Kinetic CAIQ Responses

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
1	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)?	Yes			The Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable process designed to increase resiliency and trustworthiness of Cisco products. CSDL conforms with the guidelines of: • Common Criteria • OWASP • Center for Internet Security (CIS) • DoDI 8500.02 - (B-Level Orange Book) • ISO 27034 - application security guideline. • NIST - FIPS/USGv6 • Trusted Computing Group Cisco incorporates the following in its CSDL Process: • A Product Security Baseline defines security related functionality, development processes, and documentation requirements for a component of a system or infrastructure. • Third Party Software Property Repository tracks third party software used in Cisco products. Roles are established for individuals/product groups which allow for the delivery of notifications/alerts regarding possible threats, licensing changes, or vulnerability discoveries/disclosures which in-turn allows Cisco to balance risk and mitigate threats in a rapidly changing threat landscape. • Secure Design: Designining and working with a security-mindset. Threat modeling exercises are conducted to validate the security architecture. • Secure Code: Developers follow Cisco Secure Coding guidelines, conduct regular code reviews to assure code-quality and code-compliance, employ Safe Libraries, utilize hardened build pipelines, as well as enforcing static-analysis continuously on all build artifacts, all of this and more occurs throughout the software development lifecycle at Cisco. • Secure Analysis: Architecture Reviews are conducted quartery and include controls for input validation, output of API frameworks, the privacy implications of each data artifact. • Vulnerability Testing: Conducted daily, a variety of industry-standard security tools from multiple accredited sources provide a continous vulnerability assessment and notification capability.
2			AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes			To ensure that the source code conforms to Cisco's secure coding standard, it is necessary to have an automated solution in place that can continuously check for violations of the secure coding standard. The most effective means of achieving this is to use one or more static analysis tools. Compliers and static analysis tools are used to continuously validate source code. Work tickets are automatically created by the notifications sent by the static-analysis tools when a discovery is made. This allows the appropriate development team to understand the issue and resolve it before the code is included in a new release.
3			AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	Yes			Developers follow Cisco Secure Coding guidelines, which includes holding a weekly Code Review meeting. Each commit or pull-request is reviewed and discussed by the development team leads and senior software engineering resources. A set of key security checkers maximize efficacy and reduce false positives of the Static Analysis tools in finding: • Prohibited function calls (Non-bounds-checking functions) • Buffer overflows • Input Validation / Tainted input • File inclusion or functions that call an external resource • Linked Libraries • Client-side code inclusions • False loops and traversal or enumeration opportunities All Cisco development teams are expected to deploy conformance tools, review any warnings that are generated, and fix high-priority issues. Where code cannot be checked by a tool, then a manual review is required.
4			AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Yes			The Cloud Application Service Provider Remediation Process (CASPR) governs the use of third party providers or vendors to manage Cisco business. The CASPR program ensures that all CSPs are known and their risks mitigated to acceptable levels for CSP evaluation and implementation.
5			AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes			All Cisco cloud products and service offerings must to go through a process called CSDL for Cloud (Cisco Security Development Lifecycle) to obtain a CATO (Cloud Approval to Operate), which is a certification to operate for 1 year. The CSDL process gates the progress of the release such that specific and detailed security requirements must be in-place and verified by the certifying authority (Cisco InfoSec) before the product is available to customers.The CATO is required to be renewed each year and re-certifies over 125 separate security baselines and requirements. As part of the CSDL process, continuous vulnerability testing is mandatory and a variety of security tools are orchestrated to execute an effective security test plan for vulnerability detection. A few examples of the areas of concern within the security test plan are internal and external access paths, file integrity checks, and comprehensive authenticated scans to continuously verify system and application hardening configurations. A feedback system is in place that creates notifications and work-tickets to prioritize and queue any discovered vulnerabilities for due action. This process allows for the discovery of security defects in a consistent and repeatable manner across complex infrastructures. As part of the CSDL Process, application vulnerability testing is performed continuously with multiple industry-standard tools as well as in-house developed tools. More specifically, web applications are evaluated continuously with a strong adherence to the evolving OWASP Standards.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
6	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?	Yes			Terms to be agreed upon in the contract.
7			AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	Yes			Terms to be agreed upon in the contract.
8	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?	Yes			The application code must be employ input validation to normalize and "sanitize" any inputs. This includes but is not limited to validation of the inputs received from users or other systems, validation of parameter length, type, syntax, and business rules.
9	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)?	Yes			Infrastructure is contained within a well-known Cloud Service Provider which adheres to the following industry standards:
10	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.)?	Yes			Cisco Governance Risk and Controls (GRC) Internal Audit function performs quarterly business operational and IT risk assessments. Audits are executed in accordance with the audit plan derived from an annual enterprise-wide risk assessment in collaboration with other risk management functions across Cisco. The Cisco InfoSec organization has several different internal groups which execute different types of security audits. The audit plans, tests, results, findings are Cisco Confidential and are not disclosed externally.
11	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?	Yes			Cisco will provide feedback for any request. Cisco will provide reports for certifications on a case by case basis.
12			AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes			All Cisco service offerings must undergo an annual penetration testing exercise that goes beyond the continuous vulnerability testing, which includes some types of network penetration tests. There are two main types of annual penetration testing events, which may be conducted by different types of network penetration testing groups. External groups are leveraged to conduct cursory industry-standard penetration testing to avoid conflict of interest. Internal pen-testing groups are also leveraged to perform a full-stack inspection starting with external pen-testing but also providing access to the pen-testers at the infrastructure and code levels in order to allow them to trace/analyze any application flow.
13			AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes			An annual penetration test is required by the CSDL process and is required to renew the Production CATO (Cloud Approval To Operate)
14			AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes			Yes, an SIEM assists with continuous analysis of changes (planned or unplanned) as well as continuous compliance testing which provides a notification capability for any change which violates a compliance parameter.
15			AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes			Yes, during the annual process to renew the Production CATO (Cloud Approval To Operate), an external audit is performed.
16			AAC-02.6		Are the results of the penetration tests available to tenants at their request?	Yes			Cisco may share the pen-tenting reports with the tenant upon request.
17			AAC-02.7		Are the results of internal and external audits available to tenants at their request?	Yes			No, the internal compliance documentation is Restricted-type data and shall not be shared with any tenant. However, its possible that an executive version of the report may be shared with the tenant upon request.
18			AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	Yes			This requirement is aligned with Cisco goals and best practices across the company, however there maybe isolated incidents where we may not be in compliance. There are compensating controls in place for these incidents.
19	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?	Yes			Yes, customer data is logically segmented by default.
20			AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes			Data recovery is achieved at several different layers of the CSP, from the instance level at the volume level, to data restoration through RDS replicas. Backup jobs are scheduled and enforced by policy.
