CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			The RCM Italia SDLC incorporates industry best practices, includes threat modeling and completion of a risk assessment, formal software security audits at all stages of design. RCM italia implements procedures in line with the ISO 9001 and ISO/IEC 27001 standards, whose validated and certified by an independent auditor. For further details on the controls in place, refer to the SoA of the ISMS
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			RCM Italia follows a structured code development and release process. As part of this process, all code is peer reviewed. also performs continuous post-
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			RCM Italia does not rely on software suppliers. All software is developed by RCM Italia, using a mature software development process.

		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modelling, manual code reviews, and other techniques.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			RCM Italia communicates its security and control environment to customers through industry certifications and third-party attestations. Access to data, and application solutions is provided to
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			RCM Italia conducts data integrity controls maintained through all phases including transmission, storage and processing.

Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			RCM Italia has been validated and certified by an independent auditor to confirm alignment with ISO/IEC 27001 certification standard.

Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	X			RCM Italia periodically performs internal and external audits to assess the security and compliance of its services and effectiveness of its ISMS, conform to the requirements of ISO/IEC 27001, ISO 9001 and rilevant legislation or regulations.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			RCM Italia makes its ISO 9001 and ISO/IEC 27001 certificates report available to customers. The certificates are published on the institutional website.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	X			
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Penetration tests are performed regularly by independent security firms.

		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	X			RCM ITalia undergoes several independent third party (also critical clients/suppliers) audits to test for data safety, privacy, and security as: ISO/IEC 27001, ISO 9001, AgID, others. NDA are signed by third parties before to start activities.
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	X			RCM Italia maintains an internal audits program and risk assessments
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	X			RCM Italia Security Policy prohibits sharing this information but executive Summary is available upon request or contract obligation.
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X			RCM Italia publishes and makes available its ISO/IEC 27001, ISO 9001 and other certification report online upon request. Detailed information of some confidential reports can be obtained under NDA.
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	X			Periodical project review meeting are performed to evaluate treats, vulnerabilities and takes decisions.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer data is logically segregated between tenants. RCM Italia uses data encryption mechanisms both during transmission.
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?		X		Data recovery is done for the whole application. RCM Italia implements redundancy mechanism in its systems to prevent permanent data loss.

		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			RCM Italia implements the service on qualified CSP infrastructure with primary site in Italy and secondary site in other European Community countries.
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			With Reference to ISO/IEC 27001 standard Annex 18, RCM Italia monitors relevant legislative and regulatory requirements. Have established channel with the main national authority such as the italian data protection authority and AgID. RCM Italia partecipates in network of expert, best practices sharing, specialist security forum, and professional associations
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and	Do you provide tenants with geographically resilient hosting options?	X			The service application offered in SaaS is installed on Qualified Certification Service Provider that have the characteristics of resilience and failover required by the standard organizzation.
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?		X		The secondary failover instance is located in the EU region. It is used in case of the disaster. The Provider is the same in the failover location.

Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Business Continuity policies and procedures have been developed and verified in line with ISO/IEC 27001 standards. RCM Italia performs regular testing of its business continuity plans.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	X			The services are implementd on qualified CSP infrastructure, by creating a private virtual data center. Datacenter network infrastructure is secured, monitored, and environmentally controlled.
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?	X			Data are transported only within EU. The transportation data through data centers (primary and secondary) is for backup and disaster recovery purposes only

Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			With reference to ISO/IEC 27001 Appendix A Domain 12, information System Documentation is made available internally to RCM Italia authorized personnel.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?			X	RCM Italia implements the service application on Qualified Certification Service Provider infrastructure that performs in its datacenters countermeasures to prevent or limit the impact from physical threats.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?			X	The service is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.

Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			RCM Italia implements virtual private cloud on qualified CSP that guarantee the replacement of the assigned hardware.
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			X	Service application of RCM Italia is offered as a SaaS service. Tenants do not have the ability to introduce or manage virtual machines in the this environment
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			X	
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			X	
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	X			Customers can request to export their data from the application offered as a SaaS service
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?			X	The service is implemented on Qualified CSP infrastructure that has implemented redundancies and safeguards in its datacenters to minimize the impact of service outages
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes,	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			RCM Italia makes avaible on request to its customers performace report of SLA
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		X		

		BCR-09.3	applications, business partners, and third party service providers • Understand threats to critical products and services	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			RCM Italia makes avaible on request to its customers performace report of SLA
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Policies and Procedures have been established through RCM Italia Security framework based upon ISO/IEC 27001 and ISO 9001 standard. Roles and responsabilities are explicity assigned, pubblished, and well-understood by all employees.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?	X			RCM Italia has defined and applied policies, procedure and mechanisms for data retention an storage to guarantee to its customers correct protection of all data and availability of service in accordance with result of risk assessment and with
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	X			
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	X			Recovery test is periodically performed.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			Policies and Procedures have been established through RCM Italia Security framework based upon ISO/IEC 27001, ISO 9001 standard.

		CCC-01.2	been pre-authorized by the organization's business leadership or other accountable business role or function.	Is documentation available that describes the installation, configuration, and use of products/services/features?	X			RCM Italia's application is a SaaS platform and have internal documents describing the installations and configurations.
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			RCM Italia incorporates standards of quality as part of the system development lifecycle processes.
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	RCM Italia does not generally outsource development of software.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you provide your tenants with documentation that describes your quality assurance process?	X			RCM Italia maintains an ISO 9001 certification. This is an independent validation of RCM Italia quality system and determined that RCM Italia activities comply with ISO 9001 requirements.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			Periodical release notes are 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?	X			RCM Italia has internal procedures to communicate to its customers vulnerabilities, threats likelihood and impact of its applications.
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			A specific policy is established to develop secure applications and formal process is in place. System development lifecycle incorporates industry best practices. Debugging features are available during appropriate stages.

Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			Access to product infrastructure is tightly controlled. The ability to install unapproved software is not allowed and this activity is heavily monitor.

Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		Generally, information related to RCM Italia applications and software system effort is internal documentation. Anyway, RCM Italia can provide a documentation of the continuous implementation model adopted (change management process) on request.
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			The virtual machines include tags/metadata in order to describe the data classification and purpose of the service.
		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	RCM Italia is a SaaS solution provider, and only uses virtual infrastructure in production environment on qualified CSP
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?		X		
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	X			Primary tenants data is stored in datacenter located in italy; Secondary datacenter is located in Europe region
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	X			RCM Italia follows best practice, legislation and regulation of Local Governement interoperability standards for data management

		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?			X	Tenants are not allowed to choose the geographical location
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			RCM Italia implements the service offered and collects tenants data at primary DataCenter of the qualified CSP located in ITALY and secondary site in EU region. RCM Italia will
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X			
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			RCM Italia uses qualified CSP that allow access to secure cloud infrastructures (e.g. SSH, VPN).
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Interactions are generally made via API request and requests are encrypted.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	X			RCM Italia has defined and implemented a data classification and treatment policy that sets the baseline requirements to address the
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	X			
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Production data are not replicated into non-production environments. if necessary it is mandatory the explicit permission of the customer. Production and non-production environments are segregated. No-production data are used in development or test environment.

Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			RCM Italia organizational model establishes all role and responsabilities related to service and information security. Customer responsabilities are documented in our term of service, privacy policy and related documents. Accetpable user policy has been communicated to all internal and external personnel and implemented.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			RCM Italia performs secure deletion upon termination. By agreement, the tenant determines the mode of destruction.
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Tenant may exit the service according to the Terms of our Service Agreement. See the Term of Service and Service Manual for details.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			RCM Italia implements the service offered and collects tenant data at primary DataCenter of the qualified CSP,
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	X			
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	X			RCM Italia implements the service offered and collects tenant data at primary DataCenter of the qualified CSP, which ensures that physical security controls are compliant with ISO/IEC 27001.

Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			RCM Italia implements the service offered and collects tenant data at primary DataCenter of the qualified CSP which ensures that manages equipment identification are compliant with ISO/IEC 27001.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?	X			Tenants are not allowed to designate which physical region their data will be located. The primary site is located in ITALY while the secondary site, of the same CSP is located within EU. Business Continuity Policies and Plans have been developed and tested in alignment with ISO/IEC 27001 standards RCM Italia will not move tenants' content from the region without notifying the customer unless required to comply with the law or requests of governmental entities.

Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	X			RCM Italia is a SaaS provider that implements the application offered and collects tenant data at primary DataCenter of the qualified CSP. Both are aligned with ISO/IEC 27001 standard, follows the Annex A domain 8.
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			RCM Italia implements the service offered and collects the data of the holders at the primary Data Center of the qualified CSP, which has been validated and certified by an thirdy part to confirm alignment with ISO/IEC 27001 certification standard. Refer to Annex A, domain 11 for further details.
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			In alignment with ISO/IEC 27001 standard, team members complete periodic security education, based on their role. Compliance audits are periodically performed to validate that team members understand and follow the established policies.

Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	X			RCM Italia implements the service application (SaaS in Private Cloud) offered and collects the data of the holders at the primary Data Center of the qualified CSP which located the primary and secondary sites within EU.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			RCM Italia implements the service application (SaaS in Private Cloud) and collects the data of the holders at the primary Data Center of the qualified CSP, which provides high levels of physical and network security and maintain various levels of audited (internal and extrernal) security mechanism, including ISO/IEC 27001 compliance and other standards.

Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			RCM Italia has defined a key management process to support encryption of data in transit and at rest.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	X			
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			
		EKM-02.3		Do you maintain key management procedures?		X		
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?		X		
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			RCM Italia uses an internal framework to create and manage encryption keys. Key management process are reviewed periodically in accordance with ISO/IEC 27001 standard. They are also used organization CA that provide cryptographic and symmetric and asymmetric key management services.

Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			In accordance with the data classification and treatment policy, information are stored encrypted to protect their integrity and confidentiality. RCM Italia leverages several technologies to ensure stored data is encrypted at rest. Additionally, certain databases or field-level information is encrypted at rest, based on the sensitivity of the information.
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			RCM Italia leverages advantage of the robust machine image protections. If necessary, virtual machines are encrypted during transport
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?		X		
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			RCM Italia is certified for ISO/IEC 27001 and follows the Annex A 10 domain. A specifc security policy for data encryption is defined.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			RCM Italia leverages open encryption standards.
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Key are maintained using qualified CSP infrastructure.
		EKM-04.3		Do you store encryption keys in the cloud?	X			Private keys are stored in separate vault storages.
		EKM-04.4		Do you have separate key management and key usage duties?		X		RCM Italia manages all encryption keys created.
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			In alignment with ISO 27001 standards, RCM Italia maintains system baselines for critical component.
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			

		GRM-01.3	change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?			X	RCM Italia delivers your application as a multi-tenant SaaS offering so, it does not provide clients with their own virtual machines images.
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		X		RCM Italia provides continuous monitoring for tenants.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Risk assessments occur at least annually.
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			The ISMS has established, implemented, monitored, maintained and improved considering the characteristics of the business, the organization, its location, asset and technology, legal and relulatory environment and stakeholders needs In accordance with ISO/IEC 27001 standard, compliance audits are performed so that employees understand and follow the established policies.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			RCM Italia is ISO/IEC 27001 certified by external auditors. This certification is available on website.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	X			ISMS is reviewed on an annual basis.

Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	X			RCM Italia manages third-party relationships in alignment with ISO 27001 standard. As part of ISO/IEC 27001 certification, controls and policies for service providers are reviewed.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	X			RCM Italia has established information security framework and policies which have integrated the ISO/IEC 27001 certifiable framework based on ISO/IEC 27002 controls. Also, RCM Italia leveragnes best practices and security guidance from a wid variety of sources.
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			RCM Italia information security and privacy policies align with industry standards. Contractual relationship are in place to verify and monitor supplier compliance with industry standards.
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			Evidence arising from internal audit and third party ISO 27001 activities are documented.

		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			RCM Italia compliance information are published on our website.
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			This is established by internal policies, standards, training, and processes.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			Updates security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO/IEC 27001 standard. Risk assessments and risk management produce as output security updates and treatment plan.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Tenants are informed through the RCM Italia institutional website and by email in relation to changes regarding information security and privacy policies.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			Security policies are reviewed at least annually. The privacy policy is updated and reviewed by the internal DPO.

Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			Regular risk assessments are conducted according to ISO 31000 standard. These include likelihood and impact for all identified risk categories 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 (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	X			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder	Do you have a documented, organization-wide program in place to manage risk?	X			RCM Italia is ISO/IEC 27001 certified by external auditors. This certification is available to tenants and has different
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Data breach procedure is in place within the GDPR compliance system. Privacy Policy is aligned with industry and country requirements and is
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	X			
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Staff with a relevant role for the organization data security are subject to background checks. Employment education are performed for all employees.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			Security education for all staff on an annual basis. Multiple leves of secutity training are provided to staff, based on their roles.
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	X			Staff must acknowledge completion of training and this acknowledgment is documented and stored

		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X			All staff must sign a non-disclosure agreement, read and accept the Code of Conduct and internal regulations.
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	X			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			The internal structure of HR of RCM Italia has defined and implemented policies and procedures related to human resource security prior to,
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			A specific policy about use of mobile instruments exists, in implemented and communicated to all staff. Many protections are in place to govern access from mobile devices.

Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			All policies and procedures are reviewed on at least an annual basis.

Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			All roles and responsibilities relating to information security and environment operations are documented.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile	Do you provide documentation regarding how you may access tenant data and metadata?	X			RCM Italia has a formal access control policy that is reviewed and updated annually.RCM Italia has been validated and certified by an independent auditor to confirm alignment with ISO/IEC 27001. RCM Italioa may access tenant data only if requested by
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?		X		
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			In alignment with ISO/IEC 27001 standard, security awareness training is made available to all staff. Additional traing occur when significant upadates to policies occur, and multiple levels of security training are provided to staff, based on their roles. As RCM Italia is SaaS
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal,	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			RCM Italia implements various methods of internal communication to help employees understand their

		HRS-10.2	statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	X			individual roles and responsibilities and to communicate significant events in a timely manner. Employees receive notification on the
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	X			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	X			RCM Italia data management policies are in alignment with ISO/IEC 27001 standard. Most potential confilcts of interest would be handled through contractual agreements while service level conflicts of interest would be resolved via operational management.
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	X			RCM Italia monitors production system in place (as software and data integrity) and audit log is collected to detect unauthorized access to tenant data.
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Acces to the RCM Italia product infrastructure is limited to a small subset of staff, and the infrastructure is purpose-built to be rapidly de-provisioned, and re-provisioned in short time. Server istance configuration is managed through console, and access to console configuration files is tightly controlled. The response to identified tampering or other server-level integrity question is a re-provisioning of the machine
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			In line with ISO/IEC 27001 standard, formal policies and procedures for logical access to internal systems have been defined (granted access to based on role). In particolar, access to security systems is restricted to only administrators.

		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Production systems are monitored and audit log is collected to separate server.
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			In line with ISO/IEC 27001 standard, ISMS access rights are reviewed at least annually or when users' roles changes. Refer to Annex A, domain 9 for additional details.
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			Systems access is removed within three business days as when change in the user's role takes place or when access is no longer required.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	X			Controls in place limit access to systems and data and ensure that access to systems or data is restricted and monitored per the RCM Italia access policy. Strong authentication and VPN access is needed prior access to cloud service infrastructure.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Activity of the HR function
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			

Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			RCM Italia is certified for ISO/IEC 27001 and follows the Annex A 6.1.2 domain on this. Access to the production system is limited only to named administrators and the audit log is collected to separate the server. If required, tenants are empowered to create and manage users of their portals (only Docueasy) and assign appropriate privileges to those users. Refer to the service agreement contractual and manual documentation
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			RCM Italia source code is stored in the version control system and access is limited to authorized members of the software development.
		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?	X			Strict authorization rules govern access to all parts of the internal RCM Italia product infrastructure.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	X			The service is deployed on the qualified CSP infrastructure providing multi-site capabilities using the DR failover offsite backup location. Disater recovery testing is part of RCM Italia normal processing.

		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	X			RCM Italia monitors the CSP infrastructure as service provider SLA fulfillment. In the event of provider failure the information about the incident is is recorded and communicated.
		IAM-07.3		Do you have more than one provider for each service you depend on?		X		RCM Italia relies on a single qualified CSP infrastructure as service provider.
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	X			Available for tenants upon request.
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?		X		RCM Italia is a SaaS platform and takes care of the disaster recovery.
		IAM-07.6		Do you provide a tenant-triggered failover option?		X		
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	X			Available for tenants upon request.

Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	X			Access is typically only granted to authorized employees can access a tentant's portale as part of supporting. If another party requires access for whatever reason, appropriate security measures would apply.
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	X			The Terms of Service identifies the data types that the service application is to process. Tenant data is classified with highest confidentiality level and access control to systems processing tenant data is restricted to named administrators only. Access is monitored and audit log collected.
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			In alignment with the certified ISO/IEC 27001 standard, RCM Italia has access control policies in place and approval is needed from the management before getting access to any assets. Any entitlment follows organizational changes.

		IAM-09.2	and/or customer (tenant) has some shared responsibility over implementation of control.	Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			Customers can appoint their administrators to manage service organization spaces and user roles as described in the service manual documentation. For this purpose, we offer one or more customer representatives administrator access to their data.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X			RCM Italia performs regular access reviews (depending on the criticality of the system). All administrators participate in periodic safety training courses and periodic access checks are performed to validate appropriate access provisioning. Access is revoked if the employee is terminated.
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	X			All user-privilege changes are recorded to task management system.
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			When necessary, security issues are communicated to tenants in accordance with appropriate confidentiality methods.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			In accordance with the ISO/IEC 27001 standard, user access rights are reviewed after any change in the status of employee (e.g., transfer or termination), and to revoke accounts and access where needed.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			RCM Italia does not offer native, is an optional feature.
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	X			
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			RCM Italia does not offer native, is an optional feature.

		IAM-12.4	• Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X		
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		X		RCM Italia's default authentication provider doesn't support multifactor authentication.
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?		X		
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?		X		
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	X			
		IAM-13.2		Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?		X		Actually, RCM Italia is not utilizing technology that could detect an attack that the virtual infrastructure.
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	X			
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			RCM Italia has IDS and Web Application Firewall in place.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			In alignment with the certified ISO/IEC 27001 standard, logs are accessible to authorized personnel only.

		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	X			RCM Italia Incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO/IEC 27001 standard, system utilities are appropriately restricted and monitored.
		IVS-01.4		Are audit logs centrally stored and retained?	X			RCM Italia stores audit logs in secure storage vaults with restricted access to the information security team
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			RCM Italia utilizes automated monitoring systems to provide a high level of service performance and availability. Alarmas are configured for key security events.
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Server images are protected from unauthorized access and any configuration changes to virtual machines are logged and collected.
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		X		RCM Italia takes care of the virtual machine integrity. Tenant do not interact with our products at the hypervisor or server infrastructure.
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			In alignment with ISO 27001 standards,RCM Italia information systems utilize internal system clocks synchronized via NTP.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			Server instances are not oversubscribed. RM Italia manages capacity and utilization data in alignment with ISO/IEC 27001 standard.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			
		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?	X			RCM Italia manages capacity and utilization data in alignment with ISO/IEC 27001 standard. Service scaling is performed in an optimized way.

		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			The systems are continuously monitored.
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	does not offer IaaS services.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Security documentation is updated in regular basis.
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			Access control lists and firewall rules are programmatically monitored against a standardized configuration baseline.

		IVS-06.4		Are all firewall access control lists documented with business justification?	X			Firewall rule sets and access control lists with business justification are documented and reviewed whenever any changes needs to be made.
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			RCM Italia implements least privilege throughout its infrastructure components. Server instances are configured to perform a particular function.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Tenants access only production but RCM Italia creates and maintain separate test environment for SaaS platform testing. (these are not separate per tenant). These are not generally available to customers: tenant can provision non production environment via requests, contractual agreement
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	

		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			RCM Italia network segmentation is aligned with ISO 27001 standards. Refer to ISO/IEC 27001 standard, Annex A. domain 13 for further detail. Physical segregation cannot be guaranteed because of the cloud environment.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			In alignment with the ISO/IEC 27001 standard, all services are protected by firewall.
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	X			
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	X			
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			

Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			RCM Italia uses always secured and encrypted communication channels when data is in transit. RCM Italia does not manage any physical servers.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Access to hypervisor features is restricted to a few employees whose roles require access and user permissions are limited to performing their job function.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Qualified CSP IaaS does not permit the use of wireless networks thus, RCM Italia SaaS Provider does not have the ability to implement wireless in the environment.
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	

Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			In alignment with the ISO/IEC 27001 standard, components that have regulatory or compliance impacts are well-designated, documented, and protected.
		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?		X		
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?				Actually, RCM Italia doesn't publish any public apis. Apis are internal use only.
						x		

Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			More information about building integrations and consuming the RCM Italia APIs is available on technical manual documentation.
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?				
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Interactions with the RCM Italia's application (e.g., API calls, login, etc.) are encrypted in transit.
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			RCM Italia's SaaS platform uses qualified CSP IaaS for virtualization.

		IPY-05.2	documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	Tenants do not interact with our products at the hypervisor or server infrastructure.
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			RCM Italia includes procedures to managing antivirus / malicious software in the training, in alignment with ISO/IEC 27001 standard.

Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			RCM Italia is ISO/IEC 27001 compliant based on ISO/IEC 27002 controls.

Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	X			Acceptable use policy prohibits the installation of non-approved applications. Are enforced minimal controls on employee mobile devices.

Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	BYOD is not permitted to connect to customer environments or to store customer data.

Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			In alignment with the certified ISO/IEC 27001 Standard. Part of the acceptable use policy.

Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?		X		

Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?		X		

Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	X			BYOD is not permitted to connect to customer environments or to store customer data.

Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			Asset inventory with the ownership of the assets is updated and reviewed regularly, in accordance with the ISO/IEC 27001 standard.

Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			A specific policy about use of mobile instruments exists, is implemented and communicated to all employees, in according with clauses and controls requirements ISO/IEC 27001. There are some minimal checks on employees' mobile devices

Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?		X		A specific policy about use of mobile instruments exists, is implemented and communicated to all employees, in according with clauses and controls requirements ISO/IEC 27001. Sensitive data is not permitted on mobile devices
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			Circumvention of built-in security controls is prohibited in the Acceptable Use policy.
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?		X		Laptops includes the preventative controls but mobile phones don't.
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	BYOD is not permitted to connect to customer environments or to store customer data.
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	

Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	

Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	X			Policy specifies that automatic/regural updates must be enabled.
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	BYOD is not permitted to connect to customer environments or to store customer data.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			X	
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			RCM Italia uses remote wipe on company-assigned devices.
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	X			

		MOS-19.2	devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	X			
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	BYOD is not permitted to connect to customer environments or to store customer data.
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			RCM Italia maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO/IEC 27001 standard.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			RCM Italia maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO/IEC 27001 standard. RCM Italia have well-established channels with the main national and European authority such as the italian Data Protection Authority.

		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	X			RCM Italia has an incident response program, plans and procedures have been developed in alignment with ISO/IEC 27001 standard.
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X		Generally, tenant involvement is not necessary.The terms of service cover roles and responsibilities. When a security incident is identified, security team immediately begin investigating to identify, track, communicate, and resolve the root cause of the incident. Security issues are communicated in accordance with appropriate confidentiality methods.
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	X			RCM Italia uses centralized log management system that merge difference data sources. Alerts for potential threats are escalated to technical team. Web Servers are monitored for traffic spike, port scanning, and other suspicious activities. Database servers log any invalid login attempts.
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X			RCM Italia application maintains automated log collection that support the investigation of incidents for tenant. Tenant related events can be queried by tenant id.

Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			RCM Italia can support valid request for specific tenant data from law enforcement. RCM Italia with KEEPeasy service offers a digital preservation service according to AgID rules, standard and applicabile regulatory requirements
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			RCM Italia can support valid request for specific tenant data from law enforcement. RCM Italia with KEEPeasy service offers a digital preservation service according to AgID rules, standard and applicabile regulatory requirements
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			From the snapshot the environment can be created for forensic purposes where focus can be one tenant only.
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?		X		RCM Italia's service offered (Keepeasy) is multi-tenant application. Data are separated via unique data keys.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			All Information security incidents are recorded and analyzes to determine impact, cause and opportunities for corrective action.
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	X			Upon request or contract obligation, RCM Italia provide statistical information about security metrics and security incidents.
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			The ISO/IEC 27001 compliance certification of RCM Italia demonstrates the controls in place to provide a secure service application including controls related to supply chain.
		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?				

Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			In alignment with the certified ISO/IEC 27001 and internal procedure, information about security incidents (if any) is communicated in accordance with appropriate confidentiality methods: directly via email or in-product notifications.
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			RCM Italia manages capacity and utilization data in alignment with ISO/IEC 27001 standard.
		STA-03.2		Do you provide tenants with capacity planning and use reports?		X		RCM Italia is a SaaS platform; capacity planning and usage reports are for internal use ony or upon request.

Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			RCM italia performs periodic indipendent reviews and assessments to verify compliance with policies, procedures, standard and applicabile regulatory requirements.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			RCM Italia for the SaaS platform uses only one qualified CSP Infrastructure. RCM Italia does not generally outsource development. However, agreements with any
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	X			
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			In alignment with the certified ISO/IEC 27001 RCM Italia ensures that appropriate security and privacy are in place.
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		In alignment with the certified ISO/IEC 27001, RCM Italia maintains all required subprocessing agreements and makes them available to clients upon request.

Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	X			RCM Italia maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. In addition, RCM Italia has selected Aruba SpA as a qualified cloud provider because of the compliance ISO/IEC 27001 and many other security standards.
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			In alignment with the certified ISO/IEC 27001, RCM italia maintains formal agreements with third party suppliers and those agreements are reviewed periodically and updated as needed are. The customer terms of services are reviewed and updated as needed are.
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X			RCM Italia ensures that its supply chain is regulated by the required contractual requirements. The security policy can provide on-site
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			
		STA-07.4		Do you review all agreements, policies, and processes at least annually?	X			Policies and Processes are reviewed annually. Agreements are reviewed upon renewal.

Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			In alignment with the certified ISO/IEC 27001, RCM Italia maintains formal agreements with third party suppliers and those agreements are reviewed periodically and updated as needed are.
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?		X		Currently, qualified CSP is the only provider on which the RCM Italia's service application depend on.
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?		X		RCM Italia provides an independent third party report and do not allow clients to perform assessments.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			RCM Italia uses independent third party to perform penetration tests and audit security hardening practises.
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	X			In alignment with the certified ISO/IEC 27001 standard,R CM Italia has anti-malware installed on virtual machines.
		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?	X			Updates are in place for new malware or virus signatures.

Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Authorized technical staff, periodically checks the operating systems software applications installed. The vulnerabilities are scanned and the necessary patches applied, as well as system updates. The services are exposed only in the connectivity ports essential for use to reduce the attack surface. All this in line with the ISO/IEC 27001 standard and annexed controls.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			RCM Italia collaborates with third-party penetration testing vendors recognized by the industry to perform regular penetration tests against the application layer.

		TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			In alignment with the certified ISO/IEC 27001, RCM Italia has defined and implemented a change management policy and procedure
		TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	X			The results of the vulnerability tests are used internally; tenants can request the report under NDA.

		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	X			In alignment with the certified ISO/IEC 27001 standard, RCM Italia follow security feeds for emerging threats and monitors upcoming patches continuously. RCM italia maintains and updates at the server istance and package level to meet internal compliance measures, in accordance with the criticality of the risks evaluated.
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?			X	In alignment with the certified ISO/IEC 27001 standard, RCM Italia has defined the patching timeline based on the criticality level of the vulnerability. When security relevant situations are potentially customer-impacting and publication is important or necessary, RCM Italia provide notification to customers through portal channels and direct communication.
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	No mobile code in use in the service at the moment.

		TVM-03.2	systems over a trusted or untrusted network and executed on a local system without explicit installation or	Is all unauthorized mobile code prevented from executing?			X	
© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your								

CCM v3.0.1 Compliance Mapping										
AICPA TSC 2009	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA TSC 2014	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	Canada PIPEDA	CCM V1.X	CIS-AWS-Foundations v1.1	COBIT 4.1	COBIT 5.0
S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	CC7.1	I.4	G.16.3, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-04		COBIT 4.1 AI2.4	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02

S3.2a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1		C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	10 (B) 11 (A+)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.3	SA-01			APO09.01 APO09.02 APO09.03 APO13.01 BAI02 DSS05
S3.4	(I3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. (I3.3.0) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. (I3.5.0) There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	PI1.2 PI1.3 PI1.5	I.4	G.16.3, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-05			DSS06.02 DSS06.04

	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	B.1	G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1	6 (B) 26 (A+)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-03	1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.12;1.11;1.13;2.1;2.4;2.7;2.8;3.1;3.2;3.3;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14	COBIT 4.1 DS5.11	APO09.01 APO09.02 APO09.03 APO13.01 DSS05.02 DSS06.06 MEA03.01 MEA03.02

S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	CC4.1		L.1, L.2, L.7, L.9, L.11	58 (B)		CO-01		COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	APO12.04 APO12.05 APO12.06 MEA02.01 MEA02.02
S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	CC4.1		L.2, L.4, L.7, L.9, L.11	58 (B) 59 (B) 61 (C+, A+) 76 (B) 77 (B)		CO-02		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	APO12.04 APO12.05 DSS05.07 MEA02.06 MEA02.07 MEA02.08 MEA03.01

		CC3.1						2.8;3.7	COBIT 4.1 ME 3.1	APO12.01 APO12.02 APO12.03 MEA03.01
								2.8;3.7		

								2.8;3.7		
								2.8;3.7		
A3.1.0 A3.3.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	CC3.1 A1.2 A1.3		K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15			RS-03			DSS04.01 DSS04.02 DSS04.03 DSS04.05
A3.4.0	(A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability									

A3.3	(A3.3) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	A1.2		K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	52 (B) 55 (A+)		RS-04			DSS04.04
A3.2.0 A3.4.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A3.4.0) Procedures exist to protect against unauthorized access to system resource.	A1.1 A1.2 A1.3	F.1	F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	9 (B) 10 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RS-08			DSS01.03 DSS01.04 DSS01.05 DSS04.03

S3.11.0 A.2.1.0	(S3.11.0) Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities. (A.2.1.0) The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	CC1.3 CC1.4 CC2.1		G.1.1	56 (B) 57 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	OP-02		COBIT 4.1 DS 9, DS 13.1	BAI08 BAI10 DSS01.01
A3.1.0 A3.2.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	CC3.1 A1.1 A1.2	F.1	F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RS-05	2.8;3.7		DSS01.03 DSS01.04 DSS01.05
A3.1.0 A3.2.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	CC3.1 A1.1 A1.2	F.1	F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8	53 (A+) 75 (C+, A+)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RS-06			DSS01.04 DSS01.05

A3.2.0 A4.1.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A4.1.0) The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	A1.1 A1.2 CC4.1		F.2.19	1 (B)		OP-04	2,1 2,1 2,1 2,1 2,1	COBIT 4.1 A13.3	BAI03.10 BAI04.03 BAI04.04 DSS03.05
A3.2.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	A1.1 A1.2	F.1	F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	54 (A+)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RS-07			DSS01.04 DSS01.05 DSS04.01 DSS04.02 DSS04.03
A3.1.0 A3.3.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	CC3.1 A1.2 A1.3		K.2			RS-02			BAI06.01 BAI10.01 BAI10.02 BAI10.03 DSS04.01 DSS04.02

A3.4.0	(A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system									
S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity, system security and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	CC3.2		G.1.1	45 (B)		OP-01	2,1	COBIT 4.1 DS13.1	APO01 APO07.01 APO07.03 APO09.03 DSS01.01
A3.3.0 A3.4.0 I3.20.0	(A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	A1.2 A1.3 I3.21		D.2.2.9	36 (B)	Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.5.2	DG-04	2.1;2.8;3.7 2.1;2.8;3.7 2.1;2.8;3.7 2.1;2.8;3.7	COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	BAI09.01 BAI09.02 BAI09.03 DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.07 MEA03.01
S3.12.0 S3.10.0	(S3.12.0) Procedures exist to maintain system components, including configurations consistent with the defined system security policies. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of	CC7.2 CC7.1 CC7.4	I.2	I.1.1, I.1.2, I.2.7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-01		COBIT 4.1 A12, A 16.1	APO01.02 APO01.06 BAI02.04 BAI06.01

S3.13.0	infrastructure and software are consistent with defined system security policies. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are									
S3.10.0 S3.13	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.1 CC7.4	C.2 I.1 I.2 I.4	C.2.4, G.4, G6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.18, I.2.22.6, I.2.7.1, I.2.13, I.2.14, I.2.17, I.2.20, I.2.22.2, I.2.22.4, I.2.22.7,	27 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-04	1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.13;2.1;2.4;2.7;2.8;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14 1.5;1.6;1.7;1.8;1.11;1.13;2.1;2.4;2.7;2.8;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14		APO07.06 APO09.03 APO09.04 APO10.01 APO10.04 APO10.05 APO11.01 APO11.02 APO11.04 APO11.05
A3.13.0 C3.16.0 I3.14.0 S3.10.0 S3.13	(A3.13.0, C3.16.0, I3.14.0, S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.1 CC7.1 CC7.1 CC7.1 CC7.4		C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7. I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I.2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-03		COBIT 4.1 PO 8.1	APO11.01 APO11.02 APO11.04 APO11.05 BAI02.04 BAI03.06 BAI03.08 BAI07.03 BAI07.05

A3.6.0 S3.5.0 S3.13.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.5.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC5.5 CC5.8 CC7.4	G.1 I.2	G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-05	2.1;2.4;2.7;2.8;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14		APO13.01 BAI06.01 BAI10 DSS05.03 DSS05.04 DSS05.05 DSS05.07 DSS06.03

A3.16.0 S3.13.0	(A3.16.0, S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.4 CC7.4		I.2.17, I.2.20, I.2.22		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-02	3.10;3.11;3.12;3.13;3.14;4.3;4.4	COBIT 4.1 A16.1, A17.6	BAI06.01 BAI06.02 BAI06.03 BAI06.04 BAI07.01 BAI07.03 BAI07.04 BAI07.05 BAI07.06
S3.8.0 C3.14.0	(S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.	CC3.1 CC3.1		D.1.3, D.2.2			DG-02	2.8;3.7 2.8;3.7 2.8;3.7 2.8;3.7 2.8;3.7 2.8;3.7	COBIT 4.1 PO 2.3, DS 11.6	APO01.06 APO03.02 APO08.01 APO09.03 APO13.01 BAI09.01 BAI09.02 BAI09.03 DSS04.07 DSS05.04 DSS05.05 DSS06.06

								2.8;3.7		
										APO01.06 APO03.01 APO03.02 APO09.01 APO09.01 BAI06.03
S3.6 I13.3.a-e	(S3.6) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (I13.3.a-e) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error	CC5.7 PI1.5	G.4 G.11 G.16 G.18 I.3 I.4	G.19.1.1, G.19.1.2, G.19.1.3, G.10.8, G.9.11, G.14, G.15.1		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-28	2.8;3.7 2.8;3.7	COBIT 4.1 DS 5.10 5.11	APO01.06 APO03.02 APO08.01 APO13.01 APO13.02 DSS05 DSS06
S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1	G.13	D.2.2			DG-03		COBIT 4.1 PO 2.3, DS 11.6	APO01.06 APO03.02 APO08.01 APO09.03 APO13.01
C3.5.0 S3.4.0 C3.21.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources. (C3.21.0) Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.	C1.3 CC5.6 C1.1		I.2.18			DG-06			APO01.06 BAI01.01 BAI03.07 BAI07.04

S2.2.0 S2.3.0 S3.8.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	CC2.3 CC3.1		C.2.5.1, C.2.5.2, D.1.3, L.7		Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.1.3	DG-01	2.8;3.7	COBIT 4.1 DS5.1, PO 2.3	APO01.06 APO03.02 APO13.01 APO13.03
C3.5.0 S3.4.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	C1.3 CC5.6		D.2.2.10, D.2.2.11, D.2.2.14,	37 (B)	Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.7.5 and 4.5.3	DG-05	2.8;3.7 2.8;3.7	COBIT 4.1 DS 11.4	APO01.06 APO13.01 BAI09.03 DSS01.01
S3.1.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified	CC3.1 CC3.1				Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-08			APO01.06 APO03.02 APO08.01 APO09.03
A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-03		COBIT 4.1 DS 12.3	APO13.01 DSS01.01 DSS01.05 DSS05.05 DSS06.03 DSS06.06

S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1	D.1	D.1.1, D.1.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-13		COBIT 4.1 DS5.7	APO13.01 DSS05.02 DSS05.03
S3.2.f C3.9.0	(S3.2.f) f. Restriction of access to offline storage, backup data, systems, and media. (C3.9.0) Procedures exist to restrict physical access to the defined system including, but not limited to: facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.1 CC5.5		F.2.18, F.2.19,		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.5	FS-06			EDM05.02 APO01.02 APO03.02 BAI02.03 BAI02.04 BAI03.09 BAI06.01

S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	D.1	D.1.1, D.2.1. D.2.2,		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.5	FS-07			APO09.03 APO10.04 APO10.05 APO13.01 DSS01.02
A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	H.6	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-01		COBIT 4.1 DS5.7, DS 12.1, DS 12.4 DS 4.9	APO13.01 DSS01.04 DSS01.05 DSS04.01 DSS04.03

A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-04		DS 12.2, DS 12.3	APO13.01 APO13.02 DSS05.05
A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	G.21	F.2.18		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-05		COBIT 4.1 DS 12.3	APO13.01 APO13.02 DSS05.05 DSS06.03

A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B) 10 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3	FS-02			APO13.01 APO13.02 DSS05.04 DSS05.05 DSS06.03
								1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.3;3.7		APO01.06 APO13.01 DSS05.04 DSS05.06 DSS06.03 DSS06.06
	(S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.7 CC5.6		L.6	38 (B) 39 (C+)		IS-19	1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;3.2 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7	COBIT 4.1 DS5.8	APO13.01 APO13.02 APO09.03 BAI06.01 BAI09.01 BAI09.02 BAI09.03

C3.12.0 S3.6.0 S3.4	(C3.12.0, S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.7 CC5.6	G.4 G.15 I.3	G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	23 (B) 24 (B) 25 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-18	1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7 1.1;1.2;1.3;1.4;1.5;1.6;1.7;1.8;1.11;1.12;2.8;3.2;3.7	COBIT 4.1 DS5.8 COBIT 4.1 DS5.10 COBIT 4.1 DS5.11	APO13.01 DSS05.02 DSS05.03 DSS06.06
								2.8;3.7 2.8;3.7 2.8;3.7 2.8;3.7		APO01.06 BAI09.02 BAI09.03
S1.1.0 S1.2.0(a-i)	(S1.1.0) The entity’s security policies are established and periodically reviewed and approved by a designated individual or group. (S1.2.0(a-i)) The entity's security policies include, but may not be limited to, the following matters:	CC3.2	L.2	L.2, L.5, L.7 L.8, L.9, L.10	12 (B) 14 (B) 13 (B) 15 (B) 16 (C+, A+) 21 (B)	Schedule 1 (Section 5), 4.7 - Safeguards	IS-04	3.10;3.11;3.12;3.13;3.14;4.3;4.4 3.10;3.11;3.12;3.13;3.14;4.1;4.2;4.3;4.4	COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3 COBIT 4.1 DS2.3 COBIT 4.1 DS11.6	APO01.06 APO03.02 APO13.01 APO13.02 BAI02.01 BAI02.03 BAI02.04

								3.10;3.11;3.12;3.13;3.14;4.3;4.4		BAI06.01 BAI10.01 BAI10.02 MEA02.01
S3.1.0 C3.14.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (C3.14.0) Procedures exist to provide that system	CC3.1 CC3.1		L.4, L.5, L.6, L.7	34 (B)	Schedule 1 (Section 5), 4.7 - Safeguards	DG-08		COBIT 4.1 PO 9.1, PO 9.2, PO 9.4, DS 5.7	EDM03.02 APO01.03 APO12.01 APO12.02 APO12.03 APO12.04 BAI09.01
S1.2.f S2.3.0	(S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	CC3.2	E.1	E.4	5 (B) 65 (B)	Schedule 1 (Section 5) 4.1 Accountability; 4.7 Safeguards, Sub 4.7.4	IS-14		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4 COBIT 4.1 DS5.5	APO01.03 APO01.04 APO01.08 DSS01.01
x1.2.	(x1.2.) The entity's system [availability, processing integrity, confidentiality and related] security policies include, but may not be limited to, the following matters:			A.1, B.1	2 (B) 3 (B) 5 (B)	Schedule 1 (Section 5), 4.1 - Accountability; 4.7 Safeguards	IS-01		COBIT 4.1 R2 DS5.2 COBIT 4.1 R2 DS5.5	APO13.01 APO13.02 APO13.03

S1.3.0	(S1.3.0) Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned. The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users The security obligations of users and the entity's security commitments to users are communicated to authorized users.	CC1.2		C.1	5 (B)	Schedule 1 (Section 5), 4.1 Safeguards, Subsec. 4.1.1	IS-02		COBIT 4.1 DS5.1	APO01.02 APO01.03 APO01.04 APO01.08 APO13.01 APO13.02 APO13.03
S1.1.0 S1.3.0 S2.3.0	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group. (S1.3.0) Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	CC3.2 CC1.2 CC2.3		B.1		Schedule 1 (Section 5) 4.1 Accountability, Subsec 4.1.4	IS-03	1.1;1.2;1.3;1.4;1.12 1.1;1.2;1.3;1.4;1.12 1.1;1.2;1.3;1.4;1.12	COBIT 4.1 DS5.2	APO01.03 APO01.04 APO13.01 APO13.02

								1.1;1.2;1.3;1.4;1.12		
S3.9 S2.4.0	(S3.9) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis. (S2.4.0) The security obligations of users and the	CC6.2 CC2.5		B.1.5		Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4	IS-06		COBIT 4.1 PO 7.7	APO01.03 APO01.08 APO07.04
			B.2 G.21 L.2	B.1.1, B.1.2, B.1.6, B.1.7.2, G.2, L.9, L.10		Schedule 1 (Section 5), 4.7 - Safeguards	RI-04		COBIT 4.1 PO 9.6	APO12 APO13.01 APO13.03
S1.1.0	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	CC3.2	B.2	B.1.33. B.1.34,			IS-05		COBIT 4.1 DS 5.2 DS 5.4	APO12 APO13.01 APO13.03 MEA03.01 MEA03.02

S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidentiality] commitments and (2)	CC3.1 CC3.3	I.1 I.4	C.2.1, I.4.1, I.5, G.15.1.3, I.3	46 (B) 74 (B)	Schedule 1 (Section 5), 4.7 - Safeguards	RI-02		COBIT 4.1 PO 9.4	APO12
S3.1	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified	CC3.1	L.2	A.1, L.1		Schedule 1 (Section 5), 4.7 - Safeguards	RI-01		COBIT 4.1 PO 9.1	EDM03.02 APO01.03 APO12
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	D.1	E.6.4		Schedule 1 (Section 5) 4.5 Limiting Use, Disclosure and Retention; 4.7 Safeguards, Subs.	IS-27			APO01.08 APO07.06 APO13.01 BAI09.03
S3.11.0	(S3.11.0) Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.	CC1.3 CC1.4	E.2	E.2	63 (B) HR-01	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3			COBIT 4.1 PO 7.6	APO07.01 APO07.05 APO07.06
S2.2.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users	CC2.2 CC2.3	C.1	E.3.5	66 (B)	Schedule 1 (Section 5) 4.7 Safeguards, Subsec. 4.7.4	HR-02		COBIT DS 2.1	APO01.03 APO13.01 APO07.06 APO09.03 APO10.01

