IBM Bluemix PaaS Platform

V1.0 Oct 2017

Introduction

Designed using secure engineering practices, the IBM Bluemix PaaS Platform has layered security controls across network and infrastructure. It aligns with a broader set of IBM security and privacy standards which are referenced where applicable in this CSA CAIQ submission. Bluemix ensures security readiness by adhering to security policies that are driven by best practices in IBM for systems, networking, and secure engineering. These policies include practices such as source code scanning, dynamic scanning, threat modelling, and penetration testing. In addition, Bluemix provides a group of security services that can be used by application developers to secure their mobile and web apps. These elements combine to make Bluemix a platform with clear choices for secure application development. Bluemix Public and Dedicated use Bluemix Infrastructure-as-a-Service (IaaS) cloud services and take full advantage of its security architecture. Bluemix IaaS provides multiple, overlapping tiers of protection for your applications and data. In addition, Bluemix adds security capabilities at the Platform as a Service layer in different categories: platform, data, and application.
IBM Bluemix PaaS Platform has been assessed by independent auditors as part of many compliance standard certifications including ISO 27001 and SOC2. Refer to this link for more details on the different compliance standards applicable to IBM Bluemix Platform
https://console.bluemix.net/docs/security/compliance.html#compliance

For more reading on how IBM security and privacy standards ensure complete privacy and security for our customer data, refer to these links
https://www.ibm.com/security/secure-engineering/
https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy

For IBM Bluemix PaaS Platform, refer to these links for additional information on using Bluemix to develop and deploy secure applications and services.
https://console.bluemix.net/docs/security/index.html#security
https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/
https://developer.ibm.com/bluemix/

The CAIQ was designed to help with one of the leading concerns that companies have when moving to the cloud: the lack of transparency into what technologies and tactics cloud providers implement, relative to data protection and risk management, and how they implement them. This CAIQ document gives detailed responses to those questions for the IBM Bluemix PaaS Platform and provides additional links where required on IBM and Bluemix security processes.

Control Group	CID	Consensus Assessment Questions	IBM Response
Application & Interface Security *Application Security*	AIS-01.1	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)?	The IBM Secure Engineering Standard ensure security as part of our SDLC. Those standards include processes for secure coding, vulnerability assessment, penetration testing, education, processes for 3rd party code approval and threat modelling. The standards used are regularly evaluated and updated for inclusion or replacement. See https://www.ibm.com/security/ Penetration testing is performed by both IBM and third parties and covers both external and internal testing of endpoints. Vulnerability assessment requires automated code and application scanning in addition to manual testing. Secure coding mandates manual review for secure related code and reviews against OWASP top ten attacks. Blumemix has been certified by an independent auditor against the ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modelling, manual code reviews, and other techniques.
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modelling, manual code reviews, and other techniques.
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Development work for the Bluemix PaaS Platform is not outsourced. For all 3rd party components used, e.g. libraries or open source code, the IBM Secure Engineering Standard prohibits their use unless approved by IBM's Open Source Software Process. That approval process includes technical, legal and marketing reviews.
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modelling, manual code reviews, and other techniques. New functionality or code may not be moved to production without a threat model and vulnerability assessment being performed
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	IBM Bluemix customers are ultimately responsible for the data integrity of their workload. IBM Bluemix compliance certifications demonstrate the controls Bluemix has in place to provide a secure platform. https://console.bluemix.net/docs/security/compliance.html - compliance
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	Requirements and trust levels for customer access are established contractually for each Customer.
Application & Interface Security *Data Integrity*	AIS-03.1	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?	IBM Bluemix customers are ultimately responsible for the data integrity of their workload. SOC2 compliance demonstrates the controls IBM Bluemix has in place to safeguard against the unauthorized access, destruction, loss or alteration of data stored in Bluemix.
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	All IBM Bluemix PaaS Platform data is encrypted in transit. Data in transit encryption uses TLS from internet to the reverse proxy at edge of Bluemix Platform network which terminates TLS. IPSEC based encryption is provided within the Bluemix Platform network for all data in transit from the reverse proxy to Bluemix components. IBM Bluemix customers must ensure their applications are TLS enabled. Custom certs can be associated with the Bluemix application endpoints using the UI as outlined here: https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemix-custom-domains/ Data at rest encryption for a Bluemix application's data is the responsibility of the application developer, and they can use services provided by Bluemix to do so - see details under the Cloud Data Services section of the Bluemix Services catalogue.
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	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.)?	IBM Bluemix PaaS Platform uses external auditors to conduct multiple structured, industry standard audit assertions and reports. See https://console.bluemix.net/docs/security/compliance.html - compliance
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	IBM Bluemix PaaS Platform provides relevant third party audit certification reports where a Non-Disclosure Agreement (NDA) is in place.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Penetration testing is performed by IBM teams against IBM Bluemix PaaS Platform staging environments on at least a quarterly basis. This testing covers network and application level testing and includes testing for both SANS top25 and OWASP top ten vulnerabilities. 3rd-party vendors (external) perform application and network penetration against IBM Bluemix PaaS Platform Pen Test production environments (public and private clouds) on an annual basis. Those tests include both external testing against public endpoints and internal testing where the vendor is provided with access to the environment to test for
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	