21			AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
22			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?	Yes			Cisco has a strong internal controls and compliance program with regular internal audits monitoring the design and operating effectiveness of controls that reduce risk, increase the likelihood of value delivery, improve efficiency, and ensure consistent practice across the organization. Cisco follows best-in-class and industry-recognized patterns for its operational environments and focus on continuous improvement of its operational, security, and quality processes for both products and services. Cisco Governance Risk and Controls (GRC) Internal Audit function performs quarterly business operational and IT risk assessments and audits in accordance with its annual audit plan derived from an annual enterprise-wide risk assessment in collaboration with other risk management functions across Cisco. Cisco internal audit preserves independence and is only accountable to Cisco's Audit Committee, meeting the Standards of the Professional Practice of Internal Auditing of The Institute of Internal Auditors and the Association of Certified Fraud Examiners. Pricewaterhouse Coopers is Cisco's external audit firm. Cisco meets with its external auditors quarterly, and they are on the distribution list for all audit reports. There is an audit committee, which is a subset of The Cisco Board of Directors also has an Audit Committee. The GRC VP reports to the Audit Committee. Cisco Global Compliance Enablement (GCE) function is responsible for embedding compliance risk management into Cisco's business strategy, processes and systems in accordance with the recognized parameters of an effective compliance program pursuant to Federal Sentencing Guidelines. The GCE function is divided into Compliance and Ethics (C&E) and Corporate Investigations (CCI). The C&E function generally aligns with the following organizational pillars: Anti-Corruption & Bribery, Ethics, Remediation, Risk Management, Training and Knowledge Delivery, and Tools and Operations. The CCI team is responsible for investigating and reporting on allegations of ethics and policy violations. The GCE team is directly accountable to the Chief Compliance Officer, the Executive Compliance Committee and the Audit Committee of the Board of Directors.
23	Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide tenants with geographically resilient hosting options?	Yes			
24			BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?			N/A	Kinetic does not enable other providers
25	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?	Yes			Cisco Services has established an exercise, testing, and maintenance program for the Cisco Services Business Continuity Managed Service (BCMS) to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization. Policies require appropriate Cisco Services business function groups to conduct exercises of their BCPs on an annual basis if no real BCP activation has occurred during that timeframe. Exercises are conducted to identify opportunities for documentation improvements and to familiarize personnel with disaster recovery procedures. Controlled templates are used to document the results of the exercises. Business continuity plans and job aids are also updated after exercises. Policies require these documents to be reviewed annually.
26	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?	Yes			Upon request, Cisco may provide a tenant with a flow diagram showing details about the flow of data between components of the Kinetic solution.
27			BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?	Yes			The Kinetic Data Orchestrator and Rules Generator can determine where data is routed, pooled, and stored.
28	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?	Yes			Yes, a comprehensive wiki is maintained which includes but is not limited to: • Support Runbook • Security Operations Playbook • Security Incident Response Plan • Breach Incident Response Plan • Documentation for Automation Source Codes

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
29	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?	Yes			Cisco infrastructure is deployed into "hardened data centers" which are capable of withstanding various extreme natural catastrophes. Physical access to the data center is permitted through multiple layers of screening, physical inspection of all personnel and hardware is required, biometric access mechanisms are used throughout the facility, and the locations of technicians are tracked in real-time through the orchestration of various environmental sensors.
30	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.)?		No		
31	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?	Yes			The Cloud Service Provider (CSP) provides world-class hardware support, Cisco is responsible for the automation code that deploys on top of the hardware through the CSP API. The same automation code that is used to continuously verify and deploy the solution built in a given CSP is the same automation code that is regularly tested as part of the annual BCP test-plan activities.
32			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?			N/A	Depending on the circumstances and the design, various aspects of the infrastructure are backed up during a regularly scheduled automated backup event. In some cases the backup apparatus is authored by Cisco development teams to encrypted and store a backup, in other cases mechanisms offered by the Cloud Service Provider (CSP) are leveraged, for example in the case of storage volume snapshots or in the case of roles/policies which are versioned as part of the CSP services feature set.
33			BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		No		A comprehensive review of data artifacts must be completed, approved, and certified by Cisco InfoSec group to allow the migration of data between Cloud Service Providers (CSP) or even different accounts with the same CSP.
34			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?		No		Special arrangements can be made for collaboration with customers.
35			BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?			N/A	Cisco builds infrastructure utilizing a DevOps toolchain to ensure predictable and repeatable outcome. Cisco development teams abide by the DevSecOps methodology under which security is manifested and maintained as code. From the applications and configurations, to the supporting operating systems of the infrastructure, to the supporting systems of the CI pipeline, as well as the posture and configuration of the CSP account in which the infrastructure is erected, Cisco is committed to end-to-end security at every layer of the solution stack.
36	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.)?	Yes			Cisco data centers are protected by uninterruptible power supply (UPS) and generator back-up power systems. The data centers can be supported by generator power indefinitely as Cisco has agreements with fuel suppliers for 24-hour refueling of generator systems as needed. All critical systems are covered by preventive maintenance programs that meet or exceed equipment manufacturers recommendations and systems are tested regularly to validate proper operation.
37	Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes			Cisco provides granular status pages for all services and regions.
38			BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		No		
39			BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes			Cisco provides granular status pages for all services and regions.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
40	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?	Yes			Cisco maintains a set of comprehensive references and playbooks which outline the roles and corresponding responsibilities for every aspect of an infrastructure operation. • Document Metadata • Terms and Definitions • Kinetic Infrastructures • Cloud Service Roles • Vulnerability Management • Hardening & Patching • Incident Management & Response Plan • Asset Management • Change Management & Configuration Management • Data Handling and Privacy • Access Management • Key Management
41	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?	Yes			Ninety days of logs are kept in the centralized logging cluster, two years are kept on the source hosts. Data collected from the devices is retained per the requirements determined by each tenant.
42			BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	Yes			Cisco Legal has a process for managing subpoena requests for information under legal jurisdiction.
43			BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes			
44			BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	Yes			
45	Change Control & Configuration Management New Development / Acquisition	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes			Cisco's Corporate Strategy Office is responsible for acquisition process. Cisco's Acquisition Integration team defines the services acquisition integration methodology and processes. Cisco Services Acquisition Integration team works in collaboration with Corporate Development to implement and execute a well defined acquisition or divestiture process and methodology. Cisco's Global Strategy, Planning and Acquisitions policy also defines the delivery framework for acquisition integration. Cisco Product Development Methodologies Policy defines the standardized approaches to product development including common understanding of the development process. Approved strategic application goals, market feasibility and annual operating plans, Product roadmaps, project plans, functional requirements documents are part of the product development lifecycle from strategy to release cycle execution.
