CAIQ v4.0.3 Pre-Fill — PortalPilot by NordScope

Last reviewed: 2026-05-04

Next review due: 2026-11-04

Q-A&A-01.1: Are audit and assurance policies, procedures, and standards established, documented, ap

Answer: Yes | SSRM: CSP-owned

Q-A&A-01.2: Are audit and assurance policies, procedures, and standards reviewed and updated at leas

Answer: Yes | SSRM: CSP-owned

Q-A&A-02.1: Are independent audit and assurance assessments conducted according to relevant stand

Answer: N/A

Q-A&A-03.1: Are independent audit and assurance assessments performed according to risk-based pla

Answer: N/A

Q-A&A-04.1: Is compliance verified regarding all relevant standards, regulations, legal/contractual, and

Answer: Yes | SSRM: CSP-owned

Q-A&A-05.1: Is an audit management process defined and implemented to support audit planning, risk

Answer: Yes | SSRM: CSP-owned

Q-A&A-06.1: Is a risk-based corrective action plan to remediate audit findings established, documented

Answer: Yes | SSRM: CSP-owned

Q-A&A-06.2: Is the remediation status of audit findings reviewed and reported to relevant stakeholders?

Answer: Yes | SSRM: CSP-owned

Q-AIS-01.1: Are application security policies and procedures established, documented, approved, comm

Answer: Yes | SSRM: CSP-owned

Q-AIS-01.2: Are application security policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-AIS-02.1: Are baseline requirements to secure different applications established, documented, and m

Answer: Yes | SSRM: CSP-owned

Q-AIS-03.1: Are technical and operational metrics defined and implemented according to business obje

Answer: Yes | SSRM: CSP-owned

Q-AIS-04.1: Is an SDLC process defined and implemented for application design, development, deployn

Answer: Yes | SSRM: CSP-owned

Q-AIS-05.1: Does the testing strategy outline criteria to accept new information systems, upgrades, and

Answer: Yes | SSRM: CSP-owned

Q-AIS-05.2: Is testing automated when applicable and possible?

Answer: Yes | SSRM: CSP-owned

Q-AIS-06.1: Are strategies and capabilities established and implemented to deploy application code in a

Answer: Yes | SSRM: CSP-owned

Q-AIS-06.2: Is the deployment and integration of application code automated where possible?

Answer: Yes | SSRM: CSP-owned

Q-AIS-07.1: Are application security vulnerabilities remediated following defined processes?

Answer: Yes | SSRM: CSP-owned

Q-AIS-07.2: Is the remediation of application security vulnerabilities automated when possible?

Answer: Yes | SSRM: CSP-owned

Q-GRC-01.1: Are information governance program policies and procedures sponsored by organizationa

Answer: Yes | SSRM: CSP-owned

Q-GRC-01.2: Are the policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-GRC-02.1: Is there an established formal, documented, and leadership-sponsored enterprise risk ma

Answer: Yes | SSRM: CSP-owned

Q-GRC-03.1: Are all relevant organizational policies and associated procedures reviewed at least annua

Answer: Yes | SSRM: CSP-owned

Q-GRC-04.1: Is an approved exception process mandated by the governance program established and

Answer: Yes | SSRM: CSP-owned

Q-GRC-05.1: Has an information security program (including programs of all relevant CCM domains) be

Answer: Yes | SSRM: CSP-owned

Q-GRC-06.1: Are roles and responsibilities for planning, implementing, operating, assessing, and impro

Answer: Yes | SSRM: CSP-owned

Q-GRC-07.1: Are all relevant standards, regulations, legal/contractual, and statutory requirements appli

Answer: Yes | SSRM: CSP-owned

Q-GRC-08.1: Is contact established and maintained with cloud-related special interest groups and other

Answer: Yes | SSRM: CSP-owned

Q-IAM-01.1: Are identity and access management policies and procedures established, documented, ap

Answer: Yes | SSRM: CSP-owned

Q-IAM-01.2: Are identity and access management policies and procedures reviewed and updated at leas

Answer: Yes | SSRM: CSP-owned

Q-IAM-02.1: Are strong password policies and procedures established, documented, approved, commu

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-02.2: Are strong password policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-IAM-03.1: Is system identity information and levels of access managed, stored, and reviewed?