S3.2.d	(S3.2.d) Procedures exist to restrict logical access to the system and information resources maintained in the system including, but not limited to, the following matters: d. The process to make changes and updates to	CC5.4		E.6			HR-03		COBIT 4.1 PO 7.8	APO01.02 APO07.05 APO07.06
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6		G.11, G12, G.20.13, G.20.14		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-32		COBIT 4.1 DS5.11 COBIT 4.1 DS5.5	APO01.08 APO13.01 APO13.02 DSS05.01 DSS05.02 DSS05.03 DSS05.07 DSS06.03 DSS06.06

S4.1.0	(S4.1.0) The entity's system availability, confidentiality, processing integrity and security performance is periodically reviewed and compared with the defined system availability and related security policies.	CC4.1		C.2.5		Schedule 1 (Section 5), 4.7 - Safeguards	LG-01			APO01.02 APO01.03 APO01.08 APO07.06 APO09.03 APO10.04 APO13.01 APO13.03

S1.2.f	(S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security.		B.1	B.1.5, D.1.1,D.1.3.3, E.1, F.1.1, H.1.1, K.1.2	5 (B)	Schedule 1 (Section 5) 4.1 Accountability	IS-13		COBIT 4.1 DS5.1	APO01.02 APO01.03 APO01.08 APO07.06 APO09.03 APO10.04 APO13.01 APO13.03
S1.2 S3.9	(S1.2) The entity's security policies include, but may not be limited to, the following matters: (S3.9) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC3.2 CC6.2	B.3	B.1.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2		Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4	IS-26		COBIT 4.1 DS 5.3	APO01.03 APO01.08 APO13.01 APO13.02 DSS05.04 DSS06.06
S1.2.k S2.2.0	(S1.2.k) The entity's security policies include, but may not be limited to, the following matters: k. Providing for training and other resources to support its system security policies (S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users.	CC2.2 CC2.3	E.1	E.4	65 (B)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4; 4.7 Safeguards, Subs. 4.7.4	IS-11		COBIT 4.1 PO 7.4	APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03
S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality, processing integrity and security policies and changes and updates to those policies are	CC3.2	E.1	E.4	65 (B) 66 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.4	IS-16		COBIT 4.1 PO 4.6	APO01.02 APO01.03 APO01.08 APO07.03

	communicated to entity personnel responsible for implementing them.									APO07.06 APO13.01 APO13.03
S3.3.0 S3.4.0	(S3.3.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	CC5.5 CC5.6	E.1	E.4		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-17	1.1;1.2;1.3;1.4;1.12;3.3 1.1;1.2;1.3;1.4;1.12;3.3 1.1;1.2;1.3;1.4;1.12;3.3		APO01.02 APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03 DSS05.03 DSS06.06
S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1				Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-29	1.1;1.2;1.3;1.4;1.12;2.1;2.4;2.7;3.1;3.3;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14	COBIT 4.1 DS 5.7	APO01.03 APO01.08 APO13.01 APO13.02 DSS05.03 DSS05.05

								1.1;1.2;1.3;1.4;1.12;2.1,2.4;2.7;3.1;3.3;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14		
S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		B.1	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	8 (B) 40 (B) 41 (B) 42 (B) 43 (B) 44 (C+)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4; 4.7 Safeguards, Subs. 4.7.4	IS-07	1.1;1.2;1.3;1.4;1.12;2.8;3.7 1.1;1.2;1.3;1.4;1.12;2.8;3.7	COBIT 4.1 DS 5.4	APO01.02 APO01.03 APO01.08 APO13.01 APO13.02 DSS05.04 DSS05.05 DSS05.06 DSS06.03 DSS06.06
S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1		H1.1, H1.2, G.9.15		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-30		COBIT 4.1 DS5.7	APO13.01 DSS05.02 DSS05.03 DSS05.05 DSS06.06
								1.1;1.2;1.3;1.4;1.12 1.1;1.2;1.3;1.4;1.12		APO01.03 APO01.08 APO13.01 APO13.02 DSS05.02 DSS05.04

S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1				Schedule 1 (Section 5) 4.7 Safeguards, Subs. 4.7.3(b)	IS-15	1.1;1.2;1.3;1.4;1.12	COBIT 4.1 DS 5.4	APO01.03 APO01.08 APO13.02 DSS05.04 DSS06.03
S3.13.0	(S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.4		I.2.7.2, I.2.9, I.2.10, I.2.15		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-33			APO01.03 APO01.08 APO13.02 DSS05.04 DSS06.03
S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing	CC3.1	B.1 H.2	B.1.1, B.1.2, D.1.1, E.1, F.1.1, H.1.1, K.1.1, E.6.2, E.6.3		Schedule 1 (Section 5), 4.7 - Safeguards	RI-05		COBIT 4.1 DS 2.3	APO01.03 APO01.08 APO07.06 APO10.04 APO13.02 DSS05.04 DSS05.07 DSS06.03 DSS06.06

	integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.										

S3.2.0 S4.3.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls). (S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality, processing integrity and security is assessed on a timely basis; policies are updated for that assessment.	CC3.3					IS-08 IS-12		COBIT 4.1 DS5.4	APO01.03 APO01.08 APO10.04 APO13.02 DSS05.04 DSS06.03 DSS06.06
S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).			H.2.4, H.2.5,	35 (B) 40 (B) 41 (B) 42 (B) 44 (C+)	Schedule 1 (Section 5) Safeguards, Subs. 4.7.2 and 4.7.3	IS-08		DS5.4	APO01.03 APO01.08 APO07.06 APO10.04 APO13.02 DSS05.04 DSS06.03 DSS06.06

S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).			H.2.6, H.2.7, H.2.9,	41 (B)	Schedule 1 (Section 5), 4.7 - Safeguards	IS-10	1.1;1.2;1.3;1.4;1.12;1.2;1.3;3.3 1.1;1.2;1.3;1.4;1.12;1.2;1.3;3.3 1.1;1.2;1.3;1.4;1.12;1.2;1.3;3.3	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	APO01.03 APO01.08 APO13.02 DSS05.04 DSS06.03 DSS06.06 MEA01.03
S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		H.2	E.6.2, E.6.3		Schedule 1 (Section 5), 4.7 - Safeguards	IS-09	1.1;1.2;1.3;1.4;1.12;1.2;1.3;3.3 1.1;1.2;1.3;1.4;1.12;1.2;1.3;3.3	COBIT 4.1 DS 5.4	APO01.03 APO01.08 APO13.02 DSS05.04 DSS06.03 DSS06.06 MEA01.03
S3.2.b	(S3.2.b) b. Identification and authentication of users.	CC5.3	B.1 H.5	E.6.2, E.6.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8	6 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-02	1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	APO01.03 APO01.08 APO13.02 DSS05.04 DSS06.03 DSS06.06 MEA01.03

								1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.9;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1 1.1;1.2;1.3;1.4;1.12;2.1		
S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1		H.2.16		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-34		COBIT 4.1 DS5.7	APO13.01 APO13.02 DSS05.05
S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	CC6.2	G.7 G.8 G.9 J.1 L.2	G.14.7, G.14.8, G.14.9, G.14.10,G.14.11, G.14.12, G.15.5, G.15.7, G.15.8, G.16.8, G.16.9, G.16.10, G.15.9, G.17.5, G.17.7, G.17.8, G.17.6,		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-14	2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14 2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14	COBIT 4.1 DS5.5 COBIT 4.1 DS5.6 COBIT 4.1 DS9.2	APO13.01 APO13.02 BAI10.01 BAI10.02 BAI10.03 DSS01.03 DSS02.01 DSS05.07 DSS06.05

				G.17.9, G.18.2, G.18.3, G.18.5, G.18.6, G.19.2.6, G.19.3.1, G.9.6.2, G.9.6.3, G.9.6.4, G.9.19, H.2.16, H.3.3, J.1, J.2, L.5, L.9, L.10				2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14 2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14 2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14		
								2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14 2.1;2.4;2.7;3.1;3.4;3.5;3.6;3.7;3.8;3.9;3.10;3.11;3.12;3.13;3.14		APO08.04 APO13.01 BAI06.01 BAI06.02 BAI10.03 BAI10.04
S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	CC6.2	G.7 G.8	G.13, G.14.8, G.15.5, G.16.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1	20 (B) 28 (B) 30 (B) 35 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-12	2,1	COBIT 4.1 DS5.7	APO01.08 APO13.01 APO13.02 BAI03.05 DSS01.01
A3.2.0 A4.1.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A4.1.0) The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	A1.1 A1.2 CC4.1		G.5			OP-03		COBIT 4.1 DS 3	APO01.03 APO01.08 BAI04.01 BAI04.04 BAI04.05 BAI10.01 BAI10.02

										APO01.08 APO04.02 APO04.03 APO04.04 DSS05.03 DSS06.06
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	G.2 G.4 G.15 G.16 G.17 G.18 I.3	G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-08	4,4		APO03.01 APO03.02 APO13.01 APO13.02 BAI02.01 BAI03.02 BAI03.03 BAI03.04 BAI03.05 DSS05.02 DSS06.06

										APO13.01 APO13.02 BAI02.01 BAI03.02 BAI03.03 BAI03.04 BAI03.05 DSS05.01 DSS05.03 DSS06.06
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	B.1	I.2.7.1, I.2.20, I.2.17, I.2.22.2, I.2.22.4, I.2.22.10-14, H.1.1	22 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-06		COBIT 4.1 DS5.7	APO03.01 APO03.02 APO13.01 APO13.02 DSS05.02 DSS05.05 DSS06.06

S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	G.17	G.9.2, G.9.3, G.9.13		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-09		COBIT 4.1 DS5.10	APO03.01 APO03.02 APO13.01 APO13.02 DSS05.02 DSS05.05 DSS06.06

										APO03.01 APO03.02 APO03.04 APO13.01 APO13.02 DSS05.02
								;2.8.3.7		APO13.01 APO13.02 DSS05.02 DSS05.04 DSS06.03 DSS06.06
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	D.1 B.3 F.1 G.4 G.15 G.17 G.18	E.3.1, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	40 (B) 44 (C+)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-10	3.10;3.11;3.12;3.13;3.14;4.3;4.4 3.10;3.11;3.12;3.13;3.14;4.3;4.4 3.10;3.11;3.12;3.13;3.14;4.3;4.4	COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	APO01.08 APO13.01 APO13.02 DSS02.02 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.07 DSS06.03 DSS06.06

S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	G.2 G.4 G.15 G.16 G.17 G.18 I.3	G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-08			APO03.01 APO03.02 APO13.01 APO13.02 BAI02.01 BAI03.02 BAI03.03 BAI03.04 BAI03.05 DSS05.02 DSS06.06
							-			BAI02.04 BAI03.01 BAI03.02 BAI03.03 BAI03.04 BAI03.05

							-			APO01.03 APO01.06 APO03.01 APO08.01 APO09.03 DSS04.07
							-			APO01.08 APO02.05 APO03.01 APO03.02 APO04.02 BAI02.01 BAI02.04 APO09.03
							-			APO01.08 APO02.05 APO03.01 APO03.02 APO04.02 BAI02.01 BAI02.04 APO09.03
							-			APO01.08 APO02.05 APO03.01

										APO03.02 APO04.02 BAI02.01 BAI02.04
							-			APO01.03 APO13.01 APO07.03 APO07.06 APO09.03 APO10.04

							-			APO01.04 APO01.08 APO04.02 APO13.01 APO13.02 APO13.03

							-			APO01.03 APO01.08 APO13.01 APO13.02 APO13.03

							-			APO01.03 APO01.08 APO13.01 APO13.02 APO13.03

							-			APO01.03 APO01.08 APO13.01 APO13.02 APO13.03

							-			APO01.03 APO01.08 APO13.01 APO13.02 APO13.03

							-			APO01.03 APO01.08 APO13.01 APO13.02 BAI03.07 BAI03.08

							-			APO01.03 APO01.08 APO13.01 APO13.02 BAI02.01 BAI02.04

							-			BAI06.01 BAI06.02 BAI06.04 BAI10.01 BAI10.02 BAI10.03

							-			APO03.01 APO03.02 APO04.02 APO13.01 APO13.02 BAI02.01 BAI03.03 BAI03.04 BAI03.10

							-			APO01.03 APO13.01 APO13.02 DSS05.03 DSS05.05 DSS06.06
							-			APO01.03 APO13.01 APO13.02 DSS05.03
							-			APO01.03 APO13.01 APO13.02

							-			DSS05.03 DSS05.05

							-			APO01.03 APO13.01 APO13.02 BAI06
							-			APO01.03 APO13.01 APO13.02 DSS05.03
							-			APO01.03 APO13.01 APO13.02 DSS05.01 DSS05.03
										APO01.03 APO13.01 APO13.02 DSS05.03 DSS05.05
										APO01.03 APO13.01 APO13.02

										DSS05.03 DSS05.05 DSS05.06
										APO01.03 APO13.01 APO13.02
		CC3.3								APO01.01 APO01.02 APO01.03 APO01.08 MEA03.01 MEA03.02 MEA03.03
IS3.7.0 S3.9.0	(IS3.7.0) Procedures exist to identify, report, and act upon system security breaches and other incidents. (S3.9.0) Procedures exist to provide that issues of noncompliance with system availability, confidentiality of data, processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC5.5 CC6.2	J.1	J.1.1, J.1.2	46 (B)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4; 4.8 Openness, Subs. 4.8.2	IS-22		COBIT 4.1 DS5.6	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06

A2.3.0 C2.3.0 I2.3.0 S2.3.0 S2.4 C3.6.0	(A2.3.0, C2.3.0, I2.3.0, S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S2.4) The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	CC2.3 CC2.5 C1.4 C1.5	J.1 E.1	J.1.1, E.4	5 (B) 46 (B) 48 (A+) 49 (B) 50 (B)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.3	IS-23		COBIT 4.1 DS5.6	APO01.03 APO07.06 APO07.03 APO13.01 APO13.02 DSS02.01

S2.4.0 C3.15.0	(S2.4.0) The process for informing the entity about system availability issues, confidentiality issues, processing integrity issues, security issues and breaches of the system security and for submitting complaints is communicated to authorized users. (C3.15.0) Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC2.5 CC6.2	J.1 E.1	J.1.1, J.1.2, E.4			IS-24		COBIT 4.1 DS5.6	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06
S3.9.0 C4.1.0	(S3.9.0) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis. (C4.1.0) The entity's system security, availability, system integrity, and confidentiality is periodically reviewed and compared with the defined system security, availability, system integrity, and confidentiality policies.	CC6.2 CC4.1		J.1.2	47 (B)		IS-25		COBIT 4.1 DS 4.9	DSS04.07
										APO10 APO11 DSS05.04 DSS06.03 DSS06.06

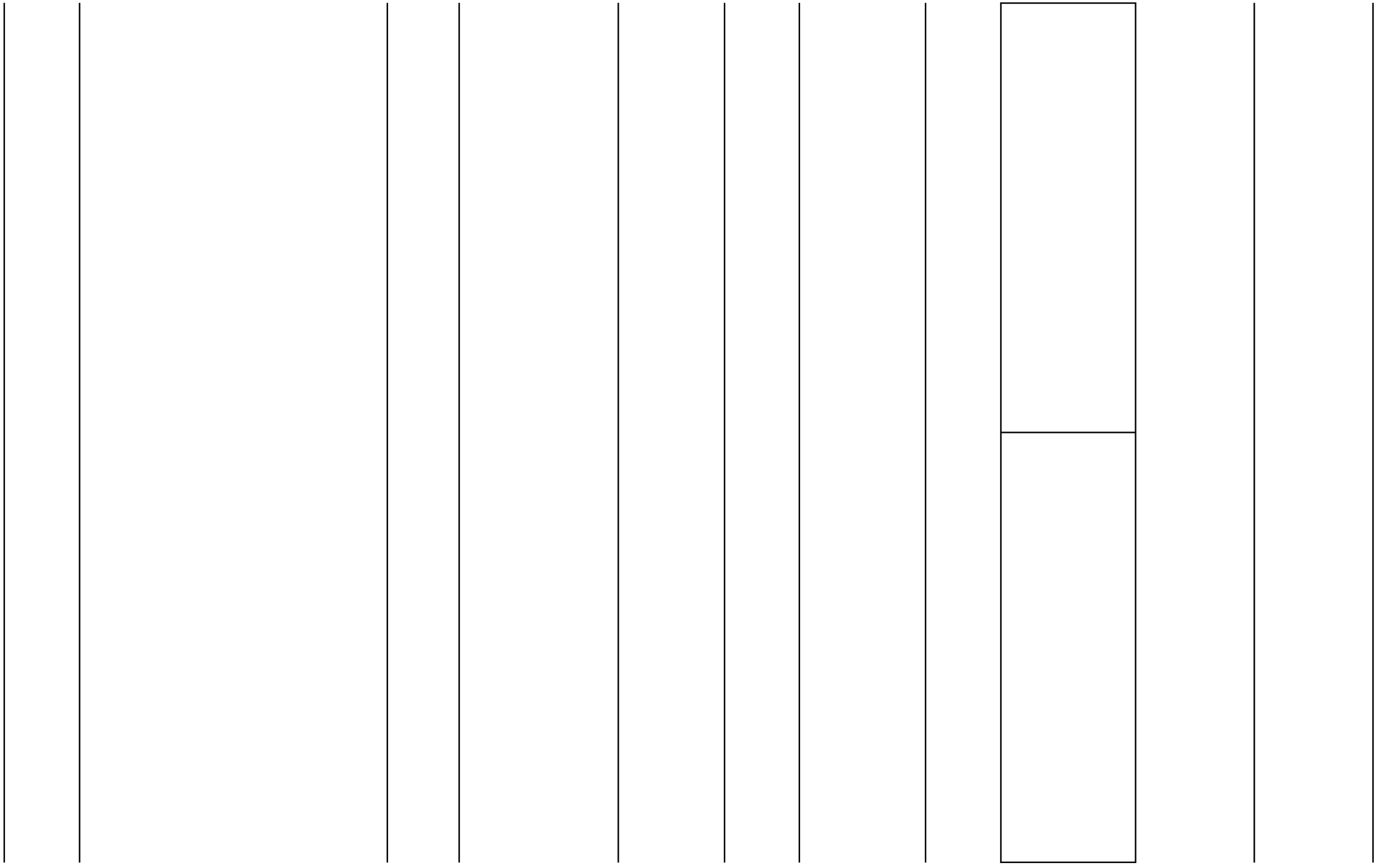
										APO09.03 APO09.04 APO10.04 APO10.05 DSS02.07
C2.2.0	(C2.2.0) The system security, availability, system integrity, and confidentiality and related security obligations of users and the entity's system security, availability, system integrity, and confidentiality and related security commitments to users are communicated to authorized users.	CC2.2 CC2.3	C.2	C.2.6, G.9.9	45 (B) 74 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-31		COBIT 4.1 DS5.10	APO01.03 APO03.01 APO03.02 APO09.03 BAI02.01 BAI02.04 BAI07.05

										MEA01 MEA02
S2.2.0 A3.6.0 C3.6.0	(S2.2.0) The availability, confidentiality of data, processing integrity, system security and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users. (A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	CC2.2 CC2.3 CC5.5 C1.4 C1.5	C.2	C.2.4, C.2.6, G.4.1, G.16.3	74 (B) 75 (C+, A+) 45 (B) 75 (C+, A+) 79 (B) 4 (C+, A+)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.3	LG-02		COBIT 4.1 DS5.11	APO09.03 APO09.05

										APO10.04 APO10.05 MEA01
					51 (B)					APO01.03 APO09.03 APO09.04 APO09.05 APO10.01 APO10.03 APO10.04

										APO09.03 MEA01 MEA02
S3.1.0 x3.1.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system [availability, processing integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.	CC2.2 CC2.3 C1.4 C1.5		L.1, L.2, L.4, L.7, L.9	76 (B) 77 (B) 78 (B) 83 (B) 84 (B) 85 (B)		CO-05		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	APO01.08 APO10.05 MEA02.01
S3.5.0	(S3.5.0) Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	CC5.8		G.7	17 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-21		COBIT 4.1 DS5.9	APO01.03 APO13.01 APO13.02 DSS05.01

S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC7.1	I.4	G.15.2, I.3	32 (B) 33 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-20		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3 COBIT 4.1 DS5.9	APO01.03 APO13.01 APO13.02 BAI06.01 BAI06.02 BAI06.03 BAI06.04 DSS01.01 DSS01.02 DSS01.03 DSS03.05 DSS05.01 DSS05.03 DSS05.07



S3.4.0 S3.10.0	(S3.4.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	CC5.6 CC7.1		G.20.12, I.2.5			SA-15			APO01.03 APO13.01 APO13.02 DSS05.01

	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of									DSS05.02 DSS05.03

COPPA	CSA Enterprise Architecture (formerly the Trusted Cloud Initiative)			CSA Guidance V3.0	ENISA IAF	95/46/EC - European Union Data Protection Directive	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	FERPA
	Domain > Container > Capability	Public	Private						
312.8 and 312.10	Application Services > Development Process > Software Quality Assurance	shared	x	Domain 10	6.03.01. (c)	Article: 27 (3)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SC-10 NIST SP 800-53 R3 SC-11 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2) NIST SP 800-53 R3 SC-12 (5) NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-14	

								NIST SP 800-53 R3 SC-17 NIST SP 800-53 R3 SC-18	
312.3, 312.8 and 312.10	BOSS > Legal Services > Contracts	shared	x	Domain 10		Article 17 (1), (2)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	
312.8 and 312.10	Application Services > Programming Interfaces > Input Validation	shared	x	Domain 10			NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-9 NIST SP 800-53 R3 SI-10 NIST SP 800-53 R3 SI-11	

312.8 and 312.10	BOSS > Data Governance > Rules for Information Leakage Prevention	shared	x	Domain 10	6.02. (b) 6.04.03. (a)	Article 17 (1), (2),(3), (4)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-8	

Title 16 Part 312	BOSS > Compliance > Audit Planning	shared	x	Domain 2, 4	6.01. (d)		NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 PL-6	
Title 16 Part 312	BOSS > Compliance > Independent Audits	shared	x	Domain 2, 4	6.03. (e) 6.07.01. (m) 6.07.01. (n)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (9)	

