Question ID	Consensus Assessment Questions
AIS-01.1	Do you use industry standards (OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?
AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?
AIS-03.1	Do your data management policies and procedures require audits to verify data input and output integrity routines?
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?
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?
AAC-0.1.2	Does your audit program take into account effectiveness of implementation of security operations?
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?
AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?
AAC-02.5	Do you conduct internal audits at least annually?

AAC-02.6	Do you conduct external audits at least annually?
AAC-02.7	Are the results of internal and external audits available to tenants at their request?
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?
BCR-01.2	Do you have more than one provider for each service you depend on?
BCR-01.3	Do you provide multi-failure disaster recovery capability?
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?
BCR-01.5	Do you provide access to operational redundancy report, including the services you depend on?
BCR-01.6	Do you provide a tenant-triggered failover option?
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?
BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?
BCR-07.1	Do you have a documented policies, procedures and supporting business processes for equipment and datacenter maintenance?
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?

BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?
BCR-09.2	Does you organization conduct impact analysis pertaining to possible disruptions to the cloud service?
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?
BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?
CCC-03.2	Is documentation describing known issues with certain products/services available?
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?
CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?
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?
DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?
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.)?
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?
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)?
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?
DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?
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?

DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?
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?
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?
DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?
DCS-05.1	Can you provide tenants with your asset management policies and procedures?
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?
EKM-01.1	Do you have key management policies binding keys to identifiable owners?
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?
EKM-02.3	Do you maintain key management procedures?
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?

EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?
EKM-04.3	Do you store encryption keys in the cloud?
EKM-04.4	Do you have separate key management and key usage duties?
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?
GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?
GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2
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?
GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?

GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?
GRM-11.2	Do you make available documentation of your organization-wide risk management program?
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?
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?
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?

HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?
HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?
HRS-09.3	Do you document employee acknowledgment of training they have completed?
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?
HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?
HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?
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?

IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?
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?
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?
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accounting (AAA)?
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurace for critical business case considerations, supported by multifactor authentication?
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?
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?
IAM-08.1	Do you document how your grant, approve and enforce access restrictions to tenant/customer credentials according to the rules of least privilege?
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?

IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?
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?
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?
IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?
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?
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?
IAM-12.7	Do you allow tenants to use third-party identity assurance services?

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?
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?
IAM-12.10	Do you support the ability to force password changes upon first logon?
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)?
IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?
IVS-01.4	Are audit logs centrally stored and retained?
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?
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?
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)?
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?
IVS-04.3	Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?
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?
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?

IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?
IVS-06.4	Are all firewall access control lists documented with business justification?
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?
IVS-08.3	Do you logically and physically segregate production and non-production environments?
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?
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?
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?

IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?
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)?
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?
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?
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?
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?
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?
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?
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?

MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?
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?
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?
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?
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?

MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?
SEF-02.1	Do you have a documented security incident response plan?
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?
SEF-02.4	Have you tested your security incident response plans in the last year?
SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?
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?
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?

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?
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?
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?
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?
STA-03.2	Do you provide tenants with capacity planning and use reports?
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?
STA-05.3	Does legal counsel review all third-party agreements?
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?
STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?
STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?
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?
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?

STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?
STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?
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)?
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?
STA-07.8	Do you review all service level agreements at least annually?
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?

TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?
TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?
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?
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?
TVM-03.2	Is all unauthorized mobile code prevented from executing?

NAIRE v3.1 Detailed Changelog	
Type of Change	**Description**
Edited	Edits have been made to AIS-01.1. Included OWASP Software Assurance Maturity Model and ISO/IEC 27034 as examples.
No Change	No change to AIS-01.2.
No Change	No change to AIS-01.3.
No Change	No change to AIS-01.4.
No Change	No change to AIS-01.5.
No Change	No change to AIS-02.1.
No Change	No change to AIS- 02.2.
Shifted	HRS-11.2 has been shifted to AIS-03.1. Question has also been edited to more accurately reflect CCM control.
Edited	Edits have been made to AIS-03.2. MD5 and SHA checksums have been used as the examples.
No Change	No change to AIS-04.1.
New Question	New question added to AAC-01.1.
Shifted	AAC-02.8 has been shifted to AAC-0.1.2. Also edited for clarify.
No Change	No change to AAC-02.1.
Edited	Edits have been made to AAC-02.2. Cadence of penetration tests have been changed to align with CCM requirements.
No Change	No change to AAC-02.3.
No Change	No change to AAC-02.4.
Edited	Edits have been made to AAC-02.5. Cadence of audits have been changed to align with CCM requirements.