46			CCC-01.2		Is documentation available that describes the installation, configuration, and use of products/services/features?	Yes			https://developer.cisco.com/docs/kinetic/
47	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?	Yes			Yes. Cisco's Secure Development Lifecycle (CSDL) directive defines that each engineering organization shall assure CSDL compliance through Cisco's Security Insights tool. Cisco's Security Insight tool provides visibility into CSDL compliance information and shall provide continuous compliance measurement for all Engineering organizations and features, products, systems, and solutions within scope of this directive. Cisco Secure Development Lifecycle. Each engineering project shall register compliance status into Security Insight tool. Please refer to http://www.cisco.com/web/about/security/cspo/csdl/index.html
48			CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?	Yes			Many Cisco products incorporate third-party software, both commercial and open source. Cisco uses two integrated tools to help us gain visibility into third-party software security threats - Central repository of intellectual property: Cisco internally tracks which Cisco products use third-party software through a single repository, providing a single point of control. The repository requires entry of any metadata associated with third-party software distributed outside the company. - Notification of third-party software threats and vulnerabilities: Cisco can automatically alert product owners from a continuously updated list of third-party software threats and vulnerabilities. And the product teams can quickly act to investigate, reduce, or eliminate the issue.
49	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?	Yes			Yes. Cisco Secure Development Lifecycle is publicly available and defines how Cisco product is validated through integration, feature test, system and regression tests, Early Field Trial and Beta testing. As part of this process, the product security functionalities integrated in the prior phases need to be verified. In addition, a number of new activities are introduced to further validate the system prior to FCS and put in place the ability to continuously monitor threats post FCS. http://www.cisco.com/web/about/security/cspo/csdl/index.html
50			CCC-03.2		Is documentation describing known issues with certain products/services available?	Yes			Yes. Subscribers can receive RSS feeds of Cisco Security Advisories, Cisco Security Responses and or Cisco Alerts or Cisco Notification Service or email announcements. The page can be customized to view by product. Please refer to https://tools.cisco.com/security/center/publicationListing.x

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
51			CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes			"Yes. The Cisco PSIRT investigates all reports regardless of the Cisco software code version or product lifecycle status. Issues will be prioritized based on the potential severity of the vulnerability and other environmental factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Cisco. Throughout the investigative process, the Cisco PSIRT strives to work collaboratively with the source of the report (incident reporter) to confirm the nature of the vulnerability, gather required technical information, and ascertain appropriate remedial action. When the initial investigation is complete, results will be delivered to the incident reporter along with a plan for resolution and public disclosure. If the incident reporter disagrees with the conclusion, the Cisco PSIRT will make every effort to address those concerns. Please refer to https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html#cpsirp."
52			CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Yes			
53	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?	Yes			Yes. Internally, Cisco Desktop Software policy defines that only software that is needed for business shall be installed on Cisco owned or leased assets. All employees, contractors and vendors at Cisco are to use software only as defined in the license agreement for that software. All software used must be licensed and legally purchased. Software inventory for compliance is gathered using inventory tools.
54	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?	Yes			Upon request we can provide change control documentation
55	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)?		No		
56			DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Yes			
57			DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?		No		
58			DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes			This is data collected from customers, partners, and vendors. Cisco can provided geographic information when requested. Based upon data that is available in DPP SSOT (Single Source of Truth).
59			DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes			This is data collected from customers, partners, and vendors. Cisco can provided geographic information when requested. Based upon data that is available in DPP SSOT (Single Source of Truth).
60			DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes			The Data Protection Policy specifies the requirements for classifying, labeling, and protecting data. This policy applies to all employees, contractors, consultants, temporary and other workers at Cisco, including all personnel affiliated with third parties or non-Cisco entities that create, access, transmit, manage, store, or share data owned by or entrusted to Cisco. There are 4 classifications of data that discusses ownership (roles/resp) data custodian and data user and discusses handling and requirements for each classification. The 4 classifications are: Cisco Public, Cisco Confidential, Cisco Highly Confidential, and Cisco Restricted. Cisco has an associated document called data protection standard which covers labeling, marking, storage, access control and distribution, transmission and destruction (a matrix).
61			DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		No		
62	Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
63			DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	Yes			
64	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)?		No		Cisco identifies that data is encrypted or unencrypted, but but do not provide any methodologies to tenants.
65			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)?			N/A	
66	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?	Yes			The Data Protection Policy specifies the requirements for classifying, labeling, and protecting data. This policy applies to all employees, contractors, consultants, temporary and other workers at Cisco, including all personnel affiliated with third parties or non-Cisco entities that create, access, transmit, manage, store, or share data owned by or entrusted to Cisco. There are 4 classifications of data that discusses ownership (roles/resp) data custodian and data user and discusses handling and requirements for each classification. The 4 classifications are: Cisco Public, Cisco Confidential, Cisco Highly Confidential, and Cisco Restricted. Cisco has an associated document called data protection standard which covers labeling, marking, storage, access control and distribution, transmission and destruction (a matrix).
67			DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes			There is a mechanism for labeling agregating data.
68	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?	Yes			
69	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?	Yes			The Data Protection Policy specifies the requirements for classifying, labeling, and protecting data. This policy applies to all employees, contractors, consultants, temporary and other workers at Cisco, including all personnel affiliated with third parties or non-Cisco entities that create, access, transmit, manage, store, or share data owned by or entrusted to Cisco. There are 4 classifications of data that discusses ownership (roles/resp) data custodian and data user and discusses handling and requirements for each classification. The 4 classifications are: Cisco Public, Cisco Confidential, Cisco Highly Confidential, and Cisco Restricted. Cisco has an associated document called data protection standard which covers labeling, marking, storage, access control and distribution, transmission and destruction (a matrix).
70	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?	Yes			
71			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?		No		This information is Cisco confidential and cannot be shared.
72	Datacenter Security Asset Management	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	Yes			Cisco has a global asset management program that maintains a current inventory of physical and software assets. The asset management teams use Web-based applications to actively monitor the asset lifecycle and ensure compliance with software licensing agreements.
73			DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	Yes			The Cloud Application Service Provider Remediation Process (CASPR) governs the use of third party providers or vendors to manage Cisco business. the CASPR program ensures that all CSPs are known and their risks mitigated to acceptable levels, thereby taking the headaches out of CSP evaluation and implementation.
74	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?	Yes			Secured facilities have photo badge card reader access, security reception areas for people and separate security gate and building for logistics deliveries. Security guards patrol and cameras monitor the external perimeter. Two factor authentication is required to enter inner data center rooms.
75	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?		No		Geo location can be for the provided service offered.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
76	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)?		No		
77	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?	Yes			Cisco Systems can provide a confidential InfoSec policy overview of security topic areas, but the specific information security policies, standards and procedures are Cisco Confidential and are not distributed externally per security policy.