Control Group	CID	Consensus Assessment Questions	IBM Response
			any internal network vulnerabilities or weaknesses. For Public Bluemix, we can make available SOC2 report for clients who are under IBM NDA as we need to show evidence of penetration testing and vulnerability scanning to SOC2 auditor. For Dedicated Bluemix clients, we can make available penetration test and vulnerability scan reports "on request" to clients for their own Dedicated Bluemix environments on approval by IBM CISO.
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Internal audits are conducted on at least an annual basis.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	IBM Bluemix PaaS Platform uses external auditors to conduct multiple structured, industry standard audit assertions and reports. See https://console.bluemix.net/docs/security/compliance.html - compliance
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	For Public Bluemix, which is multi-tenant, we can make available SOC2 report for clients who are under IBM NDA as we need to show evidence of penetration testing and vulnerability scanning to SOC2 auditor. For Dedicated Bluemix clients, we can make available penetration test and vulnerability scan reports "on request" to clients for their own Dedicated Bluemix environments on approval by IBM CISO.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	IBM Bluemix PaaS Platform provides relevant third party audit certification reports where a Non-Disclosure Agreement (NDA) is in place. Internal audit report releases must be approved by the IBM Office of the CIO.
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	IBM Bluemix PaaS Platform uses multiple internal entities to conduct cross functional audit assessments.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	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?	IBM Bluemix Customers are responsible for the encryption of their data at rest but Bluemix Cloud Data services provides a number of options to encrypt that data. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/data/ Disk Partitions where customer data resides are encrypted using LUKS
	AAC-03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	IBM Bluemix PaaS Platform customers are ultimately responsible for the data integrity of their workload. Bluemix Data services provide guidance on how to backup and recover data. Refer to the specific Bluemix Data Service within the Bluemix online documentation. https://console.bluemix.net/docs/services/WorkWithData/index.html#index Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups are encrypted and stored into IBM IaaS Evault.
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	IBM Bluemix provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
	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?	The Bluemix management team regularly surveys changes in the regulatory environment. The IBM Legal Department also monitors regulatory requirements for their impact upon IBM security programs. Customers are responsible for tracking any changes to their regulatory requirements.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	IBM Bluemix PaaS Platform provides a number of options to allow customers to deploy applications for high availability including high availability zones within a region and high availability across regions. There are a number of tutorials available at IBM developerworks and IBM Garage to assist the customer with their configurations, e.g. https://www.ibm.com/developerworks/cloud/library/cl-high-availability-and-disaster-recovery-in-bluemix-trs/index.html
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	IBM Bluemix PaaS Platform provides a number of options to allow customers to deploy applications with high availability and disaster recovery across regions.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Business continuity plans are regularly tested at least on an annual basis. The related controls have been verified by an external auditor as part of Bluemix is27001 certification.