Edited	Edits have been made to AAC-02.6. Cadence of audits have been changed to align with CCM requirements. Changed "external" with "independent".
No Change	No change to AAC-02.7.
No Change	No change to AAC-03.1.
New Question	New question added to BCR-01.1.
Shifted	IAM-07.3 has been shifted to BCR-01.2.
Shifted	IAM-07.1 has been shifted to BCR-01.3.
Shifted	IAM-07.2 has been shifted to BCR-01.4.
Shifted	IAM-07.4 has been shifted to BCR-01.5. Edits have also been made for clarity.
Shifted	IAM-07.6 has been shifted to BCR-01.6.
Shifted	IAM-07.7 has been shifted to BCR-01.7.
No Change	No change to BCR-02.1.
New Question	New question added to BCR-03.1.
New Question	New question added to BCR-03.2.
No Change	No change to BCR-04.1.
Edited	Edits have been made to BCR-05.1. The question has been edited for clarity.
No Change	No change to BCR-06.1.
New Question	New question added to BCR-07.1.
New Question	New question added to BCR-07.2.
No Change	No change to BCR-08.1.

New Question	New question added to BCR-09.1.
New Question	New question added to BCR-09.2.
No Change	No change to BCR-10.1.
Edited	Edits have been made to BCR-11.1. 'Control' has been removed.
New Question	New question added to BCR-11.2.
Edited	Edits have been made to BCR-11.3. Changed 'redundacy mechanisms' to 'recovery mechanisms' to align with the CCM.
Shifted	BCR-07.1 has been shifted to BCR-11.4.
Edited	Changed "state in time" to "configuration"
Shifted	BCR-07.5 has been shifted to BCR-11.6.
No Change	No change to BCR-11.7.
No Change	No change to CCC-01.1.
New Question	New question added to CCC-02.1.
New Question	New question added to CCC-02.2.
New Question	New question added to CCC-03.1.
No Change	No change to CCC-03.2.
No Change	No change to CCC-03.3.
Shifted	CCC-02.1 has been shifted to CCC-03.4.
Shifted	CCC-02.2 has been shifted to CCC-03.5.
No Change	No change to CCC-03.6.
No Change	No change to CCC-04.1.

No Change	No change to CCC-05.1.
New Question	New question added to CCC-05.2.
New Question	New question added to CCC-05.3.
No Change	No change to DSI-01.1.
No Change	No change to DSI-01.2.
No Change	No change to DSI-02.1.
No Change	No change to DSI-02.2.
Edited	Edits have been made to DSI-03.1. Original example of 3TDES is wrong. Instead 3DES as per suggestion is correct.
No Change	No change to DSI-03.2.
Edited	Edits have been made to DSI-04.1. Semantic of the question has been improved.
Shifted	DSI-01.6 has been shifted to DSI-04.2.
No Change	No change to DSI-04.3.
No Change	No change to DSI-05.1.
No Change	No change to DSI-06.1.
Edited	The reference to tenant is removed as there may be cases that tenant data deletion maybe prohibited by laws (e.g., tax laws)
No Change	No change to DSI-07.2.

Edited	Edits have been made to DCS-01.1. Phrasing has been improved to align with the question. Added location/geograpghical information for critical assets.
New Question	New question added to DCS-01.2.
No Change	No change to DCS-02.1.
Shifted	DSI-01.3 has been shifted to DCS-03.1.
No Change	No change to DCS-03.2.
New Question	New question added to DCS-04.1.
Edited	Edits have been made to DCS-05.1. Language has been improved for clarity.
No Change	No change to DCS-06.1.
No Change	No change to DCS-06.2.
New Question	New question added to DCS-07.1.
No Change	No change to DCS-08.1.
No Change	No change to DCS-09.1.
No Change	No change to EKM-01.1.
No Change	No change to EKM-02.1.
No Change	No change to EKM-02.2.
No Change	No change to EKM-02.3.
No Change	No change to EKM-02.4.
No Change	No change to EKM-02.5.
No Change	No change to EKM-03.1.
No Change	No change to EKM-03.2.

No Change	No change to EKM-03.3.
No Change	No change to EKM-04.1.
No Change	No change to EKM-04.2.
No Change	No change to EKM-04.3.
No Change	No change to EKM-04.4.
No Change	No change to GRM-01.1.
No Change	No change to GRM-01.2.
New Question	New question added to GRM-02.1.
No Change	No change to GRM-02.2.
No Change	No change to GRM-03.1.
No Change	No change to GRM-04.1.
No Change	No change to GRM-04.2.
New Question	New question added to GRM-05.1.
New Question	New question added to GRM-06.1.
New Question	New question added to GRM-06.2.
No Change	No change to GRM-06.3.
No Change	No change to GRM-06.4.