78	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?	Yes			Cisco Systems can provide a confidential InfoSec policy overview of security topic areas, but the specific information security policies, standards and procedures are Cisco Confidential and are not distributed externally per security policy.
79			DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	Yes			Cisco Systems can provide a confidential InfoSec policy overview of security topic areas, but the specific information security policies, standards and procedures are Cisco Confidential and are not distributed externally per security policy.
80	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)?	Yes			Customers may select an existing datacenter during the on-boarding process
81	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?	Yes			
82	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?	Yes			The Physical Security policy states; all employees, vendors, contractors, and temporary workers are issued photo access cards, which are required to access Cisco facilities. Visitors must sign in at the front desk and be escorted by a Cisco employee. As part of the security and awareness training, employees are encouraged to challenge individuals without a photo access card. Public areas are monitored by video images, card readers, and regular physical patrols. All perimeter doors are either card read or an alarmed and monitored emergency exit. Roof hatches are covered by alarm contacts. Cameras are recording and are linked to alarms. Other physical/environmental safety procedures include: - Security guards - Card readers and biometric readers (for Data Centers) - Emergency exit and perimeter alarms
83	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?	Yes			Encryption keys are managed by the key management team and are not provided to support staff.
84	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?			N/A	We do not allow tenets to manage encryption keys
85			EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?			N/A	
86			EKM-02.3		Do you maintain key management procedures?	Yes			
87			EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes			
88			EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		No		Cisco does not use any outside parties or services to manage keys. A centrally managed key management service, Project Keeper, will be available later in FY2018 that uses Hashicorp's Vault software as the back end. Software signing keys are managed in our internal SWIMS application.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
89	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?			N/A	Kinetic does not persist customer telemetry data.
90			EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes			Well, we do not use virtual machine images - but we do use container images. Those are sent into production clusters over TLS
91			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)?		No		
92			EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Yes			The Cryptographic Controls Policy establishes the requirements for the use of cryptography to protect the confidentiality, integrity, and availability of information assets. This policy helps to ensure that the use of encryption technologies conforms to applicable laws and regulations. Encryption technologies must be used as specified in the Data Protection Standard.
93	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?	Yes			Mandated by Cisco Infosec, a curated short-list of approved, known-good algorithms are utilized and validated annually against CATO compliance requirements.
94			EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?			N/A	The keys are maintained in a trusted key management provider that is offered by the CSP (Cloud Service Provider). For example, in the case of AWS, KMS is utilized. At the application layer, Hashicorp Vault and/or Consul is utilized.
95			EKM-04.3		Do you store encryption keys in the cloud?	Yes			The keys are maintained in a trusted key management provider that is offered by the CSP (Cloud Service Provider). For example, in the case of AWS, KMS is utilized. At the application layer, Hashicorp Vault and/or Consul is utilized.
96			EKM-04.4		Do you have separate key management and key usage duties?	Yes			Several roles have been established to facilitate key management compliance concerns and to reduce risk when generating, distributing, and storing secrets. The Keymaster role is typically held by several Managers and each holds the secret-zero credentials to the versioned and encrypted credentials-containers, and they are able to write/administrate to all related keystore repositories. The Power-Users role has access to only designated keystores (credentials-containers) and are given access explicitly by the Keymaster, possibly in coordination with the Security Architect. Once the credentials are delivered, a protocol is to be followed by the Power-user to secure the credentials for use in approved operational applications and preparation for using and/or applying and storing keys and credentials. An Auditor rople exists for the capability of Cisco Infosec to audit the credentials for CATO compliance. Group membership in the version control system determines the role capability of the keymaster, power-user, or auditor. A written policy in the internal wiki defined the roles, terms, definitions and methodologies of the secrets storage strategy.
97	Governance and Risk Management Baseline Requirements	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes			Cisco follows a Secure Development Lifecycle that has a security baseline as the foundation for its services
98			GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes			Yes, an internally developed tool called Continuous Security Buddy (CSB) runs daily. The tool currently covers 9 areas of concern, development is ongoing and more capabilities will be added over time. Security Advocates receive notifications daily and act on citations. The list of areas of concern are listed below: Section 1: Identity and Access Management Compliance Section 2: Network Compliance Section 3: Storage Compliance Section 4: Tagging Compliance Section 5: Vulnerability Compliance Section 6 : AWS Trusted Advisor Checks Section 7: CSIRT Findings Compliance Section 8: AWS CIS Benchmarks Compliance
99			GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		No		No we generally do not allow a client to provide artifacts which are deployed into the solution. If the client has a requirement for using a specific virtual machine image, we look forward to the discussion and working together to find an acceptable solution. Currently, we have developed an automated devops process for creating, hardening, and maintaining the base operating system according to Cisco InfoSec and accepted industry standards (CIS, NSA, et. al.).

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
100	Governance and Risk Management Risk Assessments	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	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)?		No		Filters exist permitting only network traffic related to Cisco business. Capacity monitoring for expansion of service availability ensures network activity will not negatively affect Cisco's network.
101			GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes			Cisco Governance Risk and Controls (GRC) Internal Audit function performs quarterly business operational and IT risk assessments. Audits are done in accordance with its annual audit plan derived from an annual enterprise-wide risk assessment in collaboration with other risk management functions across Cisco. InfoSec and engaged independent third parties also performs separate security audits. The audit plans, tests, results, findings are Cisco Confidential and are not disclosed externally.
102	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?	Yes			Yes, in fact each level of the chain-of-command has a responsibility involved in maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and all employees as they pertain to the manager and employees' area of responsibility, and beyond. Cisco enjoys top-down support for security compliance from the highest executive level. Because of this top-down support, managers have the authority for enforcement of security methodologies and policies that protect Cisco and Ciscos' customers. In turn, this empowers the Security Advocate at the group level to be continuously vigilant and keeps the whole team abreast of details, defenses, required changes and awareness factors when a concerning disclosure occurs or when a concerning security event is taking place.
103	Governance and Risk Management Management Program	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes			Yes, Cisco maintains and continuously updates a comprehensive internal wiki addressing the ISMP.
104			GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	Yes			Yes, the Security Advocate maintains the ISMP documentation continuously as updates as needed. The CATO (Cloud Approval to Operate) renewal process also provides an opportunity for Cisco InfoSec to not only review every aspect of the offering across a minimum of 127 individual baselines but to specifically address any needed enhancements to the ISMP.
105	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?	Yes			Cisco conducts risk assessments and audits on third party providers to ensure compliance with contract agreements.
106	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.)?	Yes			Our infosec policies align with NIST and 27001
107			GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes			Yes, the CATO (Cloud Approval to Operate) renewal process also provides the opportunity to review and measure adherence to all security policies.