Answer: Yes | SSRM: CSP-owned

Q-IAM-04.1: Is the separation of duties principle employed when implementing information system acce

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-05.1: Is the least privilege principle employed when implementing information system access?

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-06.1: Is a user access provisioning process defined and implemented which authorizes, records,

Answer: Yes | SSRM: CSP-owned

Q-IAM-07.1: Is a process in place to de-provision or modify the access, in a timely manner, of movers / l

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-08.1: Are reviews and revalidation of user access for least privilege and separation of duties con

Answer: Yes | SSRM: CSP-owned

Q-IAM-09.1: Are processes, procedures, and technical measures for the segregation of privileged acces

Answer: Yes | SSRM: CSP-owned

Q-IAM-10.1: Is an access process defined and implemented to ensure privileged access roles and rights

Answer: Yes | SSRM: CSP-owned

Q-IAM-10.2: Are procedures implemented to prevent the culmination of segregated privileged access?

Answer: Yes | SSRM: CSP-owned

Q-IAM-11.1: Are processes and procedures for customers to participate, where applicable, in granting a

Answer: N/A

Q-IAM-12.1: Are processes, procedures, and technical measures to ensure the logging infrastructure is

Answer: Yes | SSRM: CSP-owned

Q-IAM-12.2: Is the ability to disable the "read-only" configuration of logging infrastructure controlled th

Answer: Yes | SSRM: CSP-owned

Q-IAM-13.1: Are processes, procedures, and technical measures that ensure users are identifiable throu

Answer: Yes | SSRM: CSP-owned

Q-IAM-14.1: Are processes, procedures, and technical measures for authenticating access to systems,

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-14.2: Are digital certificates or alternatives that achieve an equivalent security level for system id

Answer: Yes | SSRM: CSP-owned

Q-IAM-15.1: Are processes, procedures, and technical measures for the secure management of passwo

Answer: Yes | SSRM: Shared CSP and CSC

Q-IAM-16.1: Are processes, procedures, and technical measures to verify access to data and system fu

Answer: Yes | SSRM: CSP-owned

Q-CCC-01.1: Are risk management policies and procedures associated with changing organizational as

Answer: Yes | SSRM: CSP-owned

Q-CCC-01.2: Are the policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-CCC-02.1: Is a defined quality change control, approval and testing process (with established baselin

Answer: Yes | SSRM: CSP-owned

Q-CCC-03.1: Are risks associated with changing organizational assets (including applications, systems

Answer: Yes | SSRM: Shared CSP and third party

Q-CCC-04.1: Is the unauthorized addition, removal, update, and management of organization assets res

Answer: Yes | SSRM: CSP-owned

Q-CCC-05.1: Are provisions to limit changes that directly impact CSC-owned environments and require

Answer: Yes | SSRM: CSP-owned

Q-CCC-06.1: Are change management baselines established for all relevant authorized changes on orga

Answer: Yes | SSRM: CSP-owned

Q-CCC-07.1: Are detection measures implemented with proactive notification if changes deviate from e

Answer: Yes | SSRM: CSP-owned

Q-CCC-08.1: Is a procedure implemented to manage exceptions, including emergencies, in the change

Answer: Yes | SSRM: CSP-owned

Q-CCC-08.2: Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?

Answer: Yes | SSRM: CSP-owned

Q-CCC-09.1: Is a process to proactively roll back changes to a previously known "good state" defined a

Answer: Yes | SSRM: CSP-owned

Q-BCR-01.1: Are business continuity management and operational resilience policies and procedures e

Answer: Yes | SSRM: CSP-owned

Q-BCR-01.2: Are the policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-BCR-02.1: Are criteria for developing business continuity and operational resiliency strategies and ca

Answer: Yes | SSRM: CSP-owned

Q-BCR-03.1: Are strategies developed to reduce the impact of, withstand, and recover from business di

Answer: Yes | SSRM: CSP-owned

Q-BCR-04.1: Are operational resilience strategies and capability results incorporated to establish, docu

Answer: Yes | SSRM: CSP-owned

Q-BCR-05.1: Is relevant documentation developed, identified, and acquired to support business continu

Answer: Yes | SSRM: CSP-owned

Q-BCR-05.2: Is business continuity and operational resilience documentation available to authorized st

Answer: Yes | SSRM: CSP-owned

Q-BCR-05.3: Is business continuity and operational resilience documentation reviewed periodically?