Control Group	CID	Consensus Assessment Questions	IBM Response
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	Bluemix provides customers the options to deploy their applications and data in different regions. The data remains in that region unless the customer moves it. Customers have different options on how they connect to their blue mix dedicated instance, e.g. over public network or over a dedicated VPN from their enterprise Data transport diagrams for Dedicated environments are available to tenants.
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	Data transport can be defined up to a point but in the event of network connection failure alternate paths can be used though not specific to legal jurisdiction. Customers should take legal jurisdictions into account when designing and deploying their systems across multiple datacentres.
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information on securing applications in IBM Bluemix PaaS is readily available in Bluemix docs, https://console.bluemix.net/docs/security/index.html - security, and through various online tutorials in IBM Developerworks and Bluemix Garage Information system documents that do not impact the security or availability of other tenants are available for Dedicated environments. Some information systems documents are restricted from release approval from the IBM CIO office.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Physical and Environmental Protection controls are in place in all IBM data centres and are validated frequently through internal audits and by external auditors as part of NIST and iso27001 compliance NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06.1	Are any of your data centres located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Physical and Environmental Protection controls are in place in all IBM data centres and are validated frequently through internal audits and by external auditors as part of NIST and iso27001 compliance NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	IBM Bluemix PaaS Platform does not include Virtual Infrastructure.
	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?	IBM Bluemix PaaS Platform does not include Virtual Infrastructure.
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	IBM Bluemix PaaS Platform does not include Virtual Infrastructure.
	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?	IBM Bluemix PaaS Platform does not include Virtual Infrastructure.
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	IBM Bluemix PaaS Platform does not include Virtual Infrastructure.
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Physical and Environmental Protection controls are in place in all IBM data centres. These controls are maintained through frequent internal audits and are validated by external auditors through assessments such as FedRAMP, ISO27001 and SOC2. In addition, IBM Bluemix provides a number of options to allow customers to deploy applications for high availability including high availability zones within a region and high availability across regions.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	IBM Bluemix provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	IBM Bluemix provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	IBM Bluemix provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net

Control Group	CID	Consensus Assessment Questions	IBM Response
Business Continuity Management & Operational Resilience *Policy*	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	IBM Bluemix PaaS Platform has a set of Security Policies in place which are aligned with IBM Core Security Practices covering Systems, Networking and Secure Engineering best practices. Security readiness focal points are assigned for each Bluemix Platform component and service and are responsible to drive conformance to those security policies. All IBM employees are required to take security related education.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	IBM Bluemix PaaS Platform customers are ultimately responsible for the data integrity of their workload. Refer to the Bluemix online documentation for more details on Bluemix Data services. https://console.bluemix.net/docs/services/WorkWithData/index.html#index Data retention policies and procedures for Bluemix Metadata and logs are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups are encrypted and stored into IBM Sotflayer Evault. SOC2 compliance demonstrates the controls IBM Bluemix has in place for data retention of Bluemix metadata and logs and to safeguard against the unauthorised access, destruction, loss or alteration of data stored in Bluemix.
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	IBM Bluemix PaaS Platform does not share customer data unless subject to disclosure to government agencies pursuant to judicial proceeding, court order, or legal process. For more details on privacy and trust, refer to https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy IBM complies with the U.S.-Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data from Switzerland. International Business Machines Corporation has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. To learn more about the Safe Harbor program, and to view IBM's certification, please visit http://www.export.gov/safeharbor/
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups are encrypted and stored into IBM Sotflayer Evault.
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	Disaster recovery testing is conducted on at least an annual basis.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	IBM Secure Engineering standard provides policies on the development, reviewing and scanning of code, applications and systems prior to deployment including any changes triggered via acquisition. All deployments are controlled via Bluemix Change Management Policy and associated procedures. https://www.ibm.com/security/secure-engineering/
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	Extensive documentation is available in the form of product documentation, white papers, tutorials and videos in IBM Bluemix Docs and via IBM DeveloperWorks and IBM Bluemix Garages sites. https://console.bluemix.net/docs/ https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/ https://www.ibm.com/cloud-computing/bluemix/garage
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	Development work for the Bluemix PaaS Platform is not outsourced. For all 3rd party components used, e.g. libraries or open source code, the IBM Secure Engineering Standard prohibits their use unless approved by IBM's Open Source Software Process. That approval process includes technical, legal and marketing reviews.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include static and dynamic scans, penetration tests, threat modelling, manual code reviews, and other techniques. The CR process provides a high level of control for all software development activities. https://www.ibm.com/security/secure-engineering/
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	IBM Secure Engineering standard provides policies on the development, reviewing and scanning of code, applications and systems prior to deployment including any changes triggered via acquisition. The goal of the secure engineering standard is to assure quality and minimize risks to deployed systems. It enforces security education for all IBM staff with more specific security education based on role and mandates the use of threat modelling for all deployments which includes a risk assessment phase. https://www.ibm.com/security/secure-engineering/ IBM Bluemix is iso27001 certified by external auditors. This certification is available to customers and has different control points which focus on quality assurance and risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html - compliance