312,4	BOSS > Compliance > Information System Regulatory Mapping	shared	x	Domain 2, 4						

	BOSS > Operational Risk Management > Business Continuity	provider	x	Domain 7, 8	6.07. (a) 6.07. (b) 6.07. (c)	Article 17 (1), (2)	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1) NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3)	

	BOSS > Operational Risk Management > Business Continuity	provider	x	Domain 7, 8	6.07.01. (b) 6.07.01. (j) 6.07.01. (l)		NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)	
312.8 and 312.10	Infra Services > Facility Security > Environmental Risk Management	provider	x	Domain 7, 8	6.08. (a) 6.09. (c) 6.09. (f) 6.09. (g)	Article 17 (1), (2)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)	

312.8 and 312.10	SRM > Policies and Standards > Job Aid Guidelines	shared	x	Domain 7, 8		Article 17	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-9 (1) NIST SP 800-53 R3 CP-9 (3) NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 CP-10 (2) NIST SP 800-53 R3 CP-10 (3) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)	
	Infra Services > Facility Security > Environmental Risk Management	provider	x	Domain 7, 8	6.07. (d) 6.08. (a) 6.09. (a) 6.09. (b) 6.09. (d)	Article 17 (1), (2)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	
312.8 and 312.10	Infra Services > Facility Security > Environmental Risk Management	provider	x	Domain 7, 8	6.07. (d) 6.08. (a) 6.09. (a) 6.09. (b) 6.09. (d)	Article 17 (1), (2)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	

	Infra Services > Equipment Maintenance >	provider	x	Domain 7, 8	6.09. (h)	Article 17 (1)	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-2 (1) NIST SP 800-53 R3 MA-3 NIST SP 800-53 R3 MA-3 (1) NIST SP 800-53 R3 MA-3 (2) NIST SP 800-53 R3 MA-3 (3) NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 MA-6	
312.8 and 312.10	Infra Services > Facility Security > Environmental Risk Management	provider	x	Domain 7, 8	6.08. (a) 6.09. (e) 6.09. (f)	Article 17 (1), (2)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14	
	ITOS > Service Delivery > Information Technology Resiliency - Resiliency Analysis	provider	x	Domain 7, 8	6.02. (a) 6.03.03. (c) 6.07. (a) 6.07. (b) 6.07. (c)	Article 17 (1), (2)	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3	

	SRM > Policies and Standards > Operational Security Baselines	shared	x	Domain 7, 8	6.03. (c)		NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1) NIST SP 800-53 R3 SA-12	
312,3	BOSS > Data Governance > Data Retention Rules	shared	x	Domain 5	6.03. (h) 6.07.01. (c)	Article 6(1) e	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-2 (1) NIST SP 800-53 R3 CP-2 (2) NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3)	
	ITOS > IT Operation > Architecture Governance	shared	x	None	6.03. (a)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1	

							NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7)	
	ITOS > IT Operation > Architecture Governance	shared	x	None			NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)	
	ITOS > Service Support > Release Management	shared	x	None	6.03.01. (b) 6.03.01. (d)		NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)	

312.8 and 312.10	ITOS > Service Support > Configuration Management -> Software Management	shared	x	None			NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (3) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5)	

	ITOS > Service Support > Release Management	shared	x	None	6.03. (a)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1)	
312,3	BOSS > Data Governance > Data Classification	shared	x	Domain 5	6.04.03. (a)	Article 4 (1), Article 12, Article 17	NIST SP 800-53 R3 RA-2	NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 AC-4	

	BOSS > Data Governance > Handling / Labeling / Security Policy			Domain 5					
312.8 and 312.10	SRM > Cryptographic Services > Data in Transit Encryption	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1	NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1)	
312,2	BOSS > Data Governance > Handling / Labeling / Security Policy	shared	x	Domain 5	6.03.05. (b)	Article 22 Article 23	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-16 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 PE-16	99.31.(a)(1)(ii)
	SRM > Policies and Standards > Technical Standard (Data Management Security Standard)	shared	x	Domain 5	6.03. (d)			NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)	

312,4	BOSS > Data Governance > Data Ownership / Stewardship	shared	x	Domain 5		Article 4	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	
312,3	BOSS > Data Governance > Secure Disposal of Data	shared	x	Domain 5	6.03. (h)	Article 16 Article 17	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 PE-1	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 MP-6 (4) NIST SP 800-53 R3 PE-1	
	ITOS > Service Support > Configuration Management -	provider	x	Domain 8		Article 17			
312.8 and 312.10	Infra Services > Facility Security > Controlled Physical Access	provider	x	Domain 8	6.08. (a) 6.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-8	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1) NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-8 NIST SP 800-53 R3 PE-18	99.31.a.1.ii

312.3, 312.8 and 312.10	> >			Domain 8	6.05. (a)		NIST SP 800-53 R3 IA-4	NIST SP 800-53 R3 IA-3 NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-4 (4)	
312.8 and 312.10	SRM > Facility Security > Asset Handling	provider	x	Domain 8	6.08. (a) 6.09. (j)	Article 17	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-17 (1) NIST SP 800-53 R3 AC-17 (2) NIST SP 800-53 R3 AC-17 (3) NIST SP 800-53 R3 AC-17 (4) NIST SP 800-53 R3 AC-17 (5) NIST SP 800-53 R3 AC-17 (7) NIST SP 800-53 R3 AC-17 (8) NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-17	

312.8 and 312.10	BOSS > Data Governance > Secure Disposal of Data	provider	x	Domain 8	6.05. (a) 6.05. (b) 6.05. (c)	Article 17	NIST SP 800-53 R3 CM-8	NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (3) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 SC-30	
	SRM > Policies and Standards > Information Security Policies (Facility Security Policy)	provider	x	Domain 8	6.08. (a) 6.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-4 NIST SP 800-53 R3 PE-5 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1)	99.31.a.1.ii

312.8 and 312.10	SRM > Policies and Standards > Information Security Policy (Facility Security Policy)	provider	x	Domain 8	6.08. (a) 6.09. (i)	Article 17	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-18	99.31.a.1.ii
312.8 and 312.10	SRM > Policies and Standards > Information Security Policy (Facility Security Policy)	provider	x	Domain 8	6.08. (a) 6.09. (j)	Article 17	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-2 (1) NIST SP 800-53 R3 PE-16	99.31.a.1.ii

312.8 and 312.10	Infra Services > Facility Security >			Domain 8	6.08. (a) 6.09. (i)	Article 17	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1) NIST SP 800-53 R3 PE-18	99.31.a.1.ii
	SRM > Cryptographic Services > Key Management								
312.8 and 312.10	SRM > Cryptographic Services > Key Management	shared	x	Domain 2	6.04.04. (a) 6.04.04. (b) 6.04.04. (c) 6.04.04. (d) 6.04.04. (e) 6.04.05. (d) 6.04.05. (e) 6.04.08.02. (b)	Article 17	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2) NIST SP 800-53 R3 SC-12 (5) NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-17	

312.8 and 312.10	SRM > Data Protection > Cryptographic Services - Data-At-Rest Encryption, Cryptographic Services - Data-in-Transit Encryption	shared	x	Domain 2	6.04.05. (a) 6.04.05. (c)	Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-23 NIST SP 800-53 R3 SC-28 NIST SP 800-53 R3 SI-8	
	SRM > Cryptographic Services > Key Management	shared	x	Domain 11					
312.8 and 312.10	SRM > Governance Risk & Compliance > Technical Standards	shared	x	Domain 2	6.03.01. (a) 6.03.04. (a) 6.03.04. (b) 6.03.04. (c) 6.03.04. (e) 6.07.01. (o)	Article 17	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1)	

								NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SC-30	
312,1	BOSS > Operational Risk Management > Independent Risk Management	shared	x	Domain 5	6.01. (d) 6.04.03. (a)	Article 6, Article 8, Article 17 (1)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12	
312.8 and 312.10	BOSS > Human Resources Security > Roles and Responsibilities	shared	x	Domain 3, 9			NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2)	
312.8 and 312.10	SRM > InfoSec Management > Capability Mapping	shared	x	Domain 2		Article 17			99.31.(a)(1)(ii)

312.8 and 312.10	SRM > Governance Risk & Compliance > Compliance Management	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 CM-1	NIST SP 800-53 R3 CM-1	
312.8 and 312.10	SRM > Policies and Standards > Information Security Policies	shared	x	Domain 2	6.02. (e)	Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	

312.8 and 312.10	SRM > Governance Risk & Compliance >	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8	99.31(a)(i)(ii)
312.8 and 312.10	BOSS > Operational Risk Management > Risk Management Framework	shared	x	Domain 2, 4	6.03. (a)	Article 17 (1), (2)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	
312.8 and 312.10	SRM > Governance Risk & Compliance > Policy Management	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7)	

312.8 and 312.10	BOSS > Operational Risk Management > Risk Management Framework	shared	x	Domain 2, 4	6.03. (a) 6.08. (a)	Article 17 (1), (2)	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3	NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-30	
312.8 and 312.10	BOSS > Operational Risk Management > Risk Management	shared	x	Domain 2, 4		Article 17 (1), (2)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1	
312.3, 312.8 and 312.10	BOSS > Human Resources Security > Employee Termination	provider	x	Domain 2		Article 17	NIST SP 800-53 R3 PS-4	NIST SP 800-53 R3 PS-4	
312.8 and 312.10	BOSS > Human Resources Security > Background Screening	shared	x	None	6.01. (a)	Article 17	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3	
312.3, 312.8 and 312.10	BOSS > Human Resources Security > Employee Code of Conduct	shared	x	None		Article 17	NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	

312.8 and 312.10	BOSS > Human Resources Security > Roles and Responsibilities	shared	x	None		Article 17	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8	
312.8 and 312.10	Presentation Services > Presentation Platform > Endpoints - Mobile Devices - Mobile Device Management	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-6	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-17 (1) NIST SP 800-53 R3 AC-17 (2) NIST SP 800-53 R3 AC-17 (3) NIST SP 800-53 R3 AC-17 (4) NIST SP 800-53 R3 AC-17 (5) NIST SP 800-53 R3 AC-17 (7) NIST SP 800-53 R3 AC-17 (8) NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 AC-19 (1) NIST SP 800-53 R3 AC-19 (2) NIST SP 800-53 R3 AC-19 (3) NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-2 (1) NIST SP 800-53 R3 MP-4 NIST SP 800-53 R3 MP-4 (1) NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 MP-6 (4)	

312.8 and 312.10	BOSS > Compliance > Intellectual Property Protection	shared	x	Domain 3		Article 16	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)	

312.3, 312.8 and 312.10	BOSS > Human Resources Security > Roles and Responsibilities	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	99.31(a)(1)(ii)
312.4, 312.8 and 312.10	SRM > Policies and Standards > Information Security Policies	shared	x	Domain 2		Article 5, Article 6 Article 7	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 PL-4	NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 AC-20 (1) NIST SP 800-53 R3 AC-20 (2) NIST SP 800-53 R3 PL-4	
312.8 and 312.10	SRM > GRC >	shared	x	Domain 2	6.01. (c) 6.02. (e)		NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4	NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4	99.31(a)(1)(ii)
312.8 and 312.10	BOSS > Human Resources Security > Employee Awareness	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4	

312.8 and 312.10	BOSS > Data Governance > Clear Desk Policy	shared	x	Domain 2			NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2	NIST SP 800-53 R3 AC-11 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-2 (1) NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 MP-4 NIST SP 800-53 R3 MP-4 (1)	
312.8 and 312.10	SRM > Privilege Management Infrastructure > Privilege Usage Management	shared	x	Domain 2	6.03. (i) 6.03. (j)		NIST SP 800-53 R3 AU-9	NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2)	

312.8 and 312.10	SRM > Policies and Standards >	shared	x	Domain 2	6.01. (b) 6.01. (d) 6.02. (e) 6.03. (b) 6.03.04. (b) 6.03.04. (c) 6.03.05. (b) 6.03.05. (d) 6.03.06. (b) 6.04.01. (c) 6.04.01. (f) 6.04.02. (a) 6.04.02. (b)	Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-10 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1	
312.8 and 312.10	SRM > Privilege Management Infrastructure > Privilege Usage Management - Resource Protection	provider	x	Domain 2			NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AC-5 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6)	
	SRM > Policies and Standards > Information Security Policies			Domain 12					

312.8 and 312.10	ITOS > Resource Management > Segregation of Duties	shared	x	Domain 2	6.04.01. (d) 6.04.08.02. (a)	Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AC-5 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6)	99.31(a)(1)(ii)
	ITOS > Service Support > Release Management - Source Code Management	shared	x	Domain 2		Article 17		NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5)	
312.8 and 312.10	SRM > Governance Risk & Compliance > Vendor Management	shared	x	Domain 2, 4	6.02. (a) 6.02. (b) 6.03. (a)	Article 17 (1), (2)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5	

							NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	

312.8 and 312.10	Information Services > User Directory Services > Active Directory Services, LDAP Repositories, X.500 Repositories, DBMS Repositories, Meta Directory Services, Virtual Directory Services	shared	x	Domain 12					
312.8 and 312.10	SRM > Privilege Management Infrastructure > Identity Management - Identity Provisioning	shared	x	Domain 2	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.03.06. (a) 6.03.06. (b) 6.04.01. (a) 6.04.01. (b) 6.04.01. (d) 6.04.01. (e) 6.04.01. (g)	Article 17	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-7	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AC-3 (3) NIST SP 800-53 R3 AC-5 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-2 (2) NIST SP 800-53 R3 IA-2 (3)	

					6.04.03. (c) 6.04.08.02. (a)			NIST SP 800-53 R3 IA-2 (8) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-4 (4) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6	
312.8 and 312.10	SRM > Privilege Management Infrastructure > Authorization Services - Entitlement Review	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	99.31(a)(1)(ii)
312.8 and 312.10	SRM > Privilege Management Infrastructure > Identity Management - Identity Provisioning	shared	x	Domain 2	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.03.06. (a) 6.04.02. (b)	Article 17	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 SC-30	99.31(a)(1)(ii)
312.8 and 312.10	SRM > Policies and Standards > Technical Security Standards	shared	x	Domain 10	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.04.05. (b)	Article 17 (1), (2)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AC-11 NIST SP 800-53 R3 AC-11 (1) NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-2 (3) NIST SP 800-53 R3 AU-2 (4)	99.3 99.31(a)(1)(ii)

							NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8	NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-2 (2) NIST SP 800-53 R3 IA-2 (3) NIST SP 800-53 R3 IA-2 (8) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 SC-10	
312.8 and 312.10	SRM > Privilege Management Infrastructure > Privilege Usage Management - Resource Protection	shared	x	Domain 2			NIST SP 800-53 R3 CM-7	NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1)	
312.3, 312.8 and 312.10	BOSS > Security Monitoring Services > SIEM	shared	x	Domain 10	6.03. (i) 6.03. (j) 6.03.03. (a) 6.03.03. (d) 6.03.04. (e) 6.04.07. (a) 6.07.01. (a) 6.07.01. (c)	Article 17	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-3 NIST SP 800-53 R3 AU-4 NIST SP 800-53 R3 AU-5 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 AU-12	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8 NIST SP 800-53 R3 AU-8 (1)	

							NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3		
	SRM > Privilege Management Infrastructure > Privileged Usage Management -> Hypervisor Governance and Compliance								
312.8 and 312.10	Infra Services > Network Services > Authoritative Time Source	provider	x	Domain 10	6.03. (k)		NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8 NIST SP 800-53 R3 AU-8 (1)	
312.8 and 312.10	ITOS > Service Delivery > Information Technology Resiliency - Capacity Planning	provider	x	Domain 7, 8	6.03.07. (a) 6.03.07. (b) 6.03.07. (c) 6.03.07. (d)	Article 17 (1)	NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7)	

	SRM > Threat and Vulnerability Management > Vulnerability Management	provider	x	Domain 1, 13					
312.8 and 312.10	SRM > Infrastructure Protection Services > Network	provider	x	Domain 10	6.03.03. (a) 6.03.03. (d) 6.03.04. (d) 6.04.07. (a) 6.07.01. (c)	Article 17	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-20 (1)	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)	

								NIST SP 800-53 R3 SC-20 (1) NIST SP 800-53 R3 SC-21 NIST SP 800-53 R3 SC-22 NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SC-32	
	SRM > Policies and Standards > Operational Security Baselines	shared	x						
312.8 and 312.10	Information Services > Data Governance > Data Segregation	shared	x	Domain 10	6.03. (d)			NIST SP 800-53 R3 SC-2	

312.8 and 312.10	SRM > Infrastructure Protection Services > Network - Firewall	provider	x	Domain 10	6.03.03. (b) 6.03.05. (a) 6.03.05. (b) 6.04.01. (a) 6.04.01. (g) 6.04.03. (c) 6.04.08.02. (a) 6.04.08.02. (b) 6.05. (c)	Article 17	NIST SP 800-53 R3 SC-7	NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)	

	SRM > Cryptographic Services > Data-in-transit Encryption	provider	X	Domain 1, 13					
	SRM > Privilege Management Infrastructure > Privilege Use Management - Hypervisor Governance and Compliance	provider	X	Domain 1, 13					
312.8 and 312.10	SRM > Infrastructure Protection Services > Network - Wireless Protection	provider	X	Domain 10		Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 SC-7	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 PE-4 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8)	

312.8 and 312.10	SRM > Infrastructure Protection Services > Network	provider	x	Domain 10	6.03.03. (a) 6.03.03. (d) 6.03.04. (d) 6.04.07. (a) 6.07.01. ©	Article 17	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-20 (1)	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-20 (1) NIST SP 800-53 R3 SC-21	
	Application Services > Programming Interfaces >	provider	X	Domain 6					

	Information Services > Reporting Services >	provider		Domain 6					
	Information Technology Operation Services > Service Delivery > Service Level Management - External SLA's	provider		Domain 3	6.04.03. (b) 6.04.08. (a) 6.04.08. (b) 6.06. (a) 6.06. (b) 6.06. (c) 6.06. (d) 6.06. (e) 6.06. (f)				
	SRM > Data Protection > Cryptographic Services - Data-In-Transit Encryption	provider	x	Domain 6					
	Infrastructure Services > Virtual Infrastructure >	provider	X	Domain 6					

	Server Virtualization								
	SRM > Governance Risk & Compliance > Technical Awareness and Training	provider	X	None (Mobile Guidance)					

	SRM > Policies and Standards > Technical Security Standards	provider	X	None (Mobile Guidance)					

	ITOS > Service Support > Configuration Management - Software Management	provider	X	None (Mobile Guidance)					

	SRM > Policies and Standards > Technical Security Standards	provider	X	None (Mobile Guidance)					

	SRM > Policies and Standards > Technical Security Standards	provider	X	None (Mobile Guidance)					

	SRM > Governance Risk & Compliance > Vendor Management	provider	X	None (Mobile Guidance)					

	ITOS > Service Support > Configuration Management - Software Management	provider	X	None (Mobile Guidance)					

	SRM > Policies and Standards > Information Security Policies	provider	X	None (Mobile Guidance)					

	SRM > Infrastructure Protection Services > End Point - Inventory Control	provider	X	None (Mobile Guidance)					

	Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device Management	provider	X	None (Mobile Guidance)					

	SRM > Data Protection > Cryptographic Services - Data-At-Rest Encryption	provider	X	None (Mobile Guidance)					
	Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device Management	provider	X	None (Mobile Guidance)					
	SRM > Policies and Standards > Information Security Services	shared	X	None (Mobile Guidance)					

	Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device Management	shared	X	None (Mobile Guidance)					

	ITOS > Service Support -Change Management > Planned Changes	shared	X	None (Mobile Guidance)					
	Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device	shared	X	None (Mobile Guidance)					
	SRM > Policies and Standards > Technical Security Standards	shared	X	None (Mobile Guidance)					
	BOSS > Data Governance > Secure Disposal of Data	shared	X	None (Mobile Guidance)					
	SRM > Infrastructure Protection Services-	shared	X	None (Mobile Guidance)					

	>Network > Link Layer Network Security								
	SRM > Policies and Standards > Technical Security Standards	shared	X	None (Mobile Guidance)					
312,4	BOSS > Compliance > Contact/Authority Maintenance	shared	x						
312.8 and 312.10	ITOS > Service Support > Security Incident Management	shared	x	Domain 2	6.04.07. (b) 6.07.01. (a) 6.07.01. (d) 6.07.01. (e) 6.07.01. (f) 6.07.01. (g) 6.07.01. (h)	Article 17	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-3 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8	

312.3, 312.8 and 312.10	BOSS > Human Resources Security > Employee Awareness	shared	x	Domain 2	6.07.01. (a)	Article 17	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-6 (1) NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-5	99.31(a)(1)(i) 34 CFR 99.32(a)

312.8 and 312.10	BOSS > Legal Services > Incident Response Legal Preparation	shared	x	Domain 2	6.04.07. (b) 6.07.01. (f) 6.07.01. (h)		NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 AU-7 NIST SP 800-53 R3 AU-7 (1) NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2) NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4)	
312.8 and 312.10	BOSS > Operational Risk Management > Key Risk Indicators	shared	x	Domain 2	6.07.01. (a) 6.07.01. (i)		NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8	
	SRM > Governance Risk & Compliance > Vendor Management	provider	X	Domain 2					

	ITOS > Service Support -> Incident Management > Cross Cloud Incident Response	provider		Domain 2					
312.8 and 312.10	ITOS > Service Delivery > Service Level Management	provider	x	Domain 2	6.02. (c) 6.03.07. (a) 6.03.07. (b) 6.03.07. (c) 6.03.07. (d)	Article 17	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3) NIST SP 800-53 R3 CP-7 (5)	

	SRM > Governance Risk & Compliance > Vendor Management	provider	x	Domain 2					
312.3, 312.8 and 312.10	BOSS > Legal Services > Contracts	shared	x	Domain 3	6.02. (e) 6.10. (h) 6.10. (i)	Article 17 (3)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4) NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)	

	SRM > Governance Risk & Compliance > Vendor Management	provider	x						
	ITOS > Service Delivery > Service Level Management - Vendor Management	provider	x	Domain 3	6.02. (c) 6.02. (d) 6.07.01. (k)				

	SRM > Governance Risk & Compliance > Vendor Management	provider	x	Domain 2					
312.2(a) and 312.3 (Prohibition on Disclosure)	BOSS > Compliance > Third-Party Audits	shared	x	Domain 2, 4	6.10. (a) 6.10. (b) 6.10. (c) 6.10. (d) 6.10. (e) 6.10. (f) 6.10. (g) 6.10. (h) 6.10. (i)		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-6	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-6	
312.8 and 312.10	SRM > Infrastructure Protection Services > Anti-Virus	shared	x	Domain 2	6.03. (f)	Article 17	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-5 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-8	

312.8 and 312.10	SRM > Threat and Vulnerability Management > Vulnerability Management	shared	x	Domain 2	6.03.02. (a) 6.03.02. (b) 6.03.05. (c) 6.07.01. (o)	Article 17	NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (9) NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-5	

312.8 and 312.10	SRM > Infrastructure Protection Services > End Point -	shared	x	Domain 10	6.03. (g)	Article 17			

	White Listing								

GAPP (Aug 2009)	HIPAA/HITECH (Omnibus Rule)	HITRUST CSF v8.1	ISO/IEC 27001:2005	ISO/IEC 27001:2013	ITAR	Jericho Forum	Mexico - Federal Law on Protection of Personal Data Held by Private Parties	NERC CIP	NIST SP800-53 R3	NIST SP800-53 R4 Appendix J
1.2.6	45 CFR 164.312(e)(2)(i)	10.b;10.c;10.e	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11		CIP-007-3 - R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23	AR-7 The organization designs information systems to support privacy by automating privacy controls.