Answer: Yes | SSRM: CSP-owned

Q-BCR-06.1: Are the business continuity and operational resilience plans exercised and tested at least

Answer: Yes | SSRM: CSP-owned

Q-BCR-07.1: Do business continuity and resilience procedures establish communication with stakehold

Answer: Yes | SSRM: CSP-owned

Q-BCR-08.1: Is cloud data periodically backed up?

Answer: Yes | SSRM: CSP-owned

Q-BCR-08.2: Is the confidentiality, integrity, and availability of backup data ensured?

Answer: Yes | SSRM: CSP-owned

Q-BCR-08.3: Can backups be restored appropriately for resiliency?

Answer: Yes | SSRM: CSP-owned

Q-BCR-09.1: Is a disaster response plan established, documented, approved, applied, evaluated, and m

Answer: Yes | SSRM: CSP-owned

Q-BCR-09.2: Is the disaster response plan updated at least annually, and when significant changes occ

Answer: Yes | SSRM: CSP-owned

Q-BCR-10.1: Is the disaster response plan exercised annually or when significant changes occur?

Answer: Yes | SSRM: CSP-owned

Q-BCR-10.2: Are local emergency authorities included, if possible, in the exercise?

Answer: N/A

Q-BCR-11.1: Is business-critical equipment supplemented with redundant equipment independently loc

Answer: N/A

Q-CEK-01.1: Are cryptography, encryption, and key management policies and procedures established,

Answer: Yes | SSRM: CSP-owned

Q-CEK-01.2: Are cryptography, encryption, and key management policies and procedures reviewed and

Answer: Yes | SSRM: CSP-owned

Q-CEK-02.1: Are cryptography, encryption, and key management roles and responsibilities defined and

Answer: Yes | SSRM: CSP-owned

Q-CEK-03.1: Are data at-rest and in-transit cryptographically protected using cryptographic libraries ce

Answer: Yes | SSRM: CSP-owned

Q-CEK-04.1: Are appropriate data protection encryption algorithms used that consider data classificatio

Answer: Yes | SSRM: CSP-owned

Q-CEK-05.1: Are standard change management procedures established to review, approve, implement a

Answer: Yes | SSRM: CSP-owned

Q-CEK-06.1: Are changes to cryptography-, encryption- and key management-related systems, policies

Answer: Yes | SSRM: CSP-owned

Q-CEK-07.1: Is a cryptography, encryption, and key management risk program established and maintai

Answer: Yes | SSRM: CSP-owned

Q-CEK-08.1: Are CSPs providing CSCs with the capacity to manage their own data encryption keys?

Answer: N/A

Q-CEK-09.1: Are encryption and key management systems, policies, and processes audited with a frequ

Answer: Yes | SSRM: CSP-owned

Q-CEK-09.2: Are encryption and key management systems, policies, and processes audited (preferably

Answer: Yes | SSRM: CSP-owned

Q-CEK-10.1: Are cryptographic keys generated using industry-accepted and approved cryptographic lib

Answer: Yes | SSRM: CSP-owned

Q-CEK-11.1: Are private keys provisioned for a unique purpose managed, and is cryptography secret?

Answer: Yes | SSRM: CSP-owned

Q-CEK-12.1: Are cryptographic keys rotated based on a cryptoperiod calculated while considering infor

Answer: Yes | SSRM: CSP-owned

Q-CEK-13.1: Are cryptographic keys revoked and removed before the end of the established cryptoperi

Answer: Yes | SSRM: CSP-owned

Q-CEK-14.1: Are processes, procedures and technical measures to destroy unneeded keys defined, imp

Answer: Yes | SSRM: CSP-owned

Q-CEK-15.1: Are processes, procedures, and technical measures to create keys in a pre-activated state

Answer: N/A

Q-CEK-16.1: Are processes, procedures, and technical measures to monitor, review and approve key tr