Control Group	CID	Consensus Assessment Questions	IBM Response
	CCC-03.2	Is documentation describing known issues with certain products/services available?	IBM Bluemix PaaS Platform provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	IBM Secure Engineering standard requires security validation tests and a security release checkpoint be completed before each release. https://www.ibm.com/security/secure-engineering/ IBM Product Security Incident Response Team (PSIRT) process is followed for security incident management (https://www.ibm.com/security/secure-engineering/process.html). The PSIRT team monitor and alert on any vulnerabilities discovered in any IBM system or software and each Bluemix Platform and Service has assigned PSIRT Responders to act on those vulnerabilities. SLAs are in place to ensure timely assessment on whether each component is vulnerable and subsequent patching, with the SLAs varying depending on the CVSS score.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	IBM Secure Engineering standard dictates that code reviews must be performed against a secure coding review checklist which includes checks to remove any debug code.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	IBM Bluemix PaaS Platform has a Change Control process to manage and track changes to any portion of the system, regardless of its maturity level (Experimental, Beta or GA). The change control process requires multiple levels of review approval including component owners and management. For customer private clouds, the changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance. File integrity monitoring runs on all VMs in customer environments and tracks any unauthorized changes to that VM such as identity management, networking, system management and OS configuration.
Change Control & Configuration Management *Production Changes*	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	IBM Bluemix is SOC2 certified and this includes controls on change management. Reports can be made available to customers on request. For customer private clouds, the changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance.
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	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)?	Dedicated virtual machines are assigned to customers in Bluemix dedicated environment. This information is readily available to IBM Bluemix operations and utilizes real time inventory asset tracking.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Dedicated hardware and virtual machines are assigned to each Bluemix dedicated customer. This information is readily available in the IBM IaaS portal and can be shared with customers for their environment.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	In dedicated Bluemix, customers can authenticate their own users via SSO and can utilize geography based authentication factors.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	IBM Bluemix provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	IBM Bluemix provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	IBM Bluemix customers are responsible for classifying their data
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	IBM Bluemix provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	IBM Bluemix PaaS Platform provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html Access to customer data and application metadata may be required to provide customer support, troubleshoot the service, or comply with legal requirements. information about
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	