1.2.2 1.2.6 6.2.1 6.2.2		05.j	A.6.2.1 A.6.2.2 A.11.1.1	A9.1.1.		Commandment #6 Commandment #7 Commandment #8			CA-1 CA-2 CA-5 CA-6	AP-1 The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable
1.2.6	45 CFR 164.312 (c)(1) (New) 45 CFR 164.312 (c)(2)(New) 45 CFR 164.312(e)(2)(i)(New)	10.b;10.e	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4		Commandment #1 Commandment #9 Commandment #11		CIP-003-3 - R4.2	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	AR-7 The organization designs information systems to support privacy by automating privacy controls.

1.1.0 1.2.2 1.2.6 4.2.3 5.2.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4 8.2.1 8.2.2 8.2.3 8.2.5 9.2.1		01.t;09.s	A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4		All			AC-1 AC-4 SC-1 SC-16	AR-7 The organization designs information systems to support privacy by automating privacy controls.

10.2.5	45 CFR 164.312(b)	06.i	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1		Commandment #1 Commandment #2 Commandment #3			CA-2 CA-7 PL-6	AR-4 Privacy Auditing and Monitoring. To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). Audit for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations,
1.2.5 1.2.7 4.2.1 8.2.7 10.2.3 10.2.5	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	05.h;06.i;06.j	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1		Commandment #1 Commandment #2 Commandment #3	Chapter VI, Section 1 Article 39, I. and VIII. Chapter 8 Article 59	CIP-003-3 - R1.3 - R4.3 CIP-004-3 R4 - R4.2 CIP-005-3a - R1 - R1.1 - R1.2	CA-1 CA-2 CA-6 RA-5	AR-4. Privacy Auditing and Monitoring. These assessments can be self-assessments or third party audits that result in reports on compliance gaps identified in programs, projects, and information systems.

		06.a	ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3	Clauses 4.2(b), 4.4, 5.2(c), 5.3(ab), 6.1.2, 6.1.3, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3						

			A.15.1.4 A.15.1.6	9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1, A.18.1.1, A.18.1.3, A.18.1.4, A.18.1.5							
	45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	12.d	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	Clause 5.1(h) A.17.1.2 A.17.1.2		Commandment #1 Commandment #2 Commandment #3			CP-1 CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 PE-17	UL-2 INFORMATION SHARING WITH THIRD PARTIES - a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of

	45 CFR 164.308 (a)(7)(ii)(D)	12.e	A.14.1.5	A17.3.1		Commandment #1 Commandment #2 Commandment #3			CP-2 CP-3 CP-4	
		08.h;08.i	A.9.2.2 A.9.2.3	A11.2.2, A11.2.3		Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #9 Commandment #11			PE-1 PE-4 PE-13	

1.2.6		09.a;09.r	Clause 4.3.3 A.10.7.4	Clause 9.2(g)		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11		CIP-005-3a - R1.3 CIP-007-3 - R9	CP-9 CP-10 SA-5 SA-10 SA-11	
8.2.4	45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii) (New)	08.d	A.9.1.4 A.9.2.1	A11.1.4, A11.2.1		Commandment #1 Commandment #2 Commandment #3		CIP-004-3 R3.2	PE-1 PE-13 PE-14 PE-15 PE-18	
	45 CFR 164.310 (c)	08.g	A.9.2.1	A11.2.1		Commandment #1 Commandment #2 Commandment #3			PE-1 PE-5 PE-14 PE-15 PE-18	

5.2.3 8.2.2 8.2.3 8.2.4 8.2.5 8.2.6 8.2.7	45 CFR 164.310 (a)(2)(iv)	08.j	A.9.2.4	A11.2.4		Commandment #2 Commandment #5 Commandment #11		CIP-007-3 - R6.1 - R6.2 - R6.3 - R6.4	MA-2 MA-3 MA-4 MA-5 MA-6	
		08.h	A.9.2.2 A.9.2.3 A 9.2.4	A.11.2.2, A.11.2.3, A.11.2.4		Commandment #1 Commandment #2 Commandment #3			CP-8 PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14	
	45 CFR 164.308 (a)(7)(ii)(E)	12.a;12.b;12.c	ISO/IEC 27001:2005 A.14.1.2 A 14.1.4	A.17.1.1 A.17.1.2		Commandment #1 Commandment #2 Commandment #3		CIP-007-3 - R8 - R8.1 - R8.2 - R8.3	RA-3	

8.2.1		09.a	Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1	Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1		Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7			CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12	
5.1.0 5.1.1 5.2.2 8.2.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) (New) 45 CFR 164.316(b)(2)(i) (New)	09.l	Clause 4.3.3 A.10.5.1 A.10.7.3	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1	EAR 15 § 762.6 Period of Retention EAR 15 CFR § 786.2 Recordkeeping	Commandment #11	Chapter II Article 11, 13	CIP-003-3 - R4.1	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11	FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access,
1.2.6		05.d;09.i	A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3	A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7		Commandment #1 Commandment #2 Commandment #3			CA-1 CM-1 CM-9 PL-1 PL-2 SA-1	

			A.12.5.5 A.15.1.3 A.15.1.4	A.18.1.3 A.18.1.4					SA-3 SA-4	
		10.I	A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2 A.14.2.9 A.14.1.1		Commandment #1 Commandment #2 Commandment #3			SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13	
9.1.0 9.1.1 9.2.1 9.2.2		09.i	A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	A.6.1.1 A.12.1.1 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* partial A.14.2.2 8.1* partial A.14.2.3 8.1* partial A.14.2.4 A.12.6.1 A.16.1.3 A.18.2.2 A.18.2.3		Commandment #1 Commandment #2 Commandment #3			CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13	

3.2.4 8.2.2		10.h	A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3	A.6.1.2 A.12.2.1 A.9.4.4 A.9.4.1 A.12.5.1 8.1* (partial) A.14.2.4		Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11			CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7	FTC Fair Information Principles Involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/report

1.2.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	09.i;10.k	A.10.1.4 A.12.5.1 A.12.5.2	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3		Commandment #1 Commandment #2 Commandment #3 Commandment #11		CIP-003-3 - R6	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9 PL-2 PL-5 SI-2 SI-6 SI-7	AR- 4. Privacy Monitoring and Auditing. Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight
1.2.3 1.2.6 4.1.2 8.2.1 8.2.5 8.2.6		07.d	A.7.2.1	A.8.2.1		Commandment #9	General Provisions, Article 3, V. and VI.	CIP-003-3 - R4 - R5	RA-2 AC-4	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research.

		01.m		Clause 4.2 5.2, 7.5, 8.1						TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS
3.2.4 4.2.3 7.1.2 7.2.1 7.2.2 8.2.1 8.2.5	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	09.x;09.y	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4		Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11			AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9	TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS
1.1.2 5.1.0 7.1.2 8.1.0 8.2.5		07.e	A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1		Commandment #8 Commandment #9 Commandment #10	Chapter II Article 8, 9, 11, 12, 14, 18, 19, 20, 21	CIP-003-3 - R4 - R4.1	AC-16 MP-1 MP-3 PE-16 SI-12	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used
1.2.6	45 CFR 164.308(a)(4)(ii)(B)	10.i	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.		Commandment #9 Commandment #10 Commandment #11		CIP-003-3 - R6	SA-11 CM-04	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research. SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

6.2.1	45 CFR 164.308 (a)(2)	07.b	A.6.1.3 A.7.1.2 A.15.1.4	A.6.1.1 A.8.1.2 A.18.1.4		Commandment #6 Commandment #10	Chapter IV Article 30	CIP-007-3 - R1.1 - R1.2	CA-2 PM-5 PS-2 RA-2 SA-2	AP-1 AUTHORITY TO COLLECT. AP-2 PURPOSE SPECIFICATION.
5.1.0 5.2.3	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	08.l;09.p	A.9.2.6 A.10.7.2	A.11.2.7 A.8.3.2		Commandment #11		CIP-007-3 - R7 - R7.1 - R7.2 R7.3	MP-6 PE-1	DM-2 DATA RETENTION AND DISPOSAL
	45 CFR 164.310 (d)(2)(iii)	07.a;07.b	A.7.1.1 A.7.1.2	Annex A.8					NIST SP800-53 R3 CM-8	
8.2.3		08.a	A.9.1.1	A.11.1.1 A.11.1.2		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c R1.2 - R1.3 - R1.4 - R1.6 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18	

		01.k	A.11.4.3			Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #8			IA-3 IA-4	
	45 CFR 164.310 (d)(1) (New)	08.k;08.m	A.9.2.7 A.10.1.2	A.11.2.6 A.11.2.7		Commandment #4 Commandment #5 Commandment #11			AC-17 MA-1 PE-1 PE-16 PE-17	

	45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) (New) 45 CFR 164.310 (d)(2)(i) (New)	08.k	A.9.2.5 A.9.2.6	A.8.1.1 A.8.1.2		Commandment #6 Commandment #7 Commandment #8			CM-8	
8.2.1 8.2.2 8.2.3	45 CFR 164.310 (a)(1) 45 CFR 164.310 (a)(2)(ii) 45 CFR 164.308(a)(3)(ii)(A) (New) 45 CFR 164.310 (a)(2)(iii) (New)	08.c	A.5.1.1 A.9.1.3 A.9.1.5	A.11.1.1 A.11.1.2		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c R1.2 - R1.3 - R1.4 -R2 - R2.2	PE-2 PE-3 PE-4 PE-5 PE-6	

8.2.3		08.b	A.9.1.1 A.9.1.2	A.11.1.6		Commandment #1 Commandment #2 Commandment #3 Commandment #5		CIP-006-3c R1.2 - R1.3 - R1.4	PE-7 PE-16 PE-18	
8.2.5 8.2.6		08.f	A.9.1.6	A.11.2.5 8.1* (partial) A.12.1.2		Commandment #6 Commandment #7			MA-1 MA-2 PE-16	

8.2.3	45 CFR 164.310(a)(1) (New) 45 CFR 164.310(a)(2)(ii) (New) 45 CFR 164.310(b) (New) 45 CFR 164.310 (c) (New)	08.b;08.i	A.9.1.1 A.9.1.2	A.11.1.1		Commandment #1 Commandment #2 Commandment #3 Commandment #5	Chapter II, Article 19	CIP-006-3c R1.2 - R1.3 - R1.4 - R1.6 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-18	
		06.d;10.g		Annex A.10.1 A.10.1.1 A.10.1.2						
8.1.1 8.2.1 8.2.5	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1) (New)	06.d;10.g	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	Clauses 5.2(c) 5.3(a) 5.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.3 9.2(g) A.8.2.3 A.10.1.2 A.18.1.5		Commandment #9 Commandment #10 Commandment #11			SC-12 SC-13 SC-17 SC-28	

8.1.1 8.2.1 8.2.5	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	06.d;09.l;09.o;09 .s;10.f	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	A.13.1.1 A.8.3.3 A.13.2.3 A.14.1.3 A.14.1.2 A.10.1.1 A.18.1.3 A.18.1.4		Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11		CIP-003-3 - R4.2	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8	
				Annex A.10.1 A.10.1.1 A.10.1.2						
1.2.6 8.2.1 8.2.7		10.a	A.12.1.1 A.15.2.2	A.14.1.1 A.18.2.3		Commandment #2 Commandment #4 Commandment #5 Commandment #11	Chapter II, Article 19 and Chapter VI, Section I, Article 39		CM-2 SA-2 SA-4	AR-1 Governance and Privacy Program. TR-1 PRIVACY NOTICE. TR-3 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

1.2.4 8.2.1	45 CFR 164.308(a)(1)(ii)(A) (New) 45 CFR 164.308(a)(8) (New)	03.b	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2	Clauses 5.2(c) 5.3(a) 5.3(b) 6.1.2 6.1.2(a)(2) 6.1.3(b)	EAR 15 CFR §736.2 (b)	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7 Commandment #9 Commandment #10			CA-3 RA-2 RA-3 MP-8 PM-9 SI-12	AR-2 Privacy Impact and Risk Assessment
1.1.2 8.2.1		02.d	Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	Clause 7.2(a,b) A.7.2.1 A.7.2.2 A.9.2.5 A.18.2.2		Commandment #6 Commandment #7 Commandment #8			AT-2 AT-3 CA-1 CA-5 CA-6 CA-7 PM-10	AR-1 Governance and Privacy Program
8.2.1	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR	00.a;05.a;05.c	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4	All in sections 4, 5, 6, 7, 8, 9, 10. A.6.1.1 A.13.2.4 A.6.1.3 A.6.1.4		Commandment #1 Commandment #2	Chapter II, Article 19	CIP-001-1a - R1 - R2 CIP-003-3 - R1 - R1.1 - R4 CIP-006-3c	PM-1 PM-2 PM-3 PM-4 PM-5 PM-6	AR-1 Governance and Privacy Program

8.2.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	05.a	Clause 5 A.6.1.1	All in section 5 plus clauses 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c)		Commandment #3 Commandment #6	Chapter VI, Section I, Article 39	CIP-003-3 - R1 - R1.1	CM-1 PM-1 PM-11	
8.1.0 8.1.1	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2) (New)	04.a;10.f	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2	Clause 4.3 Clause 5 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c) A5.1.1 A.7.2.2		Commandment #1 Commandment #2 Commandment #3	Chapter VI, Section I, Article 39	CIP-003-3 - R1 -R1.1 - R1.2 - R2 - R2.1 - R2.2 - R2.3	AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1	

10.2.4	45 CFR 164.308 (a)(1)(ii)(C)	02.f	A.8.2.3	A7.2.3		Commandment #6 Commandment #7	Chapter X, Article 64		PL-4 PS-1 PS-8	
		03.d	Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2	Clause 4.2.1 a, 4.2(b) 4.3 c, 4.3(a&b) 4.4 5.1(c) 5.1(d) 5.1(e) 5.1(f) 5.1(g) 5.1(h) 5.2 5.2 e, 5.2(f) 5.3 6.1.1(e)(2), 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 6.2 e, 6.12 (a) (2), 7.1 7.2(a), 7.2(b) 7.2(c) 7.2(d)				CIP-009-3 - R2	CP-2 RA-2 RA-3	AR-2 Privacy Impact and Risk Assessment
1.2.1 8.2.7 10.2.3	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306(e) (New)	04.b	Clause 4.2.3 f) A.5.1.2	Clause 8.1 A.5.1.2		Commandment #1 Commandment #2 Commandment #3		CIP-003-3 - R3.2 - R3.3 - R1.3 R3 - R3.1 - R3.2 - R3.3	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IR-1 MA-1 MP-1 PE-1 PL-1	

1.2.4 1.2.5	45 CFR 164.308 (a)(1)(ii)(A)	03.b	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1	Clause 4.2(b), 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),				CIP-002-3 - R1.1 - R1.2 CIP-005-3a - R1 - R1.2 CIP-009-3 - R.1.1	PL-5 RA-2 RA-3	
1.2.4	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(	03.a;03.c;05.a	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f)	Clause 6.1.1, 6.1.1(e)(2) 6.1.2			Chapter II Article 19	CIP-009-3 - R4	AC-4 CA-2 CA-6 PM-9	AR-2 Privacy Impact and Risk Assessment
5.2.3 7.2.2 8.2.1 8.2.6	45 CFR 164.308 (a)(3)(ii)(C)	02.h	A.7.1.1 A.7.1.2 A.8.3.2	A.8.1.1 A.8.1.2 A.8.1.4					PS-4	
1.2.9		02.b	A.8.1.2	A.7.1.1	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #2 Commandment #3 Commandment #6 Commandment #9		CIP-004-3 - R2.2	PS-2 PS-3	
1.2.9 8.2.6	45 CFR 164.310(a)(1) (New) 45 CFR 164.308(a)(4)(i) (New)	02.c	A.6.1.5 A.8.1.3	A.13.2.4 A.7.1.2	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #6 Commandment #7			PL-4 PS-6 PS-7	

8.2.2 10.2.5	45 CFR 164.308 (a)(3)(ii)(C)	02.g	A.8.3.1	A.7.3.1		Commandment #6 Commandment #7			PS-4 PS-5	
1.2.6 3.2.4 8.2.6	45 CFR 164.310 (d)(1)	01.x;09.o;09.u	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	A.8.2.1 A.8.3.1 A.8.3.2 A.8.3.3 A.6.2.1 A.6.2.2 A.18.1.4	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	All		CIP-007-3 - R7.1	AC-17 AC-18 AC-19 MP-2 MP-4 MP-6	

1.2.5		05.e	ISO/IEC 27001:2005 Annex A.6.1.5	A.13.2.4	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #6 Commandment #7 Commandment #8 Commandment #9			PL-4 PS-6 SA-9	DI-2 DATA INTEGRITY AND DATA INTEGRITY BOARD a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. IP-1 CONSENT a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

1.2.9 8.2.1		02.a;05.c;06.g	Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	Clause 5.3 A.6.1.1 A.6.1.1		Commandment #6 Commandment #7 Commandment #8			AT-3 PL-4 PM-10 PS-1 PS-6 PS-7	AR-1 GOVERNANCE AND PRIVACY PROGRAM Control: The organization: Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development,
8.1.0	45 CFR 164.310 (b)	07.c	A.7.1.3	A.8.1.3		Commandment #1 Commandment #2 Commandment #3			AC-8 AC-20 PL-4	
1.2.10 8.2.1	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	02.e	Clause 5.2.2 A.8.2.2	Clause 7.2(a), 7.2(b) A.7.2.2		Commandment #3 Commandment #6	Chapter VI, Section I, Article 39 and Chapter VI, Section II, Article 41	CIP-004-3 - R1 - R2 - R2.1	AT-1 AT-2 AT-3 AT-4	AR-5 PRIVACY AWARENESS AND TRAINING Control: The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that
1.2.10 8.2.1	45 CFR 164.308 (a)(5)(ii)(D)	01.g;02.d	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	Clause 7.2(a), 7.2(b) A.7.2.2 A.9.3.1		Commandment #5 Commandment #6 Commandment #7	Chapter VI, Section I, Article 39 and Chapter VI, Section II, Article 41		AT-2 AT-3 AT-4 PL-4	UL-1 INTERNAL USE Control: The organization uses personally identifiable information

				A.11.2.8						(PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
8.2.3		01.h	Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	Clause 7.2(a), 7.2(b) A.7.2.2 A.11.1.5 A.9.3.1 A.11.2.8 A.11.2.9	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #5 Commandment #6 Commandment #7 Commandment #11			AC-11 MP-2 MP-3 MP-4	
8.2.1		06.j	A.15.3.2			Commandment #2 Commandment #5 Commandment #11		CIP-003-3 - R5.2	AU-9 AU-11 AU-14	

8.1.0	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) (New) 45 CFR 164.308(a)(4)(ii)(C) (New)	01.a	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	S3.2.g	Commandment #6 Commandment #7 Commandment #8		CIP-007-3 - R5.1 - R5.1.2	AC-1 IA-1	
8.2.2		01.l	A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	A.13.1.1 A.9.1.1 A.9.4.4		Commandment #3 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8		CIP-007-3 - R2	CM-7 MA-3 MA-4 MA-5	
		01.c;01.q		Annex A.9.2 A.9.2.1 A.9.2.2 A.9.2.3, A.9.2.4,						

8.2.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) (New) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	09.c	A.10.1.3	A.6.1.2		Commandment #6 Commandment #7 Commandment #8 Commandment #10		CIP-007-3 R5.1.1	AC-1 AC-2 AC-5 AC-6 AU-1 AU-6 SI-1 SI-4	
1.2.6 6.2.1		10.j	Clause 4.3.3 A.12.4.3 A.15.1.3	Clause 5.2(c) 5.3(a), 5.3(b), 7.5.3(b) 7.5.3(d) 8.1, 8.3 9.2(g)	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #6 Commandment #7 Commandment #9 Commandment #10			CM-5 CM-6	
7.1.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4		05.i	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5					CA-3 MA-4 RA-3	"FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or

										disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/reports/privacy3/fairinfo.shtm". UL-2 INFORMATION SHARING WITH THIRD PARTIES

	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	01.b	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	Annex A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5					NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-9	"FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/reports/privacy3/fairinfo.shtm"
8.2.2	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	01.b;01.c;01.i;01.v;10.j	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1				CIP-003-3 - R5.1.1 - R5.3 CIP-004-3 R2.3 CIP-007-3 R5.1 - R5.1.2	AC-3 AC-5 AC-6 IA-2 IA-4 IA-5 IA-8 MA-5 PS-6 SA-7	AP-1 The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or