Answer: N/A

Q-CEK-17.1: Are processes, procedures, and technical measures to deactivate keys (at the time of their

Answer: Yes | SSRM: CSP-owned

Q-CEK-18.1: Are processes, procedures, and technical measures to manage archived keys in a secure

Answer: N/A

Q-CEK-19.1: Are processes, procedures, and technical measures to use compromised keys to encrypt i

Answer: Yes | SSRM: CSP-owned

Q-CEK-20.1: Are processes, procedures, and technical measures to assess operational continuity risks

Answer: Yes | SSRM: CSP-owned

Q-CEK-21.1: Are key management system processes, procedures, and technical measures being define

Answer: Yes | SSRM: CSP-owned

Q-DCS-01.1: Are policies and procedures for the secure disposal of equipment used outside the organi

Answer: Yes | SSRM: CSP-owned

Q-DCS-01.2: Is a data destruction procedure applied that renders information recovery information imp

Answer: Yes | SSRM: CSP-owned

Q-DCS-01.3: Are policies and procedures for the secure disposal of equipment used outside the organi

Answer: Yes | SSRM: CSP-owned

Q-DCS-02.1: Are policies and procedures for the relocation or transfer of hardware, software, or data/in

Answer: Yes | SSRM: CSP-owned

Q-DCS-02.2: Does a relocation or transfer request require written or cryptographically verifiable authori

Answer: Yes | SSRM: CSP-owned

Q-DCS-02.3: Are policies and procedures for the relocation or transfer of hardware, software, or data/in

Answer: Yes | SSRM: CSP-owned

Q-DCS-03.1: Are policies and procedures for maintaining a safe and secure working environment (in off

Answer: Yes | SSRM: Shared CSP and CSC

Q-DCS-03.2: Are policies and procedures for maintaining safe, secure working environments (e.g., offic

Answer: Yes | SSRM: CSP-owned

Q-DCS-04.1: Are policies and procedures for the secure transportation of physical media established, d

Answer: N/A

Q-DCS-04.2: Are policies and procedures for the secure transportation of physical media reviewed and

Answer: N/A

Q-DCS-05.1: Is the classification and documentation of physical and logical assets based on the organi

Answer: Yes | SSRM: CSP-owned

Q-DCS-06.1: Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a

Answer: Yes | SSRM: CSP-owned

Q-DCS-07.1: Are physical security perimeters implemented to safeguard personnel, data, and informati

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-07.2: Are physical security perimeters established between administrative and business areas,

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-08.1: Is equipment identification used as a method for connection authentication?

Answer: Yes | SSRM: CSP-owned

Q-DCS-09.1: Are solely authorized personnel able to access secure areas, with all ingress and egress a

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-09.2: Are access control records retained periodically, as deemed appropriate by the organizatio

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-10.1: Are external perimeter datacenter surveillance systems and surveillance systems at all ing

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-11.1: Are datacenter personnel trained to respond to unauthorized access or egress attempts?

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-12.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-13.1: Are data center environmental control systems designed to monitor, maintain, and test tha

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-14.1: Are utility services secured, monitored, maintained, and tested at planned intervals for con

Answer: Yes | SSRM: Third-party outsourced

Q-DCS-15.1: Is business-critical equipment segregated from locations subject to a high probability of e

Answer: Yes | SSRM: Third-party outsourced

Q-DSP-01.1: Are policies and procedures established, documented, approved, communicated, enforced

Answer: Yes | SSRM: CSP-owned

Q-DSP-01.2: Are data security and privacy policies and procedures reviewed and updated at least annu

Answer: Yes | SSRM: CSP-owned

Q-DSP-02.1: Are industry-accepted methods applied for secure data disposal from storage media so inf

Answer: Yes | SSRM: Shared CSP and CSC

Q-DSP-03.1: Is a data inventory created and maintained for sensitive and personal information (at a min

Answer: Yes | SSRM: CSP-owned

Q-DSP-04.1: Is data classified according to type and sensitivity levels?

Answer: Yes | SSRM: Shared CSP and CSC

Q-DSP-05.1: Is data flow documentation created to identify what data is processed and where it is store

Answer: Yes | SSRM: CSP-owned

Q-DSP-05.2: Is data flow documentation reviewed at defined intervals, at least annually, and after any cl

Answer: Yes | SSRM: CSP-owned

Q-DSP-06.1: Is the ownership and stewardship of all relevant personal and sensitive data documented?