No Change	No change to GRM-06.5.
No Change	No change to GRM-07.1.
No Change	No change to GRM-07.2.
No Change	No change to GRM-08.1.
No Change	No change to GRM-09.1.
No Change	No change to GRM-09.2.
No Change	No change to GRM-10.1.
Edited	Edits have been made to GRM-10.2. Risk category examples don't make sense and are removed from original question.
No Change	No change to GRM-11.1.
No Change	No change to GRM-11.2.
New Question	New question added to HRS-01.1.
New Question	New question added to HRS-01.2.
No Change	No change to HRS-02.1.
New Question	New question added to HRS-03.1.
New Question	New question added to HRS-03.2.
No Change	No change to HRS-04.1.
No Change	No change to HRS-04.2.

No Change	No change to HRS-05.1.
No Change	No change to HRS-06.1.
No Change	No change to HRS-07.1.
New Question	New question added to HRS-08.1.
New Question	New question added to HRS-08.2.
No Change	No change to HRS-09.1.
Shifted	HRS-03.1 has been shifted to HRS-09.2.
Shifted	HRS-03.2 has been shifted to HRS-09.3
Shifted	HRS-03.4 has been shifted to HRS-09.4.
Shifted	HRS-03.5 has been shifted to HRS-09.5.
No Change	No change to HRS-09.6.
Edited	Edits have been made to HRS-10.1. Language has been improved.
Edited	Edits have been made to HRS-10.2. Language has been improved.
Edited	Edits have been made to HRS-10.3. Language has been improved.
New Question	New question added to HRS-11.1.
New Question	New question added to HRS-11.2.

No Change	No change to IAM-01.1.
No Change	No change to IAM-01.2.
No Change	No change to IAM-02.1.
New Question	New question added to IAM-02.2.
New Question	New question added to IAM-02.3.
New Question	New question added to IAM-02.4.
New Question	New question added to IAM-02.5.
New Question	New question added to IAM-02.6.
No Change	No change to IAM-02.7.
New Question	New question added to IAM-03.1.
No Change	No change to IAM-04.1.
No Change	No change to IAM-04.2.
No Change	No change to IAM-05.1.
No Change	No change to IAM-06.1.
No Change	No change to IAM-06.2.
New Question	New question added to IAM-07.1.
New Question	New question added to IAM-07.2.
New Question	New question added to IAM-08.1.
New Question	New question added to IAM-08.2.

New Question	New question added to IAM-08.3.
No Change	No change to IAM-09.1.
Edited	Edits have been made to IAM-09.2. Question has been edited to incorporate providing access to users with legitimate interest.
Edited	Edits have been made to IAM-10.1. Unclear terms (e.g. 'certification') in original question. Such terms have been removed.
New Question	New question added to IAM-10.2.
Edited	Edits have been made to IAM-10.3. Edited question to align with CCM control.
Edited	Edits have been made to IAM-10.4. Unclear terms (e.g. 'certification') in original question has been removed.
No Change	No change to IAM-11.1.
No Change	No change to IAM-11.2.
No Change	No change to IAM-12.1.
No Change	No change to IAM-12.2.
No Change	No change to IAM-12.3.
No Change	No change to IAM-12.4.
No Change	No change to IAM-12.5.
No Change	No change to IAM-12.6.
No Change	No change to IAM-12.7.

No Change	No change to IAM-12.8.
No Change	No change to IAM-12.9.
No Change	No change to IAM-12.10.
No Change	No change to IAM-12.11.
Edited	Edits have been made to IAM-13.1. Significantly' has been removed.
No Change	No change to IVS-01.1.
No Change	No change to IVS-01.2.
No Change	No change to IVS-01.3.
No Change	No change to IVS-01.4.
No Change	No change to IVS-01.5.
No Change	No change to IVS-02.1.
Shifted	HRS-11.3 has been shifted to IVS-02.2.
No Change	No change to IVS-02.3.
No Change	No change to IVS-03.1.
No Change	No change to IVS-04.1.
No Change	No change to IVS-04.2.
No Change	No change to IVS-04.3.
No Change	No change to IVS-04.4.
No Change	No change to IVS-05.1.

No Change	No change to IVS-06.1.
No Change	No change to IVS-06.2.
No Change	No change to IVS-06.3.
No Change	No change to IVS-06.4.
No Change	No change to IVS-07.1.
No Change	No change to IVS-08.1.
No Change	No change to IVS-08.2.
No Change	No change to IVS-08.3.
No Change	No change to IVS-09.1.
Edited	Edits have been made to IVS-09.2. Legislative' has been substituted for 'legal'.
New Question	New question added to IVS-09.3.
Shifted	AAC-03.1 has been shifted to IVS-09.4.
No Change	No change to IVS-09.5.
No Change	No change to IVS-10.1.
No Change	No change to IVS-10.2.
No Change	No change to IVS-11.1.