	45 CFR 164.312 (a)(1)									SI-9	information system need.
8.2.1 8.2.7	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	01.e	A.11.2.4	A.9.2.5	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #6 Commandment #7 Commandment #8 Commandment #10		CIP-004-3 R2.2.2 CIP-007-3 - R5 - R.1.3	AC-2 AU-6 PM-10 PS-6 PS-7		
8.2.1	45 CFR 164.308(a)(3)(ii)(C)	02.g;02.i	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	Annex A A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.3	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #6 Commandment #7 Commandment #8		CIP-004-3 R2.2.3 CIP-007-3 - R5.1.3 - R5.2.1 - R5.2.3	AC-2 PS-4 PS-5	"FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49)
	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312	01.d	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.4 A.9.2.5 A.9.4.2		Commandment #6 Commandment #7 Commandment #8 Commandment #9		CIP-004-3 R2.2.3 CIP-007-3 - R5.2 - R5.3.1 - R5.3.2 - R5.3.3	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2	"FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access,

	(a)(2)(iii) 45 CFR 164.312 (d)								IA-5 IA-6 IA-8 SC-10	destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/reports/privacy3/fairinfo.shtm"
		01.s	A.11.4.1 A 11.4.4 A.11.5.4	A.9.1.2 Deleted A.9.4.4		Commandment #1 Commandment #5 Commandment #6 Commandment #7		CIP-007-3 - R2.1 - R2.2 - R2.3	AC-5 AC-6 CM-7 SC-3 SC-19	
8.2.1 8.2.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)(c) (New)	09.aa;09.ab;09.ad;09.ae	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2 A.11.5.4 A.11.6.1 A.13.1.1	A.12.4.1 A.12.4.1 A.12.4.2, A.12.4.3 A.12.4.3 A.12.4.1 A.9.2.3 A.9.4.4 A.9.4.1 A.16.1.2		Commandment #6 Commandment #7 Commandment #11		CIP-007-3 - R6.5	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11	

			A.13.2.3 A.15.2.2 A.15.1.3	A.16.1.7 A.18.2.3 A.18.1.3					AU-12 AU-14 SI-4		
		10.k		Annex A.12.1.2 A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3,							
		09.a	A.10.10.1 A.10.10.6	A.12.4.1 A.12.4.4					AU-1 AU-8		
1.2.4		09.h	A.10.3.1	A.12.1.3		Commandment #1 Commandment #2 Commandment #3			SA-4		

		10.m		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
8.2.5		01.i;01.m;01.n;09.m	A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4		Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11		CIP-004-3 R2.2.4	SC-7	

		01.l;10.h		Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1							
1.2.6		09.d	A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	A.12.1.4 A.14.2.9 A.9.1.1 8.1,partial, A.14.2.2 8.1,partial, A.14.2.3 8.1,partial, A.14.2.4		Commandment #1 Commandment #10 Commandment #11			SC-2		

	45 CFR 164.308 (a)(4)(ii)(A)	01.m;01.n	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	A.13.1.3 A.9.4.1 A.18.1.4		Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11		CIP-004-3 R3	AC-4 SC-2 SC-3 SC-7	

		01.m;09.m		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),						
		01.c		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
8.2.5	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) (New) 45 CFR 164.312(e)(1) (New) 45 CFR 164.312(e)(2)(ii) (New)	09.m	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7	A.8.1.1 A.8.1.2 A.8.1.3 A.11.2.1 A.11.2.4 A.13.1.1 A.13.1.2 A.13.2.1 A.8.3.3 A.12.4.1 A.9.2.1, A.9.2.2 A.13.1.3 A.10.1.1 A.10.1.2		Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11		CIP-004-3 R3 CIP-007-3 - R6.1	AC-1 AC-18 CM-6 PE-4 SC-3 SC-7	

8.2.5		09.m;11.c	A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4		Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11		CIP-004-3 R2.2.4		
		10.h		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		10.h		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
		05.k		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),						
		09.s		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)						
		09.s		Clause 6.1.1, 6.1.1(e)(2)						

				6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)						
		02.e		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		02.d;02.e		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		01.x;02.e		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		02.d		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		10.k		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		02.d		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		07.a		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)						
		02.d		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)						

		01.t		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						

		10.k		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
		01.d		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)						
		01.x;09.j;09.l		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)						
		01.x		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)						
		01.x		Clause 6.1.1, 6.1.1(e)(2)						

				6.1.2 6.1.2(a)(1) 6.1.2(a)(2),						
		02.d		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)						
		05.f;05.g	A.6.1.6 A.6.1.7	A.6.1.3 A.6.1.4			Chapter VI, Article 44. Chapter II, Article 16, part I			
1.2.4 1.2.7 7.1.2 7.2.2 7.2.4 10.2.1 10.2.4	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	11.a;11.c	Clause 4.3.3 A.13.1.1 A.13.2.1	Clause 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex A.16.1.1 A.16.1.2	ITAR 22 CFR § 127.12	Commandment #2 Commandment #6 Commandment #8	Chapter II, Article 20	CIP-007-3 - R6.1 CIP-008-3 - R1	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8	IP-4 COMPLAINT MANAGEMENT. SE-2 PRIVACY INCIDENT RESPONSE

1.2.7 1.2.10 7.1.2 7.2.2 7.2.4 10.2.4	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) (New) 16 CFR 318.5 (a) (New) 45 CFR 160.410 (a)(1) (New)	11.a;11.b;11.c	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.6.1.1 A.7.2.1, A.7.2.2,	ITAR 22 CFR § 127.12	Commandment #2 Commandment #6 Commandment #8	Chapter II, Article 20	CIP-003-3 - R4.1 CIP-004-3 R3.3	IR-2 IR-6 IR-7 SI-4 SI-5	IP-4 COMPLAINT MANAGEMENT. SE-2 PRIVACY INCIDENT RESPONSE

1.2.7	45 CFR 164.308 (a)(6)(ii)	11.a;11.e	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.7.2.2, A.7.2.3, A.16.1.7, A.18.1.3				CIP-004-3 R3.3	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8	
1.2.7 1.2.10	45 CFR 164.308 (a)(1)(ii)(D)	11.d	A.13.2.2	A.16.1.6				CIP-008-3 - R1.1	IR-4 IR-5 IR-8	
		05.i		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)						

		11.a		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
8.2.2 8.2.5		05.k;09.n	A.6.2.3 A.10.6.2	A.15.1.2 A.13.1.2		Commandment #6 Commandment #7 Commandment #8			SC-20 SC-21 SC-22 SC-23 SC-24	

		06.g		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
1.2.5		05.i;05.k;09.t	A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #1 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	Chapter II Article 14.		CA-3 MP-5 PS-7 SA-6 SA-7 SA-9	

		03.a		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2)						
		05.k		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1						

		05.i		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1)						
1.2.2 1.2.4 1.2.6 1.2.11 3.2.4 5.2.1	45 CFR 164.308(b)(1) (New) 45 CFR 164.308 (b)(4)	05.k;09.e;09.f	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	A.15.1.2 8.1* partial, 8.1* partial, A.15.2.1 A.13.1.2		Commandment #1 Commandment #2 Commandment #3	Chapter II Article 14, 21 Chapter III Article 25 Chapter V Article 36		AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 RA-2 SA-1	
8.2.2	45 CFR 164.308 (a)(5)(ii)(B)	09.j;09.k	A.10.4.1	A.12.2.1		Commandment #4 Commandment #5		CIP-007-3 - R4 - R4.1 - R4.2	SA-7 SC-5 SI-3 SI-5 SI-7 SI-8	

1.2.6 8.2.7	45 CFR 164.308 (a)(1)(i)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)	10.m	A.12.5.1 A.12.5.2 A.12.6.1	8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1		Commandment #4 Commandment #5		CIP-004-3 R4 - 4.1 - 4.2 CIP-005-3a - R1 - R1.1 CIP-007-3 - R3 - R3.1 - R8.4	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5	

		09.k	A.10.4.2 A.12.2.2	A.12.2.1		Commandment #1 Commandment #2 Commandment #3 Commandment #5			SC-18		

						Commandment #11				

NZISM	NZISM v2.5	ODCA UM: PA R2.0		PCI DSS v2.0	PCI DSS v3.0	PCI DSS v3.2	Shared Assessments 2017 AUP
		PA ID	PA level				
14.5 14.6	4.3.8.C.01. 14.4.4.C.01. 14.4.5.C.01. 14.4.6.C.01. 14.4.6.C.02. 14.4.6.C.03. 14.5.6.C.01. 14.5.7.C.01. 14.5.8.C.01.	PA17 PA31	SGP BSGP	PCI DSS v2.0 6.5	6, 6.5	6; 6.5	I.13

9,2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01.				4.1.1, 4.2, 4.3	4.1.1; 4.2; 4.3	L.3 P.4 P.5 A.8
14.5 14.6	14.4.4.C.01. 14.4.5.C.01. 14.4.6.C.01. 14.4.6.C.02. 14.4.6.C.03. 14.5.6.C.01. 14.5.7.C.01. 14.5.8.C.01. 20.3.13.C.01. 20.3.13.C.02.	PA25	GP	PCI DSS v2.0 6.3.1 PCI DSS v2.0 6.3.2	6.3.1 6.3.2	6.3.1;6.3.2	N.4

16.5 16.8 17.4	17.5.5.C.01. 17.5.6.C.01. 17.5.6.C.02. 17.5.7.C.01. 17.5.7.C.02. 17.5.7.C.03. 17.5.8.C.01. 17.5.9.C.01. 17.8.10.C.01. 17.8.10.C.02. 17.8.11.C.01. 17.8.12.C.01. 17.8.13.C.01. 17.8.14.C.01. 17.8.15.C.01. 17.8.16.C.01. 17.8.17.C.01. 18.3.7.C.01. 18.3.8.C.01. 18.3.8.C.02. 18.3.9.C.01. 18.3.10.C.01. 18.3.10.C.02. 18.3.11.C.01. 18.3.11.C.02. 18.3.12.C.01. 18.3.12.C.02. 18.3.12.C.01. 18.3.12.C.02. 18.3.12.C.03.	PA20 PA25 PA29	GP P SGP	PCI DSS v2.0 2.3 PCI DSS v2.0 3.4.1, PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.3.2a PCI DSS v2.0 6.5c PCI DSS v2.0 8.3 PCI DSS v2.0 10.5.5 PCI DSS v2.0 11.5	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c, 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8 10.5.5, 10.8 11.5, 11.6	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2 6.5b; 7.1; 7.2; 7.3; 8.1; 8.2; 8.3; 8.3.1;8.3.2; 8.4; 8.5; 8.6; 8.7; 8.8 10.5.5; 10.9 11.5; 11.6	B.1

5.1, 5.3, 5.4	4.2.10.C.01. 4.2.11.C.01. 4.2.12.C.01 4.5.17.C.01. 4.5.18.C.01. 4.5.18.C.02. 4.5.18.C.03. 4.3.7.C.01. 4.3.8.C.01. 4.3.9.C.01. 4.3.9.C.02. 4.3.9.C.03. 4.3.9.C.04. 4.3.9.C.05. 4.3.10.C.01. 4.3.11.C.01. 4.3.11.C.02. 4.3.11.C.03. 4.3.12.C.01. 4.4.4.C.01. 4.4.5.C.04.	PA15	SGP	PCI DSS v2.0 2.1.2.b			A.1 A.2
6,1	6.1.6.C.01. 6.1.7.C.01. 6.1.8.C.01.	PA18	GP	PCI DSS v2.0 11.2 PCI DSS v2.0 11.3 PCI DSS v2.0 6.6 PCI DSS v2.0 12.1.2.b	11.2 11.3 6.3.2, 6.6 11.2.1, 11.2.2, 11.2.3, 11.3.1, 11.3.2, 12.1.2.b, 12.8.4	11.2 11.3 6.3.2; 6.6 11.2.1; 11.2.2; 11.2.3; 11.3.1; 11.3.2; 11.3.3; 11.3.4; 12.8.4	L.2

1.2 2.2 3.3 5.2	1.2.13.C.01. 1.2.13.C.02. 2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01. 3.3.4.C.01. 3.3.4.C.02. 3.3.4.C.03. 3.3.4.C.04. 3.3.4.C.05.			PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	3,1	3.1	L.3

	3.3.5.C.01. 3.3.5.C.02. 3.3.6.C.01. 3.3.6.C.02. 3.3.6.C.03. 3.3.6.C.04. 3.3.6.C.05. 3.3.6.C.06. 3.3.6.C.07. 3.3.7.C.01. 3.3.8.C.01. 3.3.8.C.02. 3.3.8.C.03. 3.3.8.C.04. 3.3.8.C.05. 3.3.9.C.01. 3.3.10.C.01. 3.3.10.C.02. 3.3.10.C.03. 3.3.10.C.04. 3.3.11.C.01. 3.3.12.C.01.						
6,4	6.4.4.C.01. 6.4.5.C.01. 6.4.6.C.01. 6.4.7.C.01.			PCI DSS v2.0 12.9.1 PCI DSS v2.0 12.9.3 PCI DSS v2.0 12.9.4 PCI DSS v2.0 12.9.6	12.9.1 12.9.3 12.9.4 12.9.6		K.1

4.4 5.2(time limit) 6.3(whenever change occurs)	5.4.5.C.01. 5.4.5.C.02. 5.4.5.C.03. 4.4.4.C.01. 4.4.5.C.01 4.4.5.C.02. 4.4.5.C.03. 4.4.5.C.04. 4.4.6.C.01. 4.4.7.C.01. 4.4.7.C.02. 4.4.8.C.01. 4.4.8.C.02. 4.4.8.C.03. 4.4.8.C.04. 4.4.9.C.01. 4.4.10.C.01. 4.4.11.C.01. 4.4.12.C.01. 4.4.12.C.02. 4.4.12.C.03. 4.4.12.C.04. 4.4.12.C.05. 6.3.5.C.01. 6.3.5.C.02. 6.3.6.C.01. 6.3.6.C.02. 6.3.6.C.03.	PA15	SGP	PCI DSS v2.0 12.9.2	12.9.2, 12.10.2	12.10.2	K.6
10.1 10.2 10.3 10.4 10.5 10.6	10.1.17.C.01. 10.1.17.C.02. 10.1.18.C.01. 10.1.18.C.02. 10.1.18.C.03. 10.1.18.C.04. 10.1.19.C.01. 10.1.20.C.01. 10.1.20.C.02. 10.1.21.C.01. 10.1.21.C.02. 10.1.21.C.03. 10.1.21.C.04. 10.1.22.C.01. 10.1.22.C.02.	PA15	SGP		4.1, 4.1.1, 9.1, 9.2	4.1; 4.1.1; 9.1; 9.2	F.1

10.5 13.5 17.1	10.5.4.C.01. 10.5.5.C.01. 10.5.6.C.01. 10.5.6.C.02. 10.5.7.C.01. 10.5.8.C.01. 10.5.8.C.02. 10.5.9.C.01. 10.5.9.C.02. 10.5.10.C.01. 10.5.10.C.02. 10.5.11.C.01. 13.6.5.C.01. 13.6.6.C.01. 13.6.7.C.01. 13.6.8.C.01. 13.6.9.C.01. 13.6.9.C.02. 18.1.8.C.01. 18.1.8.C.02. 18.1.8.C.03. 18.1.8.C.04. 18.1.8.C.05. 18.1.9.C.01. 18.1.9.C.02. 18.1.9.C.03. 18.1.9.C.04. 18.1.10.C.01.			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	1.1.2, 1.1.3, 2.2, 12.3 12.6	1.1.2; 1.1.3; 2.2; 12.3 12.6	I.16 U.1
8.1 8.4	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.4.8.C.01. 8.4.9.C.01. 8.4.10.C.01. 8.4.11.C.01. 8.4.12.C.01. 8.4.13.C.01.	PA15	SGP		3.5.2, 3.6.3, 3.7, 5.1, 5.2, 5.3, 6.1, 6.2, 7.1, 7.2, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 12.2	3.5.3;3.6.3;3.7;5.1;5.2;5.3; 6.1;6.2;7.1;7.2;9.1;9.2;9.3; 9.4;9.5;9.6;9.7;9.8;9.9;12. 2	K.3 K.4
8,1	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01.	PA15	SGP	PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.9 PCI DSS v2.0 9.9.1	9.1.3 9.5 9.6 9.9 9.9.1, 12.2	9.1.3 9.5 9.6 9.9 9.9.1; 12.2	K.3

3.3 12.1 12.5 14.5 (software)	3.3.4.C.01. 3.3.4.C.02. 3.3.4.C.03. 3.3.4.C.04. 3.3.4.C.05. 3.3.5.C.01. 3.3.5.C.02. 3.3.6.C.01. 3.3.6.C.02. 3.3.6.C.03. 3.3.6.C.04. 3.3.6.C.05. 3.3.6.C.06. 3.3.6.C.07. 3.3.7.C.01. 3.3.8.C.01. 3.3.8.C.02. 3.3.8.C.03. 3.3.8.C.04.	PA8 PA15	BSGP SGP		10.8, 11.6	10.9; 11.6	D.1 G.5
8.1 8.2 8.3 8.4	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01. 8.3.3.C.01. 8.3.3.C.02. 8.3.4.C.01. 8.3.4.C.02. 8.3.5.C.01. 8.4.8.C.01. 8.4.9.C.01. 8.4.10.C.01. 8.4.11.C.01. 8.4.12.C.01. 8.4.13.C.01.	PA15	SGP				K.4
6,4	6.4.4.C.01. 6.4.5.C.01. 6.4.6.C.01. 6.4.7.C.01.	PA8 PA15	BSGP SGP				K.2

	NA			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	4.3, 10.8, 11.1.2, 12.1 12.2 12.3 12.4 12.5, 12.5.3, 12.6, 12.6.2, 12.10	4.3;10.9;11.1.2;12.1;12.2; 12.3;12.4;12.4.1;12.5;12.5 .3;12.6;12.6.1;12.6.2;12.1 0	C.1 G.5
6.4 13.1	6.4.4.C.01. 6.4.5.C.01. 6.4.6.C.01. 6.4.7.C.01. 13.2.10.C.01. 13.2.11.C.01. 13.2.11.C.02. 13.2.11.C.03. 13.2.11.C.04. 13.2.12.C.01.	PA10 PA29	BSGP SGP	PCI DSS v2.0 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0 9.9.1 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 10.7	3.1 3.1.a 3.2 9.9.1 9.5. 9.5.1 9.6. 9.7, 9.8 10.7, 12.10.1	3.1;3.2;3.2.1;3.2.2;3.2.3;9. 9.1;9.5;9.5.1;9.6;9.7;9.8;1 0.7;12.10.1	D.1 K.5
12,1	12.1.28.C.01 12.1.28.C.02 12.1.28.C.03 12.1.29.C.01 12.1.30.C.01 12.1.30.C.02			PCI DSS v2.0 6.3.2	6.3.2, 12.3.4	6.3.2;12.3.4	G.1

	12.1.30.C.03 12.1.31.C.01 12.1.32.C.01 12.1.32.C.02 12.1.33.C.01						
2.2 4.1	2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01. 5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01.	PA17	SGP	PCI DSS v2.0 3.6.7 PCI DSS v2.0 6.4.5.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 8.5.1 PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.2b PCI DSS v2.0 9.3.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 11.5	2.1, 2.2.4, 2.3, 2.5 3.3, 3.4, 3.6 4.1, 4.2 6.3.1, 6.3.2, 6.4.2, 6.4.3, 6.4.4, 6.4.5.2 6.7 7.1, 7.1.3	2.1;2.2.4;2.2.5;2.3;2.5;2.6; 3.3;3.4;3.5.4;3.6;4.1;4.2;6. 3.1;6.3.2;6.4.2;6.4.3;6.4.4; 6.4.5.1;6.4.5.2;6.4.5.3;6.5. 4.4;6.7;7.1;7.1.3;7.1.4;8.3; 8.3.1;8.3.2;8.5.1;8.7;9.1;9. 1.2;9.2;10.5;11.5;12.3;12. 8	G.1
12.1 14.1 14.2	5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01. 5.1.10.C.02. 5.1.11.C.01. 5.1.12.C.01. 5.1.13.C.01. 5.1.14.C.01. 5.1.14.C.02. 5.1.15.C.01. 5.1.16.C.01. 5.1.17.C.01. 5.1.18.C.01. 5.1.18.C.02. 5.1.19.C.01. 5.1.19.C.02. 12.1.24.C.01. 12.1.24.C.02. 12.1.24.C.03. 12.1.25.C.01. 12.1.26.C.01. 12.1.26.C.02. 12.1.26.C.03. 12.1.27.C.01.			PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.4	6.1 6.2 6.3 6.4 6.5 6.6 6.7	6.1 6.2 6.3 6.4 6.5 6.6 6.7	G.1

14,1	14.1.6.C.01. 14.1.7.C.01. 14.1.7.C.02. 14.1.8.C.01. 14.1.8.C.02. 14.1.9.C.01. 14.1.10.C.01. 14.1.10.C.02. 14.1.10.C.03. 14.1.11.C.01. 14.1.11.C.02. 14.1.11.C.03. 14.1.11.C.01. 18.1.9.C.02				1.3.3 2.1, 2.2.2 3.6 4.1 5.1, 5.2, 5.3, 5.4 6.2 7.1 9.1 9.1.1 9.1.2 9.1.3 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7 11.1, 11.4, 11.5 12.3	2.1; 2.2.2 3.6 4.1 5.1; 5.1.1; 5.1.2; 5.2; 5.3; 5.4 6.2 7.1 9.1 9.1.1 9.1.2 9.1.3 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 10.1; 10.2; 10.2.1; 10.2.2; 10.2.3; 10.2.4; 10.2.5; 10.2.6; 10.2.7; 10.3; 10.3.1; 10.3.2; 10.3.3; 10.3.4; 10.3.5; 10.3.6; 10.4; 10.5; 10.6; 10.6.1; 10.6.2; 10.6.3; 10.7 11.1; 11.4; 11.5; 11.5.1 12.3; 12.3.1; 12.3.2; 12.3.5; 12.3.6; 12.3.7	O.5