108			GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	Yes			Cisco Infrastructure and Intercloud Services ISO 27001 security controls are tested for operational effectiveness annually and attested in an SOC 1 and SOC 2 report by our external auditors. (A Type II (test of controls) report is planned for completion in late summer 2016).
109			GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Yes			Yes, we comply with the PSB's (Product Security Baselines) which are defined by an internal security group at Cisco called Cisco InfoSec in the Cisco Security & Trust Organization, a large body of career security experts. The controls, standards, and certifications include but are not limited to CIS, NIST, NSA, OWASP, FIRST, and SANS.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
110	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?	Yes			Any employee found to have violated a policy may be subject to disciplinary action, up to and including termination of employment as outlined in the Code of Business Conduct (COBC). Any violation of a policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with Cisco.
111			GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes			Yes, a full lifecycle policies and consequences are in-place and active at all times.
112	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?	Yes			Yes, the CATO (Cloud Approval to Operate) renewal process also provides the opportunity to review and measure adherence to all security policies.
113	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?	Yes			Cisco information security policies changes are communicated through Cisco website updates, questionnaire responses to customers under an NDA. Cisco has an online privacy portal: http://www.cisco.com/web/siteassets/legal/privacy_full.html and privacy supplements for service offering(s).
114			GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?		No		Cisco reviews its information security policies biennially and its standards annually.
115	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?	Yes			Security risk assessments and audits are conducted in accordance with an annual audit plan derived from an annual enterprise-wide risk assessment in collaboration with other risk management functions across Cisco.
116			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)?	Yes			Cisco Infrastructure and Intercloud Services performs an annual internal and external audit of sampled hosting data centers. The independent auditors provide risk exposure commentary based on design and test findings to management.
117	Governance and Risk Management Program	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	Yes			Yes, there are policies that cover the employees conduct in general, but each offering has a risk profile which are managed and developed independently so they can be adjusted and tuned for the specific operations of a given offering.
118			GRM-11.2		Do you make available documentation of your organization-wide risk management program?	Yes			High level evidence of the annual risk assessment is shared.
119	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?	Yes			Privacy incidents are reported directly to Cisco's Data Protection and Privacy team who engages the CSIRT team if necessary. The CSIRT Incident Response Handbook includes sensitive incident response procedures for privacy breaches. The CSIRT procedure include gathering details about the privacy breach and following the case handling procedures to classify the case and determine the appropriate resolution.
120			HRS-01.2		Is your Privacy Policy aligned with industry standards?	Yes			Online Privacy Statement aligns to industry standards and has been certified by TRUSTe as consistent with the APEC Cross Border Privacy Rules system and EU/Swiss-US Privacy Shield requirements.
121	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?	Yes			Pre-employment background checks are conducted on all job applicants who receive an offer of employment. Cisco uses a third-party agency to conduct background checks to verify the accuracy of the information provided by the applicant during the selection process. Cisco complies with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting background checks. Offers of employment are conditional upon Cisco's receipt of a pre-employment background check that is acceptable to Cisco, at Cisco's sole discretion. Any applicant who refuses to complete the background check process will not be eligible for employment.
122	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?	Yes			Employees receive Information Security education and training on an annual basis. The Information Security Awareness Program within the Corporate Security Programs Organization (CSPO) designs the training and education to raise awareness of information security policies and best practices. This awareness program targets all employee types (new, existing, permanent, temporary, or contract) through regular awareness, training, and education campaigns

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
123		HR-02	HRS-03.2		Do you document employee acknowledgment of training they have completed?	Yes			The Cisco Code of Business Conduct states that all employees are required to know and adhere to Corporate Information Security policies. Employees must acknowledge that they have read, understood, and agree to comply with the policies and guidelines established in the Code of Business Conduct. New hires are asked to review the COBC at the time they join Cisco. Annually, employees are asked to acknowledge an updated Code of Business Conduct (COBC). Contractors, temporary works sign non-disclosure agreements when they start a relationship with Cisco.
124			HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Yes			All employees sign the Cisco Proprietary Information Agreement in the US or have similar instruments as part of their employment contracts outside of the US
125			HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes			Yes, a specific PSB (Product Security Baseline, SEC-ASU-TRAIN) is in effect at all times which requires that any employees working in a given environment have completed a security training program.
126			HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	Yes			Yes, a specific PSB (Product Security Baseilne, SEC-ASU-TRAIN) is in effect at all times which requires that any employees working in a given environment have completed a security training program. All teams are audited during the CATO renewal process (Cloud Approval to Operate) which ensures that all employees with access, even to non-sensitive systems, have completed training and ensures that the whole team is compliant with SEC-ASU-TRAIN.
127	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?	Yes			Access is revoked upon termination. Account access is revalidated when one of the following events occurs: - User is a new hire - User changes roles or departments - User has a manager or supervisor change - User has held the account for more than 18 months
128			HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes			Upon employee termination, all access rights are revoked/de-provisioned via scripting that runs at least once per day.
129	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)?	Yes			Endpoint policies are established that define minimum device requirements that must be met before a device is authorized to access network environments per a network admission control.
130	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?	Yes			Yes, the Security & Trust Organization maintains and continuously updates, as needed, any and all policies or documents used with clients/customers.
131	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?	Yes			"This is dependent on the products and services provided. See offer description and related documentation for relevant product(s). Please refer to Cisco's Online Privacy Statement here: https://www.cisco.com/c/en/us/about/legal/privacy-full.html. When customers use any Cisco's cloud service, the customer is subjected to the applicable Cisco SaaS Terms of Service or Cisco SaaS Agreement."
132	Human Resources Acceptable Use	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may access tenant data and metadata?	Yes			This is dependent on the products and services provided. See offer description and related documentation for relevant product(s). Please refer to Cisco's Online Privacy Statement here: https://www.cisco.com/c/en/us/about/legal/privacy-full.html. When customers use any Cisco's cloud service, the customer is subjected to the applicable Cisco SaaS Terms of Service or Cisco SaaS Agreement.
133			HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	Yes			This is dependent on the products and services provided. See offer description and related documentation for relevant product(s). Please refer to Cisco's Online Privacy Statement here: https://www.cisco.com/c/en/us/about/legal/privacy-full.html. When customers use any Cisco's cloud service, the customer is subjected to the applicable Cisco SaaS Terms of Service or Cisco SaaS Agreement.
134			HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Yes			This is dependent on the products and services provided. See offer description and related documentation for relevant product(s). Please refer to Cisco's Online Privacy Statement here: https://www.cisco.com/c/en/us/about/legal/privacy-full.html. When customers use any Cisco's cloud service, the customer is subjected to the applicable Cisco SaaS Terms of Service or Cisco SaaS Agreement.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
135	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?	Yes			Where applicable. Cisco provides training and development opportunities to its employees to help them continually improve their skills, knowledge, work quality and efficiency. Managers and employees work together to determine training and development requirements and opportunities in order to help employees improve their skills and knowledge.