No Change	No change to IVS-12.1.
No Change	No change to IVS-12.2.
No Change	No change to IVS-12.3.
No Change	No change to IVS-13.1.
No Change	No change to IVS-13.2.
No Change	No change to IPY-01.1.
No Change	No change to IPY-02.1.
No Change	No change to IPY-03.1.
Shifted	BCR-07.3 has been shifted to IPY-03.2.
No Change	No change to IPY-03.3.
Edited	Edits have been made to IPY-04.1. Mandatory requirement of CCM is reflected.
No Change	No change to IPY-04.2.
No Change	No change to IPY-05.1.
Shifted	BCR-07.4 has been shifted to IPY-05.2.
No Change	No change to IPY-05.3.
No Change	No change to MOS-01.1.

No Change	No change to MOS-02.1.
No Change	No change to MOS-03.1.
No Change	No change to MOS-04.1.
No Change	No change to MOS-05.1.
No Change	No change to MOS-06.1.
No Change	No change to MOS-07.1.
No Change	No change to MOS-08.1.
No Change	No change to MOS-09.1.
No Change	No change to MOS-10.1.
No Change	No change to MOS-11.1.
No Change	No change to MOS-12.1.
No Change	No change to MOS-12.2.
No Change	No change to MOS-13.1.
New Question	New question added to MOS-13.2.
No Change	No change to MOS-14.1.
No Change	No change to MOS-15.1.
No Change	No change to MOS-16.1.

No Change	No change to MOS-16.2.
No Change	No change to MOS-16.3.
No Change	No change to MOS-17.1.
No Change	No change to MOS-17.2.
No Change	No change to MOS-17.3.
No Change	No change to MOS-18.1.
No Change	No change to MOS-18.2.
No Change	No change to MOS-19.1.
No Change	No change to MOS-19.2.
No Change	No change to MOS-20.1.
No Change	No change to MOS-20.2.
No Change	No change to SEF-01.1.
No Change	No change to SEF-02.1.
No Change	No change to SEF-02.2.
No Change	No change to SEF-02.3.
No Change	No change to SEF-02.4.
New Question	New question added to SEF-03.1.
New Question	New question added to SEF-03.2.
No Change	No change to SEF-04.1.
No Change	No change to SEF-04.2.

No Change	No change to SEF-04.3.
No Change	No change to SEF-04.4.
No Change	No change to SEF-05.1.
No Change	No change to SEF-05.2.
No Change	No change to STA-01.1.
No Change	No change to STA-01.2.
No Change	No change to STA-02.1.
No Change	No change to STA-03.1.
No Change	No change to STA-03.2.
No Change	No change to STA-04.1.
No Change	No change to STA-05.1.
New Question	New question added to STA-05.2.
No Change	No change to STA-05.3.
No Change	No change to STA-05.4.
Shifted	AAC-03.2 has been shifted to STA-05.5.
Shifted	AAC-03.3 has been shifted to STA-05.6.
Shifted	DSI-01.4 has been shifted to STA-05.7.
Shifted	DSI-01.5 has been shifted to STA-05.8.
Shifted	DSI-01.7 has been shifted to STA-05.9.
Shifted	HRS-01.1 has been shifted to STA-05.10.
Shifted	HRS-08.3 has been shifted to STA-05.11.

No Change	No change to STA-05.12.
No Change	No change to STA-06.1.
No Change	No change to STA-07.1.
No Change	No change to STA-07.2.
No Change	No change to STA-07.3.
Shifted	BCR-09.1 has been shifted to STA-07.4.
Shifted	BCR-09.2 has been shifted to STA-07.5.
Shifted	BCR-09.3 has been shifted to STA-07.6.
Shifted	HRS-11.1 has been shifted to STA-07.7.
New Question	New question added to STA-07.8.
No Change	No change to STA-08.1.
No Change	No change to STA-08.2.
New Question	New question added to STA-09.1.
No Change	No change to STA-09.2.
No Change	No change to TVM-01.1.
No Change	No change to TVM-01.2.
No Change	No change to TVM-02.1.
No Change	No change to TVM-02.2.
No Change	No change to TVM-02.3.

No Change	No change to TVM-02.4.
No Change	No change to TVM-02.5.
New Question	New question added to TVM-02.6.
No Change	No change to TVM-03.1.
No Change	No change to TVM-03.2.