Answer: Yes | SSRM: Shared CSP and CSC

Q-DSP-06.2: Is data ownership and stewardship documentation reviewed at least annually?

Answer: Yes | SSRM: CSP-owned

Q-DSP-07.1: Are systems, products, and business practices based on security principles by design and

Answer: Yes | SSRM: CSP-owned

Q-DSP-08.1: Are systems, products, and business practices based on privacy principles by design and

Answer: Yes | SSRM: CSP-owned

Q-DSP-08.2: Are systems' privacy settings configured by default and according to all applicable laws ar

Answer: Yes | SSRM: CSP-owned

Q-DSP-09.1: Is a data protection impact assessment (DPIA) conducted when processing personal data a

Answer: Yes | SSRM: CSP-owned

Q-DSP-10.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-DSP-11.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: Shared CSP and CSC

Q-DSP-12.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-DSP-13.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-DSP-14.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-DSP-15.1: Is authorization from data owners obtained, and the associated risk managed, before repli

Answer: Yes | SSRM: CSP-owned

Q-DSP-16.1: Do data retention, archiving, and deletion practices follow business requirements, applica

Answer: Yes | SSRM: CSP-owned

Q-DSP-17.1: Are processes, procedures, and technical measures defined and implemented to protect s

Answer: Yes | SSRM: CSP-owned

Q-DSP-18.1: Does the CSP have in place, and describe to CSCs, the procedure to manage and respond

Answer: Yes | SSRM: CSP-owned

Q-DSP-18.2: Does the CSP give special attention to the notification procedure to interested CSCs, unles

Answer: Yes | SSRM: CSP-owned

Q-DSP-19.1: Are processes, procedures, and technical measures defined and implemented to specify a

Answer: Yes | SSRM: CSP-owned

Q-HRS-01.1: Are background verification policies and procedures of all new employees (including but n

Answer: N/A

Q-HRS-01.2: Are background verification policies and procedures designed according to local laws, reg

Answer: N/A

Q-HRS-01.3: Are background verification policies and procedures reviewed and updated at least annua

Answer: N/A

Q-HRS-02.1: Are policies and procedures for defining allowances and conditions for the acceptable use

Answer: Yes | SSRM: CSP-owned

Q-HRS-02.2: Are the policies and procedures for defining allowances and conditions for the acceptable

Answer: Yes | SSRM: CSP-owned

Q-HRS-03.1: Are policies and procedures requiring unattended workspaces to conceal confidential data

Answer: Yes | SSRM: CSP-owned

Q-HRS-03.2: Are policies and procedures requiring unattended workspaces to conceal confidential data

Answer: Yes | SSRM: CSP-owned

Q-HRS-04.1: Are policies and procedures to protect information accessed, processed, or stored at remo

Answer: Yes | SSRM: CSP-owned

Q-HRS-04.2: Are policies and procedures to protect information accessed, processed, or stored at remo

Answer: Yes | SSRM: CSP-owned

Q-HRS-05.1: Are return procedures of organizationally-owned assets by terminated employees establis

Answer: N/A

Q-HRS-06.1: Are procedures outlining the roles and responsibilities concerning changes in employmen

Answer: N/A

Q-HRS-07.1: Are employees required to sign an employment agreement before gaining access to organ

Answer: N/A

Q-HRS-08.1: Are provisions and/or terms for adherence to established information governance and sec

Answer: N/A

Q-HRS-09.1: Are employee roles and responsibilities relating to information assets and security docum

Answer: Yes | SSRM: CSP-owned

Q-HRS-10.1: Are requirements for non-disclosure/confidentiality agreements reflecting organizational d

Answer: Yes | SSRM: CSP-owned

Q-HRS-11.1: Is a security awareness training program for all employees of the organization established

Answer: Yes | SSRM: CSP-owned

Q-HRS-11.2: Are regular security awareness training updates provided?