136			HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes			Where applicable. Cisco provides training and development opportunities to its employees to help them continually improve their skills, knowledge, work quality and efficiency. Managers and employees work together to determine training and development requirements and opportunities in order to help employees improve their skills and knowledge. Cisco's Privacy and Data Protection training provides guidance on the legal responsibilities with regards to security and data integrity to administrators and data stewards.
137	Human Resources User Responsibility	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Yes			"The Cisco Code of Business Conduct states that all employees are required to know and adhere to Corporate Information Security policies. Employees must acknowledge that they have read, understood, and agree to comply with the policies and guidelines established in the Code of Business Conduct. New hires are asked to review the COBC at the time they join Cisco. Annually, employees are asked to acknowledge an updated Code of Business Conduct (COBC). Contractors, temporary works sign non-disclosure agreements when they start a relationship with Cisco."
138			HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	Yes			Cisco's Acceptable Use Policy defines requirements around clean desk practices to ensure sensitive materials are not left unattended on desks or workspaces. When an employe is away from their desk or workspace, papers and removable storage media must be palced in a secure area or inside a locke drawer.
139			HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Yes			Cisco's Acceptable Use Policy defines requirements around clean desk practices to ensure sensitive materials are not left unattended on desks or workspaces. When an employe is away from their desk or workspace, papers and removable storage media must be palced in a secure area or inside a locke drawer.
140	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?	Yes			
141			HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes			Data management policies include audit controls, such as logging and monitoring, to detect for unauthorized access.
142			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?		No		Cisco IT does not monitor for this.
143	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.)?	Yes			The Cisco Computer Security Incident Response (CSIRT) monitors Intrusion Detection Systems (IDS) using various Security Incident and Event Management Systems (SIEMS). Cisco WebEx uses network based data sources for event monitoring. Cisco WebEx has deployed IDS at the perimeter and other internal network choke points to provide alerts for security incidents.
144			IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
145	Identity & Access Management User Access Policy	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes			Cisco enforces the rule of least privilege through segregation of duties and access restriction based by roles and job functions. Upon individual's termination, all rights are revoked/deprovisioned by scripts running once per day.
146			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?	Yes			Upon individual's termination all rights are revoked/deprovisioned by scripts running once per day.
147	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?	Yes			
148	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?	Yes			
149			IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes			
150	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?	Yes			
151	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?	Yes			Application, program and object source code are protected in development Safe Libraries accessible only to developers.
152			IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
153	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?	Yes			
154			IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	Yes			Yes, the on-call operations team is alerted to issues with the CSP (Cloud Service Provider) status changes.
155			IAM-07.3		Do you have more than one provider for each service you depend on?		No		
156			IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?		No		Cisco Infrastructure and Intercloud Services operates and maintains complete control of its cloud infrastructure environment.
157			IAM-07.5		Do you provide the tenant the ability to declare a disaster?		No		
158			IAM-07.6		Do you provide a tenant-triggered failover option?		No		
159			IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?		No		CISCO PUBLIC No. Cisco Business Continuity Services has a general overview of the business continuity plan and disaster recovery process. Application/service specific BCPs are not distributed externally. CISCO CONFIDENTIAL Business Continuity and recovery plans are Cisco Confidential and are not distributed externally. The BCPs are at the technical assistance centers and service operations centers. Cisco Infrastructure and Intercloud Services maintains complete control of its cloud infrastructure environment.
160	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?	Yes			
161			IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes			Customers retain control and ownership of their data. Customers are responsible for the development, content, operation, maintenance, and use of their content.
162	Identity & Access Management User Access Authorization	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	Yes			CISCO PUBLIC Yes. Subscriber grants electronic access to individuals using the service through identity provider that permits synchronization of service to your contact directory or through registration with the subscriber's site administrator. Subscriber's site configuration information is accessible by Cisco support personnel using Cisco credentials. Cisco credentials are maintained under Cisco password policy, and their strength and rotation are enforced by Cisco policy. CISCO CONFIDENTIAL Cisco WebEx individuals, providing role based support and billing, don't have access to the host recording key, or the subscriber host streaming server to reassemble different video, audio, metadata streams into a meaningful recording.
163			IAM-09.2		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?	Yes			A support process exists which examines each request and determines the appropriate response.
164	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)?	Yes			Yes, at the enterprise layer Cisco uses an internal tool that provides ITIL feedbacks for approvers, whereby every 90 days, a group permissions notification is sent to a list of approvers. Group membership provides authorization for an object (e.g. access to a specific Cloud Service Provider account) and physical action must be taken by the approver to reauthorize the group membership for an additional 90 days. The cycle repeats and when users leave the company, owners and approvers have the ability to then remove the user from the group, effectively finalizing the deauthorization of the users former capabilities.
165			IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes			Yes, the internally-developed ITIL approval apparatus provides a record of activity.
166			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?	Yes			Perhaps, in some circumstances, with appropriate agreements in writing and approved by Cisco DPP Legal, and possibly other Cisco-internal authorities, and with the use of a mutually acceptable safe-exchange medium, there could be some visibility provided should an event occur that affects the tenant.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
167	Identity & Access Management User Access Revocation	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Yes			Account access is revalidated when one of the following events occurs: - User is a new hire - User changes roles or departments - User has a manager or supervisor change - User has held the account for more than 18 months
168			IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes			"Account access is revalidated when one of the following events occurs: - User is a new hire - User changes roles or departments - User has a manager or supervisor change - User has held the account for more than 18 months"
169	Identity & Access Management User ID Credentials	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		No		
170			IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?			N/A	
171			IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?			N/A	
172			IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			N/A	
173			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?	Yes			
174			IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		No		Work in progress
175			IAM-12.7		Do you allow tenants to use third-party identity assurance services?		No		
176			IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	Yes			
177			IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes			
178			IAM-12.10		Do you support the ability to force password changes upon first logon?	Yes			
179			IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes			
180	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?	Yes			The base-image is a very minimal image, part of the hardening process at the base-image layer (the base-image created through devops pipeline) involves removing unnecessary packages to minimize the image as much as possible, and to harden it such that it may take any role in the architecture during the provisioning event. Additional hardening for the operating system and application after the base-image is instantiated into a running system further removes any non-essentials. All logs on the hosts (system and application logs) are sent to a centralized logging cluster such that due action may commence.