12.1 12.4	12.1.24.C.01. 12.1.24.C.02. 12.1.24.C.03. 12.1.25.C.01. 12.1.26.C.01. 12.1.26.C.02. 12.1.26.C.03. 12.1.27.C.01. 12.1.28.C.01. 12.1.28.C.02. 12.1.29.C.01. 12.1.30.C.01. 12.1.31.C.01. 12.4.3.C.01. 12.4.4.C.01. 12.4.4.C.02. 12.4.4.C.03. 12.4.4.C.04. 12.4.4.C.05. 12.4.4.C.06. 12.4.5.C.01. 12.4.6.C.01. 12.4.7.C.01.	PA14	SGP	PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.3.2 PCI DSS v2.0 6.4 PCI DSS v2.0 6.1	1.1.1 6.3.2 6.4.5	1.1.1 6.3.2 6.4.5	G.1
		PA10	SGP	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10 PCI DSS v2.0 12.3	3.1 9.6.1, 9.7.1 9.10 12.3	3.1 9.6.1; 9.7.1 9.10 12.3	D.1

					1.1.3 12.3.3	1.1.3 12.3.3; 12.3.10	L.4 P.1
		PA25 PA21 PA5	GP GP BSGP	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	2.1.1 3.1 4.1 4.1.1 4.2	2.1.1;3.1;4.1;4.1.1;4.2	D.1 D.6 P.1
13,1	13.1.7.C.01. 13.1.8.C.01. 13.1.8.C.02. 13.1.8.C.03. 13.1.8.C.04.			PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.10	9.5, 9.5.1 9.6 9.7 9.8 9.9	9.5; 9.5.1 9.6 9.7 9.8 9.9	D.2
17,8	12.4.4.C.02 14.4.4.C.01 19.1.21.C.01 20.1.5.C.01. 20.1.5.C.02. 20.1.6.C.01. 20.1.6.C.02. 20.1.7.C.01. 20.1.8.C.01. 20.1.9.C.01. 20.1.9.C.02. 20.1.10.C.01. 20.1.11.C.01. 20.1.12.C.01.			PCI DSS v2.0 6.4.3	6.4.3	6.4.3	I.11

3,4	3.4.8.C.01. 3.4.8.C.02. 3.4.9.C.01. 3.4.10.C.01. 3.4.10.C.02.				3.7 12.5.5 12.10.4	3.7 12.5.5 12.10.4	D.1
13.4 13.5	13.1.7.C.01 13.5.5.C.01. 13.5.6.C.01. 13.5.6.C.02. 13.5.7.C.01. 13.5.8.C.01. 13.5.9.C.01. 13.5.9.C.02. 13.5.9.C.03. 13.5.10.C.01.	PA10 PA39 PA34 PA40	BSGP SGP SGP SGP	PCI DSS v2.0 3.1.1 PCI DSS v2.0 9.10 PCI DSS v2.0 9.10.1 PCI DSS v2.0 9.10.2 PCI DSS v2.0 3.1	3.1.1 9.8, 9.8.1, 9.8.2, 3.1	3.1 9.8; 9.8.1; 9.8.2; 3.1	D.8
12,3	12.3.4.C.01. 12.3.5.C.01. 12.3.5.C.02. 12.3.6.C.01.	PA4 PA8 PA37 PA38	BSGP BSGP SGP SGP	PCI DSS v2.0 9.9.1 PCI DSS v2.0 12.3.3 PCI DSS v2.0 12.3.4	9.7.1 9.9 9.9.1	9.7.1 9.9 9.9.1; 9.9.2; 9.9.3	D.1
8.1 8.2	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.	PA4	BSGP	PCI DSS v2.0 9.1	9.1 9.1.1 9.1.2, 9.1.3 9.2, 9.3, 9.4, 9.4.1, 9.4.2, 9.4.3, 9.4.4	9.1 9.1.1 9.1.2; 9.1.3 9.2; 9.3; 9.4; 9.4.1; 9.4.2; 9.4.3; 9.4.4	F.2

		PA22 PA33	GP SGP				0
12.5 19.1	12.5.3.C.01. 12.5.3.C.02. 12.5.4.C.01. 12.5.4.C.02. 12.5.4.C.03. 12.5.4.C.04. 12.5.5.C.01. 12.5.6.C.01. 12.5.6.C.02. 21.1.8.C.01. 21.1.8.C.02. 21.1.8.C.03. 21.1.9.C.01. 21.1.9.C.02. 21.1.10.C.01 21.1.11.C.01. 21.1.11.C.02. 21.1.11.C.03. 21.1.11.C.04. 21.1.11.C.05. 21.1.12.C.01. 21.1.13.C.01. 21.1.14.C.01. 21.1.14.C.02 21.1.15.C.01. 21.1.15.C.02. 21.1.15.C.03. 21.1.16.C.01.	PA4	BSGP	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9	9.6.3	9.6.3	D.1

12,6	12.6.4.C.01. 12.6.4.C.02. 12.6.5.C.01. 12.6.5.C.02. 12.6.5.C.03. 12.6.5.C.04. 12.6.5.C.05. 12.6.6.C.01. 12.6.6.C.02. 12.6.7.C.01. 12.6.7.C.02. 12.6.8.C.01. 12.6.9.C.01. 13.1.7.C.01. 13.1.10.C.01. 13.1.11.C.01. 13.1.11.C.02. 13.1.11.C.03. 13.1.11.C.04.	PA4	BSGP	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 9.10	9.8, 9.8.1, 9.8.2 12.3	9.8; 9.8.1; 9.8.2 12.3	D.8
4.2 8.1	5.2.3.C.01. 5.2.3.C.02. 8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01.	PA4	BSGP	PCI DSS v2.0 9.1 PCI DSS v2.0 9.2 PCI DSS v2.0 9.3 PCI DSS v2.0 9.4	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4	F.3

8.2 8.1	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.	PA4	BSGP	PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.2	9.1 9.1.1 9.1.3	9.1;9.1.1;9.1.3	F.4
8.1 8.2 8.3 8.4	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01. 8.3.3.C.01. 8.3.3.C.02. 8.3.4.C.01. 8.3.4.C.02. 8.3.5.C.01. 8.4.8.C.01. 8.4.9.C.01. 8.4.10.C.01. 8.4.11.C.01. 8.4.12.C.01. 8.4.13.C.01.	PA4	BSGP		9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	F.4

8.1 8.2	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01. 8.2.5.C.01. 8.2.5.C.02. 8.2.6.C.01. 8.2.6.C.02. 8.2.7.C.01. 8.2.8.C.01.	PA4 PA13 PA24	BSGP SGP P	PCI DSS v2.0 9.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	9.1 9.1.1 9.1.2 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 9.4.4 9.5 9.5.1	F.2
		PA36			3.5, 7.1.3 8.1 8.1.1 8.2.2 8.5 8.5.1	3.5; 7.1.3 8.1 8.1.1; 8.1.2; 8.1.6; 8.1.7 8.2.1; 8.2.2; 8.2.3; 8.2.4; 8.2.5; 8.2.6 8.5 8.5.1	D.5
16,2	17.2.13.C.01. 17.2.14.C.01. 17.2.15.C.01. 17.2.16.C.01. 17.2.16.C.02. 17.2.17.C.01. 17.2.18.C.01. 17.2.18.C.02. 17.2.19.C.01. 17.2.20.C.01. 17.2.20.C.02. 17.2.21.C.01. 17.2.22.C.01. 17.2.23.C.01 17.2.24.C.01.	PA36		PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 3.5 PCI-DSS v2.0 3.5.1 PCI-DSS v2.0 3.5.2 PCI-DSS v2.0 3.6 PCI-DSS v2.0 3.6.1 PCI-DSS v2.0 3.6.2 PCI-DSS v2.0 3.6.3 PCI-DSS v2.0 3.6.4 PCI-DSS v2.0 3.6.5 PCI-DSS v2.0 3.6.6 PCI-DSS v2.0 3.6.7 PCI-DSS v2.0 3.6.8	3.4.1 3.5 3.5.1 3.5.2 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8, 4.1 6.5.3 8.2.1 8.2.2	3.4.1 3.5; 3.5.1; 3.5.4 3.5.2 3.5.3 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8; 4.1 6.5.3 8.2.1 8.2.2	D.5

16,1	17.1.21.C.01. 17.1.22.C.01. 17.1.22.C.02. 17.1.23.C.01. 17.1.23.C.02. 17.1.23.C.03. 17.1.23.C.04. 17.1.24.C.01. 17.1.25.C.01. 17.1.25.C.02. 17.1.25.C.03. 17.1.26.C.01. 17.1.26.C.02. 17.1.27.C.01. 17.1.28.C.01. 17.1.28.C.02. 17.1.28.C.03.	PA25	GP	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 3.4 PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	2.1.1 2.3 3.3 3.4 3.4.1 4.1 4.1.1 4.2 4.3 6.5.3 6.5.4 8.2.1	2.1.1 2.3 3.3 3.4 3.4.1 4.1 4.1.1 4.2 4.3; 6.5.1; 6.5.2 6.5.3 6.5.4; 6.5.5; 6.5.6; 6.5.7; 6.5.8; 6.5.9; 6.5.10 8.2.1	D.5
	22.1.18.C.01. 22.1.18.C.02. 22.1.18.C.03. 22.1.18.C.04. 22.1.18.C.05. 22.1.19.C.01. 22.1.19.C.02. 22.1.19.C.03. 22.1.19.C.04.				3.5.2, 3.5.3 3.6.1, 3.6.3	3.5.3; 3.5.4 3.6.1; 3.6.3	D.5
4.4 5.1	5.4.5.C.01. 5.4.5.C.02. 5.4.5.C.03. 4.2.10.C.01. 4.2.11.C.01. 4.2.12.C.01. 4.4.12.C.01			PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1 PCI DSS v1.2 1.1.2 PCI DSS v1.2 1.1.3 PCI DSS v1.2 1.1.4 PCI DSS v1.2 1.1.5 PCI DSS v1.2 1.1.6	1.1 1.1.1 1.1.2 1.1.3 1.1.4 1.1.5 1.1.6	1.1 1.1.1 1.1.2 1.1.3 1.1.4 1.1.5 1.1.6; 1.1.7	A.1 B.2

	4.4.12.C.02 4.4.12.C.05			PCI DSS v1.2 2.2 PCI DSS v1.2 2.2.1 PCI DSS v1.2 2.2.2 PCI DSS v1.2 2.2.3 PCI DSS v1.2 2.2.4	2.2 2.2.1 2.2.2 2.2.3 2.2.4	2.2 2.2.1 2.2.2 2.2.3 2.2.4	
3.3 4.3 8.4	3.3.4.C.01. 3.3.4.C.02. 3.3.4.C.03. 3.3.4.C.04. 3.3.4.C.05. 3.3.5.C.01. 3.3.5.C.02.	PA10 PA18	BSGP GP	PCI DSS v2.0 12.1 PCI DSS v2.0 12.1.2	12,2	12.2	A.2 B.2
3,2	3.2.7.C.01. 3.2.7.C.02. 3.2.7.C.03. 3.2.7.C.04. 3.2.7.C.05. 3.2.8.C.01. 3.2.9.C.01. 3.2.9.C.02. 3.2.9.C.03. 3.2.10.C.01. 3.2.10.C.02. 3.2.10.C.03. 3.2.11.C.01. 3.2.11.C.02. 3.2.11.C.03. 3.2.12.C.01. 3.2.12.C.02. 3.2.13.C.01. 3.2.14.C.01. 3.2.15.C.01. 3.2.16.C.01. 3.2.17.C.01. 3.2.18.C.01.			PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	12.6, 7.3, 8.8, 9.10	12.6; 7.3; 8.8; 9.10	C.1
4,1	5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01. 5.1.10.C.02.	PA8	BSGP	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	12.1 12.2	12.1 12.2	B.2

4,1	3.1.9.C.01 3.2.10.C.01 3.2.10.C.02 3.2.10.C.03 3.2.11.C.01 3.2.11.C.02 3.2.11.C.03 5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01. 5.1.10.C.02. 5.1.11.C.01. 5.1.12.C.01. 5.1.13.C.01. 5.1.14.C.01. 5.1.14.C.02. 5.1.15.C.01. 5.1.16.C.01. 5.1.17.C.01. 5.1.18.C.01. 5.1.18.C.02. 5.1.19.C.01. 5.1.19.C.02.			PCI DSS v2.0 12.5	12,4	12.4; 12.4.1	C.1
4.2 4.3 4.4 4.5	3.1.9.C.01 3.2.10.C.01 3.2.10.C.02 3.2.10.C.03 3.2.11.C.01 3.2.11.C.02 3.2.11.C.03 5.2.3.C.01. 5.2.3.C.02. 4.5.17.C.01. 4.5.18.C.01. 4.5.18.C.02. 4.5.18.C.03. 5.4.5.C.01. 5.4.5.C.02. 5.4.5.C.03. 5.5.3.C.01. 5.5.4.C.01. 5.5.5.C.01. 5.5.6.C.01. 5.5.7.C.01.	PA30	BSGP	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	7.3, 8.8, 9.10, 12.1 12.2	7.3; 8.8; 9.10; 12.1 12.2	B.1

	5.2.3.C.01. 5.2.3.C.02.						J.4
4,3	4.5.17.C.01. 4.5.18.C.01. 4.5.18.C.02. 4.5.18.C.03.			PCI DSS v2.0 12.1.3	12,2	12.2	A.2
4.1 6.1	5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01. 5.1.10.C.02. 5.1.11.C.01. 5.1.12.C.01. 5.1.13.C.01. 5.1.14.C.01. 5.1.14.C.02. 5.1.15.C.01. 5.1.16.C.01.			PCI DSS v2.0 12.1.3	12.1.1	12.1.1	B.1

1.1 3.3 5.1 5.2 5.3 5.4 7.1 12.2 17.7 18.1	1.1.61.C.01. 1.1.62.C.01. 1.1.63.C.01. 1.1.63.C.02. 1.1.64.C.01. 1.1.65.C.01. 1.1.66.C.01. 1.1.66.C.02. 3.3.4.C.01. 3.3.4.C.02.	PA2 PA15	BSGP SGP	PCI DSS v2.0 12.1.2	12,2	12.2	A.2
3.2 (responsibility) 3.3 3.4 4.1	3.2.7.C.01. 3.2.7.C.02. 3.2.7.C.03. 3.2.7.C.04.			PCI DSS v2.0 12.1.2	12,2	12.2	A.2
2,2	2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01.				9,3	9.3	B.2 E.5 H.2
9,29	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02. 9.2.11.C.01. 9.2.12.C.01. 9.2.12.C.02. 9.2.13.C.01. 9.2.14.C.01. 9.2.14.C.02. 9.2.14.C.03. 9.2.14.C.04. 9.2.15.C.01.	PA27	BSGP	PCI DSS v2.0 12.7 PCI DSS v2.0 12.8.3	12.7 12.8.3	12.7 12.8.3	E.3
9,2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02. 9.2.11.C.01.	PA27	BSGP	PCI DSS v2.0 12.4 PCI DSS v2.0 12.8.2			E.4

	9.2.12.C.01. 9.2.12.C.02. 9.2.13.C.01. 9.2.14.C.01. 9.2.14.C.02. 9.2.14.C.03. 9.2.14.C.04. 9.2.15.C.01.						
		PA27	BSGP				E.5
19.1 19.2 19.3	21.1.8.C.01. 21.1.8.C.02. 21.1.8.C.03. 21.1.9.C.01. 21.1.9.C.02. 21.1.10.C.01 21.1.11.C.01. 21.1.11.C.02. 21.1.11.C.03. 21.1.11.C.04. 21.1.11.C.05. 21.1.12.C.01. 21.1.13.C.01. 21.1.14.C.01. 21.1.14.C.02 21.1.15.C.01. 21.1.15.C.02. 21.1.15.C.03. 21.1.16.C.01. 21.1.16.C.02. 21.1.17.C.01. 21.1.17.C.02. 21.1.18.C.01. 21.1.18.C.02. 21.1.18.C.03. 21.1.19.C.01. 21.1.20.C.01. 21.1.20.C.02.	PA33 PA34	SGP SGP	PCI DSS v2.0 9.7 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 11.1 PCI DSS v2.0 12.3	11.1 12.3	11.1 12.3	A.1 B.2

		PA7	BSGP	PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4			E.3

2,2	2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01.	PA9 PA24	BSGP		12.8.5	12.8.5	C.1
2.2 5.2 4.2	2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01. 4.4.4.C.01. 4.4.5.C.01 4.4.5.C.02.		PCI-DSS v2.0 12.3.5	12,3		12.3	E.3
9,1	9.1.3.C.01. 9.1.4.C.01. 9.1.4.C.02. 9.1.5.C.01. 9.1.5.C.02. 9.1.5.C.03. 9.1.6.C.01. 9.1.7.C.01.	BSGP	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	12,6		12.6	E.1
9,1	3.2.17.C.01 3.2.18.C.01 3.3.13.C.01 3.3.13.C.02		PCI DSS v2.0 8.5.7 PCI DSS v2.0 12.6.1	12,4		12.4.1	E.1

	3.3.14.C.01 3.3.14.C.02 3.3.14.C.03 9.1.3.C.01. 9.1.4.C.01.						
8,1	8.1.9.C.01. 8.1.10.C.01. 8.1.10.C.02. 8.1.11.C.01. 8.1.12.C.01.			8.1.8		8.1.8	F.3
15,4	16.5.6.C.01. 16.5.6.C.02. 16.5.7.C.01. 16.5.8.C.01. 16.5.9.C.01. 16.5.10.C.01. 16.5.10.C.02. 16.5.11.C.01. 16.5.11.C.02		PCI DSS v2.0 10.5.5	10.5 7.1.2 7.1.4 7.2 8.1 8.1.5 8.5		10.5 7.1.2 7.1.4 7.2 8.1 8.1.5 8.5	O.5

	16.5.11.C.03. 16.5.12.C.01 16.5.12.C.02. 16.5.12.C.03. 16.5.13.C.01						
15.1 15.2	5.2.3.C.01 5.2.3.C.02 16.1.13.C.01. 16.1.14.C.01 16.1.15.C.01. 16.1.15.C.02 16.1.16.C.01. 16.1.17.C.01 16.1.17.C.02. 16.1.18.C.01. 16.1.19.C.01. 16.1.20.C.01. 16.1.20.C.02		PCI DSS v2.0 3.5.1 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	3.5.1, 7.0 8.0 12.5.4		3.5.2;7.1;8.1;12.3.8;12.3.9 ;12.5.4	H.3 H.8 H.9 H.10
15,4	16.5.6.C.01. 16.5.6.C.02. 16.5.7.C.01. 16.5.8.C.01. 16.5.9.C.01. 16.5.10.C.01. 16.5.10.C.02. 16.5.11.C.01. 16.5.11.C.02 16.5.11.C.03. 16.5.12.C.01 16.5.12.C.02. 16.5.12.C.03. 16.5.13.C.01. 16.5.13.C.02. 16.5.13.C.03. 16.5.13.C.04. 16.5.14.C.01.		PCI-DSS v2.0 9.1.2	1.2.2 7.1 7.1.2 7.1.3 7.2 7.2.3 9.1.2 9.1.3		1.2.2 7.1 7.1.2 7.1.3 7.2 7.2.3 9.1.2 9.1.3	O.5
	5.5.3.C.01 5.5.5.C.01 5.5.7.C.01 9.2.5.C.01 14.2.6.C.01 16.3.5.C.01			7.3 8.8 9.10		7.3 8.8 9.10	H.3

3.0 3.1 3.2 3.3 3.4 3.5	1.1.26 1.1.32 3.1.8.C.01. 3.1.8.C.02. 3.1.8.C.03. 3.1.9.C.01. 3.2.7.C.01. 3.2.7.C.02. 3.2.7.C.03. 3.2.7.C.04. 3.2.7.C.05. 3.2.8.C.01. 3.2.9.C.01. 3.2.9.C.02. 3.2.9.C.03. 3.2.10.C.01. 3.2.10.C.02. 3.2.10.C.03. 3.2.11.C.01. 3.2.11.C.02. 3.2.11.C.03. 3.2.12.C.01. 3.2.12.C.02. 3.2.13.C.01. 3.2.14.C.01. 3.2.15.C.01. 3.2.16.C.01. 3.2.17.C.01.	P	PCI DSS v2.0 6.4.2	6.4.2, 7.3 8.8 9.10		6.4.2; 7.3 8.8 9.10	H.3
9.4 14.1 14.2 19.1	9.3.4.C.01. 9.3.5.C.01. 9.3.5.C.02. 9.3.6.C.01. 9.3.7.C.01. 9.3.7.C.02. 9.3.7.C.03. 9.3.7.C.04. 9.3.8.C.01.		PCI-DSS v2.0 6.4.1 PCI-DSS v2.0 6.4.2	6.4.1 6.4.2, 7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2 7.2.2 7.3		6.4.1 6.4.2; 7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2; 7.2.1 7.2.2 7.3	H.3
2.2 4.3	2.2.5.C.01. 2.2.5.C.02. 2.2.6.C.01. 2.2.6.C.02. 2.2.7.C.01. 3.4.10.C.01 3.4.10.C.02 4.1.7 5.3.5.C.01.		PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	12.8 12.2		12.8 12.2	A.5

	5.3.6.C.01. 5.3.7.C.01. 5.3.8.C.01.		PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				
			PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				
			PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				
			PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				
			PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				
			PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4				