Answer: Yes | SSRM: CSP-owned

Q-HRS-12.1: Are all employees granted access to sensitive organizational and personal data provided w

Answer: Yes | SSRM: CSP-owned

Q-HRS-12.2: Are all employees granted access to sensitive organizational and personal data provided w

Answer: Yes | SSRM: CSP-owned

Q-HRS-13.1: Are employees notified of their roles and responsibilities to maintain awareness and comp

Answer: Yes | SSRM: CSP-owned

Q-IPY-01.1: Are policies and procedures established, documented, approved, communicated, applied, e

Answer: Yes | SSRM: CSP-owned

Q-IPY-01.2: Are policies and procedures established, documented, approved, communicated, applied, e

Answer: Yes | SSRM: CSP-owned

Q-IPY-01.3: Are policies and procedures established, documented, approved, communicated, applied, e

Answer: Yes | SSRM: CSP-owned

Q-IPY-01.4: Are policies and procedures established, documented, approved, communicated, applied, e

Answer: Yes | SSRM: CSP-owned

Q-IPY-01.5: Are interoperability and portability policies and procedures reviewed and updated at least a

Answer: Yes | SSRM: CSP-owned

Q-IPY-02.1: Are CSCs able to programmatically retrieve their data via an application interface(s) to enab

Answer: Yes | SSRM: Shared CSP and CSC

Q-IPY-03.1: Are cryptographically secure and standardized network protocols implemented for the man

Answer: Yes | SSRM: CSP-owned

Q-IPY-04.1: Do agreements include provisions specifying CSC data access upon contract termination, a

Answer: Yes | SSRM: CSP-owned

Q-IVS-01.1: Are infrastructure and virtualization security policies and procedures established, documen

Answer: Yes | SSRM: Shared CSP and third party

Q-IVS-01.2: Are infrastructure and virtualization security policies and procedures reviewed and updated

Answer: Yes | SSRM: CSP-owned

Q-IVS-02.1: Is resource availability, quality, and capacity planned and monitored in a way that delivers r

Answer: Yes | SSRM: CSP-owned

Q-IVS-03.1: Are communications between environments monitored?

Answer: Yes | SSRM: CSP-owned

Q-IVS-03.2: Are communications between environments encrypted?

Answer: Yes | SSRM: CSP-owned

Q-IVS-03.3: Are communications between environments restricted to only authenticated and authorized

Answer: Yes | SSRM: CSP-owned

Q-IVS-03.4: Are network configurations reviewed at least annually?

Answer: Yes | SSRM: CSP-owned

Q-IVS-03.5: Are network configurations supported by the documented justification of all allowed servic

Answer: Yes | SSRM: CSP-owned

Q-IVS-04.1: Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according

Answer: Yes | SSRM: Shared CSP and third party

Q-IVS-05.1: Are production and non-production environments separated?

Answer: Yes | SSRM: CSP-owned

Q-IVS-06.1: Are applications and infrastructures designed, developed, deployed, and configured such t

Answer: Yes | SSRM: CSP-owned

Q-IVS-07.1: Are secure and encrypted communication channels including only up-to-date and approved

Answer: Yes | SSRM: CSP-owned

Q-IVS-08.1: Are high-risk environments identified and documented?

Answer: Yes | SSRM: CSP-owned

Q-IVS-09.1: Are processes, procedures, and defense-in-depth techniques defined, implemented, and ev

Answer: Yes | SSRM: Shared CSP and third party

Q-LOG-01.1: Are logging and monitoring policies and procedures established, documented, approved,

Answer: Yes | SSRM: CSP-owned

Q-LOG-01.2: Are policies and procedures reviewed and updated at least annually?

Answer: Yes | SSRM: CSP-owned

Q-LOG-02.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-LOG-03.1: Are security-related events identified and monitored within applications and the underlyin

Answer: Yes | SSRM: CSP-owned

Q-LOG-03.2: Is a system defined and implemented to generate alerts to responsible stakeholders based

Answer: Yes | SSRM: CSP-owned

Q-LOG-04.1: Is access to audit logs restricted to authorized personnel, and are records maintained to p

Answer: Yes | SSRM: CSP-owned

Q-LOG-05.1: Are security audit logs monitored to detect activity outside of typical or expected patterns

Answer: Yes | SSRM: CSP-owned

Q-LOG-05.2: Is a process established and followed to review and take appropriate and timely actions on

Answer: Yes | SSRM: CSP-owned

Q-LOG-06.1: Is a reliable time source being used across all relevant information processing systems?