181			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.)?	No			
182			IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	Yes			Industry standard techniques for avoiding problems with a VM or container compromising another running VM or container are employed. For example, ASLR is turned on, modern kernels are in use, containers have their capabilities groomed for only what is needed for the application to function correctly using Seccomp and Apparmor Linux Security Modules.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
183	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?	Yes			Our CSIRT team employs a number of tools including IDS/IPS.
184			IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	Yes			
185			IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?		No		This is Cisco Confidential and cannot be shared.
186			IVS-01.4		Are audit logs centrally stored and retained?	Yes			Security event data is stored in Splunk, Stealthwatch, passive DNS, and in the Cisco Threat Intelligence Platform for a minimum of 90 days.
187			IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes			The CSIRT Incident Response Playbook defines the criteria that is used to extract security events of interest from the data that is collected.
188	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)?		No		Cisco does not log all changes made to virtual images.
189			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)?			N/A	
190	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?	Yes			NTP is in use throughout our infrastructure
191	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?			N/A	
192			IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			N/A	
193			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?			N/A	
194			IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	Yes			
195	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)?	Yes			
196	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?			N/A	
197			IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes			
198			IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes			
199			IVS-06.4		Are all firewall access control lists documented with business justification?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
200	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?	Yes			
201	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?	Yes			Customers can use multiple accounts/organizations to separate test and production data
202			IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Yes			
203			IVS-08.3		Do you logically and physically segregate production and non-production environments?	Yes			This depends on the environment. Our network non production is our SVL (Solution Validation Lab), but our non-prod DC hosts are in the same physical DCs, however they are logically separated.
204	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?	Yes			
205			IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	Yes			
206			IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	Yes			
207			IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes			
208	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?	Yes			
209			IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	Yes			
210	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)?	Yes			
211	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?	Yes			
212			IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
213			IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes			
214	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?	Yes			
215			IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes			
216	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?	Yes			
217	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)?	Yes			Reports are available in csv format
218	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?		No		
219			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?		No		
220	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?	Yes			Technically, it is data ingress/outgress, available over MQTT/TLS, MQTT/SecureWebSeockets and AMQP/TLS. APIs are over HTTPS
221			IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes			
222	Interoperability & Portability Virtualization	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			N/A	
223			IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			N/A	
224	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?	Yes			
225	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?	Yes			Internally, access to additional licensed software tools must be approved by management and downloaded from a software repository. Cisco application stores aren't published externally.
226	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?	Yes			All devices that receive certificate based remote VPN access to Cisco are subject to enrollment in the dedicated Mobile Device Management (MDM) solution. Internally, access to additional licensed software tools must be approved by management and downloaded from a software repository. Cisco application stores aren't published externally.
227	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?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
228	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?	Yes			
229	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?	Yes			
230	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?	Yes			
231	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?	Yes			Cisco Network Admission Control (NAC) allows only compliant and trusted endpoint devices, such as PCs, servers, managed devices onto the network, restricting the access of noncompliant devices.
232	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)?	Yes			All devices that receive certificate based remote VPN access to Cisco are subject to enrollment in the dedicated Mobile Device Management (MDM) solution.
233	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?	Yes			All devices that connect to the Exchange servers must meet a minimum set of policies that are applied at the Exchange/ActiveSync level. All devices that receive certificate based remote VPN access to Cisco are subject to enrollment in the dedicated Mobile Device Management (MDM) solution.
234	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?		No		Customer manages their mobile hardware security.
235	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)?		No		
236			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?		No		Customer manages their mobile hardware security.
237	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?	Yes			The Cisco Mobile Device document governs the roles and responsibilities of mobile device users. On the Cisco managed device, Cisco owns company data; personal data is owned by the individual. Service cancellations (e.g. when user is terminated) result in removal of access. In emergency termination scenarios the mobile device is wiped.
238			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?	Yes			
239	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?	Yes			
240	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?	Yes			Where possible. It cannot be done for 3rd party applications that are not pushed out by our Device Management suite.
241	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?	Yes			
242			MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	Yes			All devices that connect to the Exchange servers must meet a minimum set of policies that are applied at the Exchange/ActiveSync level. All devices that receive certificate based remote VPN access to Cisco are subject to enrollment in the dedicated Mobile Device Management (MDM) solution.
243			MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Yes			
244	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?	Yes			
245			MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	Yes			

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
246			MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Yes			
247	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?	Yes			The Cisco Mobile Device document governs the roles and responsibilities of mobile device users. On the Cisco managed device, Cisco owns company data; personal data is owned by the individual. Service cancellations (e.g. when user is terminated) result in removal of access. In emergency termination scenarios the mobile device is wiped.
248			MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Yes			The Cisco Mobile Device document governs the roles and responsibilities of mobile device users. On the Cisco managed device, Cisco owns company data; personal data is owned by the individual. Service cancellations (e.g. when user is terminated) result in removal of access. In emergency termination scenarios the mobile device is wiped.
249	Mobile Security Security Patches	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Yes			Where possible. When patches are available, users must install them. We use minimal OS enforcement to prevent unpatched devices from accessing critical services.
250			MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Yes			All devices that connect to the Exchange servers must meet a minimum set of policies that are applied at the Exchange/ActiveSync level. All devices that receive certificate based remote VPN access to Cisco are subject to enrollment in the dedicated Mobile Device Management (MDM) solution.
251	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?	Yes			
252			MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	Yes			
253	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?	Yes			Cisco InfoSec has established regular contacts with the U.S. Federal Bureau of Investigation (FBI), U.S. Secret Service, U.S. Customs, U.S. Internal Revenue Service (IRS), U.S. Office of the Attorney General, U.S. Department of Defense, Interpol, Scotland Yard, Internet Engineering Task Force (IETF), IntelliShield, Symantec, DHS NCCIC, US-CERT, CERT/CC, Forum of Incident Response and Security Teams (FIRST) as well as FVEY based organizations (UK NCSC, UK MoD, Australian Federal Police and DoD, Canadian CCIRC and CSEC). In addition, InfoSec has established relationships with academic institutions, customers, regulatory bodies, and local law enforcement agencies to foster a relationship of trust and credibility through the exchange of information about intelligence and security matters.
254	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?	Yes			A comprehensive Incident Response Plan is maintained in an internal wiki and undergoes a review annually, but is often periodically updated as the plan is put into effect. Nearly every incident is initially treated as a potential security incident.
255			SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		No		Cisco has an established Computer Security Incident Response Team (CSIRT) that provides proactive threat analysis, incident detection, and coordinated incident response. CSIRT coordinates and investigates policy violations, unauthorized access to Cisco assets, malicious code related incidents, and other security incidents. CSIRT does not integrate customized client requirements into our CSIRT handbook.
256			SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	No			Cisco does not publish a document, but if a tenant was interested in reviewing the incident response plan, and the greater SecOps Playbook that contains the roles and responsibilities, the request can likely be accomodated.