Control Group	CID	Consensus Assessment Questions	IBM Response
			any potential access to that data from outside that region are documented and made available to customers.
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03.1	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)?	Data in transit encryption uses TLS from internet to the reverse proxy at edge of Bluemix Platform network which terminates TLS. IPSEC based encryption is provided within the Bluemix Platform network from the reverse proxy to Cloud Foundry Router and from Cloud Foundry Router to the Cloud Foundry application container host in which the Bluemix application runs. IBM Bluemix customers must ensure their applications are TLS enabled. Custom certs can be associated with the Bluemix application endpoints using the UI as outlined here: https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemix-custom-domains/ or using an API outlined here: http://bluemixapi-docs.stage1.mybluemix.net/swagger/?api=api-server#/default
	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)?	IPSEC based encryption is utilised for all component to component traffic.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	IBM Bluemix follows IBM Corporate Standards which dictate an extensive labeling and handling scheme for all assets containing IBM owned data. Containers with customer data are labelled and treated as such. IBM Bluemix customers are responsible for managing and labelling their own data.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	IBM Bluemix has segregated development, staging and production environments deployed in different VLANs in different IaaS accounts. Each customer environment is considered to be a production environment but Bluemix provides customers with the ability to deploy code into production and non-production spaces. It is the customer's responsibility to restrict the movement of workload between their environments and ensure production data is not replicated to non-production environment. https://www.ibm.com/developerworks/cloud/library/cl-intro4-app/index.html
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	IBM Bluemix follows IBM Corporate Standards which dictate an extensive labeling and handling scheme for all IBM owned data. Containers with customer data are labelled and treated as such. IBM Bluemix customers are responsible for managing and labelling their own data.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	IBM employs a decommissioning and reclaim process for all hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. See http://blog.softlayer.com/tag/disposal
	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?	The process outlined in DSI07.1 is followed for any service being cancelled in IBM Bluemix.
Datacentre Security *Asset Management*	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	IBM Bluemix records all physical and virtual assets in a IBM asset inventory system that captures details including asset owner, classes of data managed, locations of hosting infrastructure and contact details. The asset inventory process has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html - compliance.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	Critical suppliers are documented, along with appropriate contact information.
Datacentre Security *Controlled Access Points*	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	IBM Data centres are secured, with server-room access limited to certified employees. Physical security parameters can include but are not limited to fences, walls, barriers, security guards, gates, electronic surveillance, video surveillance, physical authentication mechanisms, reception desks, and security patrols. The controls have been certified by an external auditor. See NIST 800-53 PE and ISO27001 A11 for the relevant controls https://www.ibm.com/cloud-computing/bluemix/complianceSee https://www.ibm.com/cloud-computing/bluemix/data-centersfor more details on IBM Data centre security.

Control Group	CID	Consensus Assessment Questions	IBM Response
Datacentre Security *Equipment Identification*	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	IBM Bluemix manages all assets following an IBM asset inventory process and this has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html - compliance
Datacentre Security *Offsite Authorization*	DCS-04.1	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)	IBM Bluemix provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
Datacentre Security *Offsite equipment*	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	IBM employs a decommissioning and reclaim process for all hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. See http://blog.softlayer.com/tag/disposal IBM Bluemix manages all assets following an IBM asset inventory process and this has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html - compliance
Datacentre Security *Policy*	DCS-06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	See DCS-02.1
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role.
Datacentre Security *Secure Area Authorization*	DCS-07.1	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)?	This is performed during the ordering process.
Datacentre Security *Unauthorized Persons Entry*	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	IBM Data Centre Physical security is controlled at many levels such as perimeter and building entrances, the physical security is not limited to, professional security staff, 24/7 video surveillance, security check point. Physical access points to the data halls all are recorded and monitored by onsite security, only authorized staff have the ability to access the data halls and they must authenticate a minimum of 2 times. Physical Security is reviewed by periodic internal audits as well as by third party audits such as FedRAMP, PCI, SOC, ISO27001 https://www.ibm.com/cloud-computing/bluemix/compliance
Datacentre Security *User Access*	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	
Encryption & Key Management *Entitlement*	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	IBM Bluemix has defined a Key Management process to support encryption of data at rest and in transit for all Bluemix platform components. Customers may use their own customer managed keys for their applications deployed on Bluemix using the UI as outlined here: https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemix-custom-domains/ or using an API outlined here: http://bluemixapi-docs.stage1.mybluemix.net/swagger/?api=api-server - /default
Encryption & Key Management *Key Generation*	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	All keys are managed by the IBM Bluemix PaaS Platform team and these are recycled on a regular basis. Customers may use their own customer managed keys for their applications deployed on Bluemix. Unique keys are issued to each dedicated tenant for VPN access.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	Customers may provide their own customer managed keys for their applications deployed on Bluemix and Bluemix stores these securely for the customer.
	EKM-02.3	Do you maintain key management procedures?	IBM Bluemix has Key Management policies which cover key lifecycle, key access and key strength. Access to keys are governed using the Bluemix access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. NIST recommendations for key strength and algorithms are followed. These policies have been audited by external auditors as part of iso27001 and SOC2 compliance certifications.
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	IBM Bluemix has Key Management policies which cover key lifecycle. Access to keys are governed using the Bluemix access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. Only members of the key management team can generate, recycle or revoke key and all actions are logged and sent to QRadar SIEM.