3.2 9.2 15.2	3.2.7.C.01. 3.2.7.C.02. 3.2.7.C.03. 3.2.7.C.04. 3.2.7.C.05. 3.2.8.C.01. 3.2.9.C.01. 3.2.9.C.02. 3.2.9.C.03. 3.2.10.C.01. 3.2.10.C.02. 3.2.10.C.03. 3.2.11.C.01. 3.2.11.C.02. 3.2.11.C.03. 3.2.12.C.01. 3.2.12.C.02. 3.2.13.C.01. 3.2.14.C.01. 3.2.15.C.01. 3.2.16.C.01. 3.2.17.C.01. 3.2.18.C.01. 9.2.4.C.01 9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02.		PCI DSS v2.0 7.1 PCI DSS v2.0 7.1.1 PCI DSS v2.0 7.1.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 7.2.1 PCI DSS v2.0 7.2.2 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2		7.1;7.1.1;7.1.2;7.1.3;7.1.4. 7.2	H.3
			PCI DSS v2.0 7.1 PCI DSS v2.0 7.1.1 PCI DSS v2.0 7.1.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 7.2.1 PCI DSS v2.0 7.2.2 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4				
9.2 15.2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02. 9.2.11.C.01.	GP	7.1 7.1.1 7.1.2 7.1.3 7.2.1 7.2.2 8.5.1 12.5.4	7.1 7.1.1 7.1.2 7.1.3 7.1.4 12.5.4		7.1 7.1.1 7.1.2 7.1.3 7.1.4 12.5.4	H.3 H.8

	9.2.12.C.01. 9.2.12.C.02. 9.2.13.C.01. 9.2.14.C.01. 9.2.14.C.02. 9.2.14.C.03. 9.2.14.C.04. 9.2.15.C.01. 16.2.3.C.01. 16.2.3.C.02. 16.2.4.C.01. 16.2.5.C.01.						
9,2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02. 9.2.11.C.01. 9.2.12.C.01. 9.2.12.C.02. 9.2.13.C.01. 9.2.14.C.01. 9.2.14.C.02. 9.2.14.C.03. 9.2.14.C.04. 9.2.15.C.01.			8.1.4		8.1.4	H.4 H.10
9,2	9.2.5.C.01. 9.2.6.C.01. 9.2.6.C.02. 9.2.7.C.01. 9.2.8.C.01. 9.2.8.C.02. 9.2.9.C.01. 9.2.10.C.01. 9.2.10.C.02. 9.2.11.C.01.		PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5 PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5	8.1.3 8.1.4 8.1.5, 12.5.4		8.1.3 8.1.4 8.1.5; 12.5.4	H.10
15.1 15.2	16.1.13.C.01. 16.1.14.C.01 16.1.15.C.01. 16.1.15.C.02 16.1.16.C.01. 16.1.17.C.01 16.1.17.C.02. 16.1.18.C.01.	BSGP BSGP P GP	PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4 PCI DSS v2.0 8.5 PCI DSS v2.0 10.1, PCI DSS v2.0	8.0 10.1, 12.3		8.0 10.1; 12.3	D.6 H.1

	16.1.19.C.01. 16.1.20.C.01. 16.1.20.C.02 16.1.21.C.01. 16.1.21.C.02 16.1.22.C.01. 16.1.22.C.02. 16.1.22.C.03. 16.1.22.C.04. 16.1.23.C.01. 16.1.24.C.01 16.1.25.C.01. 16.1.26.C.01 16.1.26.C.02. 16.1.27.C.01 16.1.27.C.02. 16.1.28.C.01. 16.1.29.C.01. 16.1.29.C.02 16.1.29.C.03. 16.1.30.C.01 16.2.3.C.01. 16.2.3.C.02. 16.2.4.C.01. 16.2.5.C.01 16.2.6.C.01.		12.2, PCI DSS v2.0 12.3.8				
12.2	12.2.5.C.01.		PCI DSS v2.0	5.0		5.0	O.5
12.2 14.2	12.2.5.C.02. 12.2.6.C.01. 12.2.6.C.02. 14.2.4.C.01. 14.2.5.C.01. 14.2.5.C.02. 14.2.5.C.03. 14.2.5.C.04. 14.2.6.C.01.		7.1.2	7.1 7.1.2 7.2		7.1 7.1.2 7.2	I.4
17,6	18.4.5.C.01. 18.4.5.C.02. 18.4.5.C.03. 18.4.6.C.01. 18.4.6.C.02. 18.4.6.C.03. 18.4.7.C.01. 18.4.7.C.02. 18.4.8.C.01	BSGP SGP SGP P	PCI DSS v2.0 10.1 PCI DSS v2.0 10.2 PCI DSS v2.010.3 PCI DSS v2.0 10.5 PCI DSS v2.010.6 PCI DSS v2.0 10.7	10.1 10.2 10.3 10.4 10.5 10.6 10.7, 10.8 11.4, 11.5, 11.6 12.5.2		10.1 10.2 ; 10.2.1; 10.2.2; 10.2.3; 10.2.4; 10.2.5; 10.2.6; 10.2.7 10.3; 10.3.1; 10.3.2; 10.3.4; 10.3.5; 10.3.6 10.4 10.5; 10.5.1; 10.5.2; 10.5.3; 10.5.4	O.4 U.2

	18.4.9.C.01. 18.4.9.C.02. 18.4.9.C.03. 18.4.10.C.01. 18.4.11.C.01. 18.4.12.C.01. 22.2.4 22.2.5 22.2.8 22.2.9 22.2.11 22.2.12 22.2.14 22.2.15		PCI DSS v2.0 11.4 PCI DSS v2.0 12.5.2 PCI DSS v2.0 12.9.5			10.6 10.7; 10.9 11.4; 11.5; 11.6 12.5.2	
	22.2.11.C.01. 22.2.11.C.02. 22.2.11.C.03. 22.2.11.C.04. 22.2.12.C.01. 22.2.12.C.02. 22.2.13.C.01. 22.2.13.C.02. 22.2.13.C.03. 22.2.13.C.04. 22.2.13.C.05.	GP		10.5.5, 12.10.5		10.5.5; 12.10.5	O.5 V.1
	16.5.11.C.02 16.5.11.C.03		PCI DSS v2.0 10.4	10,4		10.4; 10.4.1; 10.4.2; 10.4.3	J.6
3,3	3.3.4.C.01. 3.3.4.C.02. 3.3.4.C.03. 3.3.4.C.04. 3.3.4.C.05. 3.3.5.C.01. 3.3.5.C.02. 3.3.6.C.01. 3.3.6.C.02. 3.3.6.C.03. 3.3.6.C.04. 3.3.6.C.05.	SGP					O.5

	3.3.6.C.06. 3.3.6.C.07. 3.3.7.C.01. 3.3.8.C.01.						
	22.2.11.C.01. 22.2.11.C.02. 22.2.11.C.03. 22.2.11.C.04. 22.2.12.C.01. 22.2.12.C.02. 22.2.13.C.01. 22.2.13.C.02. 22.2.13.C.03. 22.2.13.C.04. 22.2.13.C.05. 22.2.13.C.06. 22.2.13.C.07. 22.2.14.C.01. 22.2.14.C.02. 22.2.14.C.03. 22.2.14.C.04. 22.2.14.C.05. 22.2.14.C.06. 22.2.14.C.07. 22.2.15.C.01. 22.2.15.C.02. 22.2.15.C.03.			6,1		6.1	V.1
17.1 17.2	18.1.8.C.01. 18.1.8.C.02. 18.1.8.C.03. 18.1.8.C.04. 18.1.8.C.05. 18.1.9.C.01. 18.1.9.C.02. 18.1.9.C.03. 18.1.9.C.04. 18.1.10.C.01. 18.1.11.C.01. 18.1.11.C.02. 18.1.12.C.01.	BSGP BSGP SGP GP SGP	PCI DSS v2.0 1.1 PCI DSS v2.0 1.1.2 PCI DSS v2.0 1.1.3 PCI DSS v2.0 1.1.5 PCI DSS v2.0 1.1.6 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0	1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 1.2.2 1.2.3 1.3 2.2.2 2.2.3 2.2.4		1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 1.2.2 1.2.3 1.3; 1.3.1; 1.3.2; 1.3.3; 1.3.4; 1.3.5; 1.3.6; 1.3.7; 1.5 2.2.2	O.5 V.1

	18.1.12.C.02. 18.1.13.C.01 18.1.14.C.01 18.1.14.C.02 18.1.14.C.03 18.1.14.C.04 22.2.8.C.01		2.2.2, PCI DSS v2.0 2.2.3	2.5 4.1		2.2.3 2.2.4 2.5 4.1	
	22.2.4 22.2.5 22.2.11.C.01. 22.2.11.C.02. 22.2.11.C.03. 22.2.11.C.04. 22.2.12.C.01. 22.2.12.C.02. 22.2.13.C.01. 22.2.13.C.02. 22.2.13.C.03. 22.2.13.C.04. 22.2.13.C.05. 22.2.13.C.06. 22.2.13.C.07. 22.2.14.C.01. 22.2.14.C.02. 22.2.14.C.03. 22.2.14.C.04. 22.2.14.C.05. 22.2.14.C.06. 22.2.14.C.07. 22.2.15.C.01. 22.2.15.C.02. 22.2.15.C.03.			2.1 2.2 2.5 5.1		2.1;2.2;2.5;5.1	U.2
14,5	14.4.4.C.01. 14.4.5.C.01. 14.4.6.C.01. 14.4.6.C.02. 14.4.6.C.03.	BSGP	PCI DSS v2.0 6.4.1 PCI DSS v2.0 6.4.2	6.4.1 6.4.2		6.4.1;6.4.2	G.1

17.6 18.1 18.4	18.4.5.C.01. 18.4.5.C.02. 18.4.5.C.03. 18.4.6.C.01. 18.4.6.C.02. 18.4.6.C.03. 18.4.7.C.01. 18.4.7.C.02. 18.4.8.C.01 18.4.9.C.01. 18.4.9.C.02. 18.4.9.C.03. 18.4.10.C.01. 18.4.11.C.01. 18.4.12.C.01 19.1.8.C.01. 19.1.9.C.01. 19.1.9.C.02. 19.1.10.C.01. 19.1.11.C.01. 19.1.12.C.01. 19.1.12.C.02. 19.1.13.C.01. 19.1.14.C.01. 19.1.14.C.02. 19.1.15.C.01. 19.1.15.C.02. 19.1.16.C.01. 19.1.16.C.02. 19.1.17.C.01. 19.1.17.C.02 19.1.17.C.03. 19.1.17.C.04. 19.1.17.C.05. 19.1.18.C.01. 19.1.18.C.02. 19.1.18.C.03. 19.1.19.C.01. 19.1.20.C.01. 19.1.20.C.02. 19.1.20.C.03.	BSGP BSGP SGP GP	PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4	1.1 1.2 1.2.1 1.2.3 1.3 1.4 2.1.1 2.2.3 2.2.4 2.3		1.1 1.2 1.2.1 1.2.3 1.3 1.4 2.1.1 2.2.3 2.2.4 2.3	V.1
			PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4				
			PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4				
			PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4				

	22.2.4 22.2.5 22.2.11.C.01. 22.2.11.C.02. 22.2.11.C.03. 22.2.11.C.04.			4,1		4.1	D.6 V.1
	16.1.13.C.01 16.1.14.C.01 16.1.15.C.01 16.1.15.C.02 16.1.17.C.02 16.1.19.C.01 16.1.27.C.01			3.5.1, 3.6.6		3.5.2;3.6.6	H.3 V.4
11.1 17.3	10.7.5.C.02 10.7.6.C.02 11.1.6.C.01. 11.1.7.C.01. 11.1.7.C.02 11.1.7.C.03. 11.1.8.C.01. 11.1.8.C.02. 11.1.8.C.03. 11.1.9.C.01. 11.1.9.C.02. 11.1.10.C.01. 11.1.11.C.01. 11.4.8.C.01 11.4.9.C.01 11.5.11.C.01	BSGP BSGP SGP GP P BSGP SGP	PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1 PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.011.1 PCI DSS v2.0 9.1.3	1.2.3 2.1.1 4.1 4.1.1 11.1, 11.1.a, 11.1.b, 11.1.c, 11.1.d, 11.1.1, 11.1.2 9.1.3		1.2.3; 2.1.1; 4.1; 4.1.1; 11.1; 11.1.a; 11.1.b; 11.1.c; 11.1.d; 11.1.1; 11.1.2; 9.1.3	N.2 N.7 N.8

17.1 17.2	3.2.12.C.02 3.3.6.C.04 3.3.8.C.04 4.3.3 4.3.8.C.01 4.3.9.C.03 18.1.8.C.01. 18.1.8.C.02. 18.1.8.C.03. 18.1.8.C.04. 18.1.8.C.05. 18.1.9.C.01. 18.1.9.C.02. 18.1.9.C.03. 18.1.9.C.04. 18.1.10.C.01. 18.1.11.C.01. 18.1.11.C.02	BSGP BSGP SGP GP SGP	1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 2.2.2 2.2.3	1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 1.2.2 1.2.3 1.3 2.2.2 2.2.3 2.2.4 2.5 4.1			P.1
							V.3

							A.8
							A.8
				4,1		4.1	D.6
	22.2.11.C.01. 22.2.11.C.02. 22.2.11.C.03.						V.1 V.4

	22.2.11.C.04. 22.2.12.C.01. 22.2.12.C.02. 22.2.13.C.01.						
	3.3.13.C.01 3.3.13.C.02 5.2.3.C.02 9.1.4.C.01 9.1.4.C.02 9.1.5.C.01 9.1.5.C.02 9.1.5.C.03 9.3.5.C.01 9.3.5.C.02 11.4.8.C.01. 11.4.9.C.01. 11.4.9.C.02. 11.4.10.C.01. 11.4.11.C.01. 11.4.11.C.02. 11.5.11.C.01. 11.5.12.C.01. 11.5.12.C.02. 11.5.13.C.01. 11.5.13.C.02. 11.5.14.C.01. 11.5.14.C.02. 11.5.14.C.03. 21.1.8.C.01 21.1.8.C03 21.1.15.C.01 21.1.15.C.02						E.1

				4.1.1		4.1.1	G.9

							G.9

	21.4.6.C.02 21.4.9.C.06 21.4.9.C.014 21.4.10.C.09 21.4.10.C.10 21.4.10.C.11 21.4.10.C.15 21.4.10.C.16						E.4

	21.4.6.C.02			4,3		4.3	E.1 G.9

							G.9

							G.9

	21.4.9.C.01 21.4.9.C.02 21.4.9.C.03 21.4.9.C.04 21.4.9.C.05 21.4.9.C.06 21.4.9.C.07 21.4.9.C.08 21.4.9.C.09 21.4.9.C.10 21.4.9.C.11 21.4.9.C.12 21.4.9.C.13 21.4.9.C.14 21.4.9.C.15 21.4.9.C.16						E.1 G.9

	21.4.13.C.01 21.4.10.C.10 21.4.10.C.12						D.1

							D.1 O.5

	21.4.12.C.01 21.4.12.C.02 21.4.12.C.04 21.4.10.C.12	BSGP		4,1		4.1	G.9
	21.4.8.C.01 21.4.10.C.12						O.5 G.9
	21.4.9.C.01 21.4.13.C.04 21.4.10.C.12						E.3

	21.4.10.C.08 21.4.12.C.09 21.4.12.C.10 21.4.12.C.11						O.5

	21.4.9.C.14 21.4.6.C.02						O.5 G.2
	21.4.12.C.09 21.4.10.C.12						H.1
	21.4.9.C.10 21.4.9.C.14						F.3 K.5 G.9
	21.4.9.C.02 21.4.9.C.06 21.4.9.C.10 21.4.10.C.12	SGP					O.5
	21.4.10.C.12						O.5 G.9 G.2

	21.4.10.C.01 21.4.10.C.02 21.4.10.C.03 21.4.10.C.04 21.4.10.C.05						G.9
3,2	3.1.8.C.01 3.1.8.C.02 3.1.8.C.03 3.2.7.C.01. 3.2.7.C.02. 3.2.7.C.03. 3.2.7.C.04. 3.2.7.C.05. 3.2.8.C.01. 3.2.9.C.01. 3.2.9.C.02. 3.2.9.C.03. 3.2.10.C.01. 3.2.10.C.02. 3.2.10.C.03. 3.2.11.C.01. 3.2.11.C.02. 3.2.11.C.03. 3.2.12.C.01. 3.2.12.C.02. 3.2.13.C.01. 3.2.14.C.01. 3.2.15.C.01. 3.2.16.C.01. 3.2.17.C.01. 3.2.18.C.01.			12.5.3 12.10.1		12.5.3 12.10.1; 12.10.3; 12.10.6	J.7
4.1 4.2 4.6 7.1	5.1.6.C.01. 5.1.7.C.01. 5.1.8.C.01. 5.1.9.C.01. 5.1.10.C.01. 5.1.10.C.02. 5.1.11.C.01. 5.1.12.C.01. 5.1.13.C.01. 5.1.14.C.01. 5.1.14.C.02. 5.1.15.C.01. 5.1.16.C.01.	BSGP	PCI-DSS v2.0 12.9 PCI-DSS v2.0 12.9.1 PCI-DSS v2.0 12.9.2 PCI-DSS v2.0 12.9.3 PCI-DSS v2.0 12.9.4 PCI-DSS v2.0 12.9.5 PCI-DSS v2.0	12,1		12.1	J.1 J.2 J.3 J.4 J.5 J.6 J.7 J.8 J.9 J.10 J.11 J.12

	5.1.17.C.01. 5.1.18.C.01. 5.1.18.C.02. 5.1.19.C.01. 5.1.19.C.02. 5.2.3.C.01. 5.2.3.C.02. 5.6.3.C.01. 5.6.3.C.02. 7.1.4.C.01. 7.1.4.C.02. 7.1.4.C.03.		12.9.6				
7,2	7.2.6.C.01. 7.2.6.C.02. 7.2.7.C.01. 7.2.8.C.01. 7.2.9.C.01. 7.2.10.C.01. 7.2.11.C.01. 7.2.12.C.01. 7.2.13.C.01.	BSGP	PCI-DSS v2.0 12.5.2 PCI-DSS v2.0 12.5.3	12.10.1		12.10.1	E.2 P.4 A.8 A.12
			PCI-DSS v2.0 12.5.2 PCI-DSS v2.0 12.5.3				

7,3	5.1.10.C.01 7.3.4.C.01. 7.3.5.C.01. 7.3.5.C.02. 7.3.5.C.03. 7.3.6.C.01. 7.3.6.C.02. 7.3.6.C.03. 7.3.6.C.04. 7.3.6.C.05. 7.3.6.C.06. 7.3.7.C.01. 7.3.7.C.02. 7.3.7.C.03. 7.3.8.C.01. 7.3.9.C.01. 7.3.10.C.01. 7.3.11.C.01.	BSGP					J.7 A.8
7.2 7.3	7.2.6.C.01. 7.2.6.C.02. 7.2.7.C.01. 7.2.8.C.01. 7.2.9.C.01. 7.2.10.C.01. 7.2.11.C.01. 7.2.12.C.01. 7.2.13.C.01. 7.3.4.C.01. 7.3.5.C.01. 7.3.5.C.02.	BSGP	PCI DSS v2.0 12.9.6 PCI DSS v2.0 12.9.6				J.12
							A.5 P.4

	12.7.17.C.01						A.8
17,1	18.1.8.C.01. 18.1.8.C.02. 18.1.8.C.03. 18.1.8.C.04. 18.1.8.C.05. 18.1.9.C.01. 18.1.9.C.02. 18.1.9.C.03. 18.1.9.C.04.	BSGP BSGP SGP					A.8 V.1

				12.1.1		12.1.1	A.9
5.2 2.2	4.4.4.C.01. 4.4.5.C.01 4.4.5.C.02. 4.4.5.C.03. 4.4.5.C.04. 4.4.6.C.01. 4.4.7.C.01. 4.4.7.C.02. 4.4.8.C.01. 4.4.8.C.02. 4.4.8.C.03. 4.4.8.C.04. 4.4.9.C.01. 4.4.10.C.01. 4.4.11.C.01. 4.4.12.C.01. 4.4.12.C.02. 4.4.12.C.03. 4.4.12.C.04. 4.4.12.C.05. 2.2.5.C.01		PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2	2.4 12.8.2		2.4;12.8.1;12.8.2	A.8

				12.8.4		12.8.4	A.9
							A.5 A.9

							A.5 A.9
5,4	4.3.7.C.01. 4.3.8.C.01. 4.3.9.C.01. 4.3.9.C.02. 4.3.9.C.03. 4.3.9.C.04. 4.3.9.C.05. 4.3.10.C.01. 4.3.11.C.01. 4.3.11.C.02. 4.3.11.C.03. 4.3.12.C.01.		PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4 Appendix A PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4 Appendix A	2.4 12.8.2 12.8.3 12.8.4 Appendix A		2.4 12.8.2 12.8.3 12.8.4 Appendix A1	A.5 A.8 A.9
14.1 17.6	5.5.4.C.01 7.3.8.C.01 12.7.20.C.05 14.1.6.C.01. 14.1.7.C.01. 14.1.7.C.02. 14.1.8.C.01. 14.1.8.C.02. 14.1.9.C.01. 14.1.10.C.01. 14.1.10.C.02. 14.1.10.C.03.	BSGP	PCI-DSS v2.0 5.1 PCI-DSS v2.0 5.1.1 PCI-DSS v2.0 5.2 PCI-DSS v2.0 5.1 PCI-DSS v2.0 5.1.1 PCI-DSS v2.0 5.2	1.4, 5.0		1.4;5.0	F.3

12.4 14.1	12.4.3.C.01. 12.4.4.C.01. 12.4.4.C.02. 12.4.4.C.03. 12.4.4.C.04. 12.4.4.C.05. 12.4.4.C.06. 12.4.5.C.01. 12.4.6.C.01. 12.4.7.C.01. 14.1.6.C.01. 14.1.7.C.01. 14.1.7.C.02. 14.1.8.C.01. 14.1.8.C.02. 14.1.9.C.01. 14.1.10.C.01. 14.1.10.C.02. 14.1.10.C.03. 14.1.11.C.01. 14.1.11.C.02. 14.1.11.C.03. 14.1.12.C.01.	BSGP	PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3		2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3	G.1 G.2 J.4 J.5
			PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3				

			PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3				
			PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3				

			PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3				
			PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3				
3 3.1 3.2 3.3							G.9

3.4 3.5							