Answer: Yes | SSRM: Shared CSP and third party

Q-LOG-07.1: Are logging requirements for information meta/data system events established, document

Answer: Yes | SSRM: CSP-owned

Q-LOG-07.2: Is the scope reviewed and updated at least annually, or whenever there is a change in the

Answer: Yes | SSRM: CSP-owned

Q-LOG-08.1: Are audit records generated, and do they contain relevant security information?

Answer: Yes | SSRM: CSP-owned

Q-LOG-09.1: Does the information system protect audit records from unauthorized access, modificatio

Answer: Yes | SSRM: CSP-owned

Q-LOG-10.1: Are monitoring and internal reporting capabilities established to report on cryptographic c

Answer: Yes | SSRM: CSP-owned

Q-LOG-11.1: Are key lifecycle management events logged and monitored to enable auditing and reporti

Answer: Yes | SSRM: CSP-owned

Q-LOG-12.1: Is physical access logged and monitored using an auditable access control system?

Answer: Yes | SSRM: Third-party outsourced

Q-LOG-13.1: Are processes and technical measures for reporting monitoring system anomalies and fail

Answer: Yes | SSRM: CSP-owned

Q-LOG-13.2: Are accountable parties immediately notified about anomalies and failures?

Answer: Yes | SSRM: CSP-owned

Q-SEF-01.1: Are policies and procedures for security incident management, e-discovery, and cloud fore

Answer: Yes | SSRM: CSP-owned

Q-SEF-01.2: Are policies and procedures reviewed and updated annually?

Answer: Yes | SSRM: CSP-owned

Q-SEF-02.1: Are policies and procedures for timely management of security incidents established, docu

Answer: Yes | SSRM: CSP-owned

Q-SEF-02.2: Are policies and procedures for timely management of security incidents reviewed and upd

Answer: Yes | SSRM: CSP-owned

Q-SEF-03.1: Is a security incident response plan that includes relevant internal departments, impacted

Answer: Yes | SSRM: CSP-owned

Q-SEF-04.1: Is the security incident response plan tested and updated for effectiveness, as necessary,

Answer: Yes | SSRM: CSP-owned

Q-SEF-05.1: Are information security incident metrics established and monitored?

Answer: Yes | SSRM: CSP-owned

Q-SEF-06.1: Are processes, procedures, and technical measures supporting business processes to tria

Answer: Yes | SSRM: CSP-owned

Q-SEF-07.1: Are processes, procedures, and technical measures for security breach notifications defin

Answer: Yes | SSRM: CSP-owned

Q-SEF-07.2: Are security breaches and assumed security breaches reported (including any relevant sup

Answer: Yes | SSRM: CSP-owned

Q-SEF-08.1: Are points of contact maintained for applicable regulation authorities, national and local la

Answer: Yes | SSRM: CSP-owned

Q-STA-01.1: Are policies and procedures implementing the shared security responsibility model (SSRM

Answer: Yes | SSRM: CSP-owned

Q-STA-01.2: Are the policies and procedures that apply the SSRM reviewed and updated annually?

Answer: Yes | SSRM: CSP-owned

Q-STA-02.1: Is the SSRM applied, documented, implemented, and managed throughout the supply chai

Answer: Yes | SSRM: CSP-owned

Q-STA-03.1: Is the CSC given SSRM guidance detailing information about SSRM applicability throughou

Answer: Yes | SSRM: CSP-owned

Q-STA-04.1: Is the shared ownership and applicability of all CSA CCM controls delineated according to

Answer: Yes | SSRM: CSP-owned

Q-STA-05.1: Is SSRM documentation for all cloud services the organization uses reviewed and validate

Answer: Yes | SSRM: CSP-owned

Q-STA-06.1: Are the portions of the SSRM the organization is responsible for implemented, operated, a

Answer: Yes | SSRM: CSP-owned

Q-STA-07.1: Is an inventory of all supply chain relationships developed and maintained?