Control Group	CID	Consensus Assessment Questions	IBM Response
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	The IBM Bluemix PaaS Platform uses an internal framework to create and manage keys and certificates. NIST recommendations for key strength and algorithms are followed. These policies have been audited by external auditors as part of iso27001 and SOC2 compliance certifications.
Encryption & Key Management *Encryption*	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	IBM Bluemix Customers are responsible for the encryption of their data at rest but Bluemix Cloud Data services provides a number of options to encrypt that data. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/data/ Disk Partitions where customer data resides are encrypted using LUKS.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	All IBM Bluemix PaaS Platform data is encrypted in transit. Data in transit encryption uses TLS from internet to the reverse proxy at edge of Bluemix PaaS Platform network which terminates TLS. IPSEC based encryption is provided within the Bluemix PaaS Platform network for all data in transit from the reverse proxy to Bluemix components. IBM Bluemix customers must ensure their applications are TLS enabled. Customers have different options on how they connect to their bluemix dedicated instance, e.g. over public network or over a dedicated VPN with unique keys from their enterprise. This can apply to both end users of their applications and developers pushing new apps to Bluemix.
	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)?	IBM Bluemix Customers are responsible for the encryption of their data at rest and may encrypt it before uploading to Bluemix Cloud Data storage. Customers may use their own customer managed keys for their applications deployed on Bluemix.
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	IBM Bluemix has Key Management policies which cover key lifecycle, key access and key strength. Access to keys are governed using the Bluemix access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. NIST recommendations for key strength, and algorithm are followed.
Encryption & Key Management *Storage and Access*	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	All encryption algorithms in use are open/validated formats and are follow NIST.SP.800-57pt1 standards. Ciphers and protocols are reviewed on at least an annual basis and updated accordingly. A minimum of TLS 1.1. is mandated across Bluemix
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	IBM Bluemix manages all keys for the Bluemix platform in a proprietary store that meets NIST standards. Access to the store is only available to members of the Key Management team with membership of that team being governed by Bluemix User Access governance. Customers may use their own customer managed keys for their applications deployed on Bluemix and these are stored in a one-way process in a virtual key store which is not accessible by operations staff. Customers may encrypt their own data prior to storing in Bluemix Cloud Data storage and are responsible for storage of those encryption keys.
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	
Governance and Risk Management *Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	IBM Bluemix maintains system baselines for all critical components and this had been verified by an independent auditor as part of ISO 27001 certification. IBM Bluemix Customer applications are deployed in standard cloud foundry containers in hardened VM images.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Agents are deployed at OS level in all Bluemix machines and these check compliance with a set of security standards on a daily basis. Those security standards follow the Bluemix security policies and checklists which in turn align with iso27001 standards.
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	IBM Bluemix applications are deployed in standardized cloud foundry containers.
Governance and Risk Management *Risk Assessments*	GRM-02.1	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)?	Security logs are created for all critical operations in the Bluemix Platform e.g. authentication, privileged operations, key management. These are available on request to all Bluemix dedicated customers for their dedicated environment. SOC2 and iso27001 reports are available on request and demonstrate the use of security controls in Bluemix. https://console.bluemix.net/docs/security/compliance.html - compliance
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	IBM Secure Engineering standard requires that threat modelling be carried out on at least an annual basis and part of that methodology is risk assessment. See https://www.ibm.com/security/secure-engineering/ IBM Bluemix is iso27001 certified by external auditors. This certification has different control points which focus on risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html - compliance