257			SEF-02.4		Have you tested your security incident response plans in the last year?	Yes			On an annual basis, Cisco performs end to end testing of the incident response infrastructure. Employees within the Incident Response Teams perform simulated incident events to ensure personnel understand their role and responsibilities and ensure the plan is updated to reflect new risks or gaps. The CSIRT Handbook is a working document that details incident policies and procedures; therefore, it is tested annually at minimum as the CSIRT team investigates incidents. After each test is performed, there is a thorough review of the process that was followed. The test results are reviewed to determine what was successful and where mistakes were made.
258	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?	Yes			CSIRT utilizes Splunk to index and correlate data source in a searchable repository for analysis and alerting. The CSIRT EA Playbook is a prescriptive collection of repeatable methods (reports) to detect security and respond to security incidents. While the bulk of the content of the Playbook is dedicated to documenting the scheduled reports and the follow-up required for each, it also provides detailed instructions on report standardization, and how to keep detection and responds methods up to date.
259			SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes			Yes, the tenant logs are isolated to their own indexes.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
260	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?	Yes			Cisco follows procedures for collecting and handling evidence through legally admissible court standards that includes chain of custody and documentation. http://www.cisco.com/web/about/security/intelligence/csirt_rfc2350.html
261			SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes			The CSIRT Incident Response Handbook includes forensic evidence guidelines that define specific procedures for chain of custody to preserve the integrity of digital evidence for use in internal, civil, or criminal action. Cisco follows procedures for collecting and handling evidence through legally admissible court standards that includes chain of custody and documentation.
262			SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes			Data labelling and routing provides flexibility to accommodate almost any request.
263			SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes			
264	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?	Yes			CSIRT works with the business to determine and quantify annual loss of revenue as a result of information security incidents based on the types and volumes.
265			SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	Yes			
266	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?	Yes			"Cisco's Cloud Service Provider Management Office has a program called Cloud and Application Service Provider Remediation Process (CASPR). The CASPR governs the use of third party providers or vendors to manage Cisco business. The process evaluates the security posture and overall stability of Cloud Service Providers (CSPs) used by Cicso to minimize risk to Cisco's data by identifying and remediating risks associated with CSPs. Customers retain control and ownership over the quality of their data and potential quality errors that may arise through the usage of Cisco products and services."
267			STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Yes			"Cisco's Cloud Service Provider Management Office has a program called Cloud and Application Service Provider Remediation Process (CASPR). The CASPR governs the use of third party providers or vendors to manage Cisco business. The process evaluates the security posture and overall stability of Cloud Service Providers (CSPs) used by Cicso to minimize risk to Cisco's data by identifying and remediating risks associated with CSPs. Risks are tracked through remediation with the provider. Cisco enforces the rule of least privilege through segregation of duties and access restriction based by roles and job functions."
268	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)?	Yes			Cisco does have a public policy for addressing vulnerabilities in its products and services. Information is located here: https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities
269	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?	Yes			
270			STA-03.2		Do you provide tenants with capacity planning and use reports?		No		
271	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?	Yes			Information security policies are monitored and enforced through manual and automated monitoring processes. A manual monitoring process can be ad hoc, such as watching e-mail on a large alias, receiving a policy violation report from an individual, discovering a violation while using an application, or identifying violations as part of a consulting engagement review of an architecture, design, or process. An automated monitoring process tests or samples certain transactions or interactions, flagging potential policy violations for further review.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
272	Supply Chain Management, Transparency, and Accountability Third Party Agreements	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Yes			Cisco's Procurement Services and Supply Chain Management contracts address data legal complance requirements and are reviewed as part of the CASPR Process. Specifically, a Data Impact Analysis is performed as part of every assessment.
273			STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes			Cisco's Procurement Services and Supply Chain Management contracts address data legal complance requirements and are reviewed as part of the CASPR Process. Specifically, a Data Impact Analysis is performed as part of every assessment.
274			STA-05.3		Does legal counsel review all third-party agreements?	Yes			All third party agreements have to go through legal review for approval.
275			STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	Yes			Cisco's third party user agreements include requirements around security and protection of information and assets. Customer specific agreements is dependent on the products and services provided.
276			STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		No		Cisco maintains a list of all subprocessing agreements however this is Cisco Confidential and cannot be shared.
277	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?		No		Cisco's standard contracts address the responsibility and liability of their suppliers use of third party processors.
278	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)?	Yes			Cisco's legal team reviews all customer agreements for approval and has provisions to ensure that the contract is agreed at high level terms that aligns with Cisco's policies, procedures and technical measures implemented.
279			STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Yes			The CASPR process performs regular compliance reviews and re-assessments of its primary suppliers. Part of this includes updating terms and requirements over time.
280			STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes			The CASPR process performs risk management and service alignment to the business requirements.
281			STA-07.4		Do you review all agreements, policies, and processes at least annually?	Yes			All Cisco policies and functional policies including any processes if applicable must be updated as needed and reviewed at least every two years or more often if business conditions necessitate changes to assure alignment with current practices.

	Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Answer: Yes	Answer: No	Answer: N/A	Notes
282	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?	Yes			The CASPR process performs annual compliance reviews and re-assessments of its primary suppliers processing high-risk and customer data.
283			STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes			The CASPR process performs annual compliance reviews and re-assessments of its primary suppliers processing high-risk and customer data.
284	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?	Yes			With pre-authorization and coordination, we permit 3rd party assessments of our service.
285			STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes			The annual CATO (Cloud Approval to Operate) renewal includes a mandatory third party penetration test. Vulnerability scans are daily, and findings are put into a work-tracking ticket and assigned to the designated individual for due action based on severity.
286	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?	Yes			Per policy for certified production requirements.
287			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?	Yes			
288	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?	Yes			
289			TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
290			TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
291			TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	Yes			Vulnerability scans may be provided, with appropriate agreements in writing and approved by Cisco DPP Legal, and possibly other Cisco-internal authorities, and with the use of a mutually acceptable safe-exchange medium.
292			TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Yes			We use automated configuration management and orchestration systems to coordinate rapid and consistent patching across the environment.
293			TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?	Yes			Patching time frames may be provided, with appropriate agreements in writing and approved by Cisco DPP Legal, and possibly other Cisco-internal authorities, and with the use of a mutually acceptable safe-exchange medium.
294	Threat and Vulnerability Management Mobile Code	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes			Cisco has established Application Vulnerability Assessment (AVA) standard for scanning the applications for insecure (vulnerable) code as per the Application Security Policy.
295			TVM-03.2		Is all unauthorized mobile code prevented from executing?	Yes			It is required for all applications that high and medium severity vulnerabilities identified during the scanning must be closed before deployment.