Answer: Yes | SSRM: CSP-owned

Q-STA-08.1: Are risk factors associated with all organizations within the supply chain periodically revie

Answer: Yes | SSRM: CSP-owned

Q-STA-09.1: Do service agreements between CSPs and CSCs (tenants) incorporate at least the followin

Answer: Yes | SSRM: CSP-owned

Q-STA-10.1: Are supply chain agreements between CSPs and CSCs reviewed at least annually?

Answer: Yes | SSRM: CSP-owned

Q-STA-11.1: Is there a process for conducting internal assessments at least annually to confirm the cor

Answer: Yes | SSRM: CSP-owned

Q-STA-12.1: Are policies that require all supply chain CSPs to comply with information security, confid

Answer: Yes | SSRM: CSP-owned

Q-STA-13.1: Are supply chain partner IT governance policies and procedures reviewed periodically?

Answer: Yes | SSRM: CSP-owned

Q-STA-14.1: Is a process to conduct periodic security assessments for all supply chain organizations d

Answer: Yes | SSRM: CSP-owned

Q-TVM-01.1: Are policies and procedures established, documented, approved, communicated, applied,

Answer: Yes | SSRM: CSP-owned

Q-TVM-01.2: Are threat and vulnerability management policies and procedures reviewed and updated a

Answer: Yes | SSRM: CSP-owned

Q-TVM-02.1: Are policies and procedures to protect against malware on managed assets established, d

Answer: Yes | SSRM: Shared CSP and third party

Q-TVM-02.2: Are asset management and malware protection policies and procedures reviewed and upd

Answer: Yes | SSRM: CSP-owned

Q-TVM-03.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-TVM-04.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: Shared CSP and third party

Q-TVM-05.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-TVM-06.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-TVM-07.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: Yes | SSRM: CSP-owned

Q-TVM-08.1: Is vulnerability remediation prioritized using a risk-based model from an industry-recogniz

Answer: Yes | SSRM: CSP-owned

Q-TVM-09.1: Is a process defined and implemented to track and report vulnerability identification and re

Answer: Yes | SSRM: CSP-owned

Q-TVM-10.1: Are metrics for vulnerability identification and remediation established, monitored, and rep

Answer: Yes | SSRM: CSP-owned

Q-UEM-01.1: Are policies and procedures established, documented, approved, communicated, applied,

Answer: Yes | SSRM: CSP-owned

Q-UEM-01.2: Are universal endpoint management policies and procedures reviewed and updated at lea

Answer: Yes | SSRM: CSP-owned

Q-UEM-02.1: Is there a defined, documented, applicable and evaluated list containing approved service

Answer: Yes | SSRM: CSP-owned

Q-UEM-03.1: Is a process defined and implemented to validate endpoint device compatibility with opera

Answer: Yes | SSRM: CSP-owned

Q-UEM-04.1: Is an inventory of all endpoints used and maintained to store and access company data?

Answer: Yes | SSRM: CSP-owned

Q-UEM-05.1: Are processes, procedures, and technical measures defined, implemented and evaluated,

Answer: Yes | SSRM: CSP-owned

Q-UEM-06.1: Are all relevant interactive-use endpoints configured to require an automatic lock screen?

Answer: Yes | SSRM: CSP-owned

Q-UEM-07.1: Are changes to endpoint operating systems, patch levels, and/or applications managed th

Answer: Yes | SSRM: CSP-owned

Q-UEM-08.1: Is information protected from unauthorized disclosure on managed endpoints with storag

Answer: Yes | SSRM: CSP-owned

Q-UEM-09.1: Are anti-malware detection and prevention technology services configured on managed en

Answer: Yes | SSRM: CSP-owned

Q-UEM-10.1: Are software firewalls configured on managed endpoints?

Answer: Yes | SSRM: CSP-owned

Q-UEM-11.1: Are managed endpoints configured with data loss prevention (DLP) technologies and rule

Answer: N/A

Q-UEM-12.1: Are remote geolocation capabilities enabled for all managed mobile endpoints?

Answer: N/A

Q-UEM-13.1: Are processes, procedures, and technical measures defined, implemented, and evaluated

Answer: N/A

Q-UEM-14.1: Are processes, procedures, and technical and/or contractual measures defined, implemen

Answer: N/A