ISO9001:2015 UKCloud ISO20000:2011 UKCloud ISO27001:2013 UKCloud ISO27017:2015 UKCloud ISO27018:2014
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	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) • 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 • 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)	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			UKCloud will endeavour to use UK-based suppliers where possible. However, all UKCloud outsourced providers deliver their services to UKCloud from within the United Kingdom, the location from which data may be processed, stored or transmitted, so the laws of England and Wales apply. UKCloud's Commercial Team review all third-party agreements. Any third-party agreements which in any way provide access to or visibility of data or the underlying infrastructure upon which the security of data depends will include specific clauses for the protection of information and its associated assets. Supplier management activities are performed in accordance with UKCloud's Supplier Relationship Management Policy and the Supplier Relationship Management Process. UKCloud provides its customers with a detailed G-Cloud 10 Assurance Information Portfolio "Evidence Pack"upon request, which provides visibility of any applicable sub-contracted/third party delivered elements of the cloud services which are being consumed by the customer.
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			
		STA-05.5		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	X			
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			
		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?	X			
		STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	X			
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?			X	
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	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.	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?	X			Partner management activities are performed in accordance with UKCloud's Supplier Relationship Management Policy and the Supplier Relationship Management Process. On an annual basis (as a minimum) each partner is required to complete and submit an assessment form - this submission confirms their ongoing compliance with applicable standards and legislation, e.g. ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001 (Information Security Management) , Cyber Essentials, UK Data Protection Act 2018, GDPR etc.
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	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.	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)?	X			Each UKCloud supplier has a named Account Owner (a senior member of UKCloud personnel), who is responsible for monitoring the services being provided, and is the escalation point for any out-of-line situations which may arise. UKCloud's own internal monitoring systems (ScienceLogic, MoogSoft., SolarWinds) oversee and report on all technical activities undertaken by third parties, as does the externally provided protective monitoring service delivered by e2e-assure. Evidence of the management and monitoring of third party supplier risk assessments is required as an input to external assessments of UKCloud's ISO9001 (Quality Management), ISO20000 (IT Service Management) and ISO27001 (Information Security Management) certifications, undertaken regularly by Lloyd's Register. UKCloud operates a comprehensive supply chain assurance process that is designed to ensure that third party services are performing in line with agreed service levels, with formal reviews taking place on at least an annual basis. Using designated UKCloud representatives and a formal review structure helps to ensure that any inconsistences or potential conflicts are promptly identified and managed to an acceptable solution. All UKCloud suppliers undergo a thorough selection process, and regular due diligence and audit checks are conducted during the lifecycle of the service, and at least annually. These activities are undertaken in accordance with UKCloud's Supplier Relationship Management Policy and the Supplier Relationship Management Process.
		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)?	X			
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			
		STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	X			
		STA-07.8		Do you review all service level agreements at least annually?	X			
Supply Chain Management, Transparency, and Accountability *Third Party*	STA-08	STA-08.1	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.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			UKCloud operates a comprehensive supply chain assurance process that is designed to ensure that third party services are performing in line with agreed service levels, with formal reviews taking place on at least an annual basis. Using designated UKCloud representatives and a formal review structure helps to ensure that any inconsistences or potential conflicts are promptly identified and managed to an acceptable solution. All UKCloud suppliers undergo a thorough selection process, and regular due diligence and audit checks are conducted during the lifecycle of the service, and at least annually. These activities are undertaken in accordance with UKCloud's Supplier Relationship Management Policy and the Supplier Relationship Management Process.
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	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.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			In accordance with UKCloud's Supplier Relationship Management Policy and the Supplier Relationship Management Process, all third-party services provides are required to demonstrate and evidence capability and maturity with information security, confidentiality, operational stability and agreed service levels, commensurate with the service being provided to UKCloud. Each third-party provider has a named Account Owner (a senior member of UKCloud personnel), who is responsible for monitoring the services being provided, and is the escalation point for any out-of-line situations which may arise. They are also responsible for conducting formal assessments and reviews, on at least an annual basis, for all providers that they have responsibility for.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	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.	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?	X			The UKCloud Acceptable Use Policy details the acceptable uses of company assets and services, this includes complying at all times with the UKCloud Anti-Virus Policy. UKCloud utilises a number of technologies across organisational owned devices to prevent the execution of unauthorized mobile code - including Cisco Sourcefire firewalls performing content inspection of UKCloud Staff web browsing, Cisco Umbrella blocking DNS resolution of new or known malicious websites, and Cisco Advanced Malware Protection preventing threats from executing.
		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?	X			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	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.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			UKCloud has an Approved Software List and subscribes to vendor security advisories for these products. Vendor Security Advisories are assessed under the UKCloud Release Management Policy, with installation performed through the UKCloud Change Management Policy and UKCloud Patching Process. Regular scans of the UKCloud Platform are performed using Nessus (commercial product installed and operated by UKCloud), with any findings added to the UKCloud Release Management Policy. Additional regular IT Security Health Checks (ITSHC CHECK) are performed by an independent organisation. UKCloud notifies all customers of potential changes and events (including patching windows) that may impact the security or availability of their cloud services through the UKCloud Customer Portal.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	X			
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			
		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?	X			

Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	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.	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?	x			The UKCloud Acceptable Use Policy details the acceptable uses of company assets and services, this includes complying at all times with the UKCloud Anti-Virus Policy. UKCloud utilises a number of technologies across organisational owned devices to prevent the execution of unauthorized mobile code - including Cisco Sourcefire firewalls performing content inspection of UKCloud Staff web browsing, Cisco Umbrella blocking DNS resolution of new or known malicious websites, and Cisco Advanced Malware Protection preventing threats from executing, along with Protective Monitoring from an independent organisation (e2eassure).
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	x			