Control Group	CID	Consensus Assessment Questions	IBM Response
Governance and Risk Management *Management Oversight*	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	IBM Security standards require managers to own the security and risks for their services and Bluemix is027001 certification the controls and processes in place to manage that. IBM Bluemix managers must appoint a security focal to manage security and compliance for their component or service. IBM Secure Engineering standard requires all employees to take security education on an annual basis.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	IBM Bluemix is iso27001 certified by external auditors with that certification being available to customers. Iso27001 is focused on security management processes and how IBM Bluemix security processes map to iso27001 controls. https://console.bluemix.net/docs/security/compliance.html#compliance More detailed information on IBM Security processes can be made available to customers under NDA.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	IBM ISMP is reviewed on an annual basis.
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	IBM Bluemix is iso27001 certified by external auditors with that certification being available to customers. As part of Iso27001 certification, controls and policies for service providers are reviewed. https://console.bluemix.net/docs/security/compliance.html - compliance
Governance and Risk Management *Policy*	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	IBM information security and privacy policies align with industry standards. Agreements are in place to verify and monitor supplier compliance with industry standards. IBM Bluemix is iso27001 certified by external auditors with that certification being available to customers. As part of Iso27001 certification, controls and policies for engaging with service providers are reviewed. https://console.bluemix.net/docs/security/compliance.html - compliance
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management *Policy Enforcement*	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes, this is established by IBM Corporate HR policies, standards, training, and processes.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes, this is established by IBM Corporate HR policies, standards, training, and processes.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Regular risk assessments are conducted according to NIST800-53 standards. Policies, procedures and standards are subject to revision as a result of the holistic risk assessment as well as the risk assessments required as a part of the secure engineering process.
Governance and Risk Management *Policy Reviews*	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Tenants are notified of any change to their environment including those resulting from modified security policies. All deployments are controlled via Bluemix Change Management Policy and Bluemix Dedicated customers are approvers for any changes that happen outside agreed maintenance windows.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Security policies are reviewed at least annually. The privacy policy is updated and reviewed by the IBM Corporate Privacy Office.
Governance and Risk Management *Assessments*	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Regular risk assessments are conducted according to NIST800-53 standards. These include likelihood and impact for all identified risks using qualitative and quantitative methods.
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Regular risk assessments are conducted according to NIST800-53 standards. This includes the independent consideration of all risk categories.
Governance and Risk Management *Program*	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	IBM Secure Engineering standard mandates the use of threat modelling for all deployments which includes a risk assessment phase. https://www.ibm.com/security/secure-engineering/ IBM Bluemix is iso27001 certified by external auditors. This certification is available to customers and has different control points which focus on quality assurance and risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html#compliance
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	

Control Group	CID	Consensus Assessment Questions	IBM Response
Human Resources *Asset Returns*	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	IBM Bluemix has a security incident response plan which aligns with IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected security incident involving any Bluemix or Customer system or data. That scope covers any incidents related to privacy. Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	IBM privacy policy is aligned with industry and country requirements and is continuously monitored for updates Refer to https://www.ibm.com/cloud-computing/bluemix/security-privacy - privacy
Human Resources *Background Screening*	HRS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	IBM Corporate HR policies dictate that all employment candidates are subject to background verification. IBM Bluemix does not use contractors or other third parties to access client environments.
Human Resources *Employment Agreements*	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for Bluemix team members based on their role. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	IBM employees must acknowledge completion of training and this acknowledgment is documented and stored.
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	All employees of IBM sign NDA or confidentiality agreements regarding corporate and client information.
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Timely completion of the training program is a prerequisite to gaining access to customer data.
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Refer to https://www.ibm.com/security/secure-engineering/
Human Resources *Employment Termination*	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	IBM Corporate HR policies provide a baseline of standards for changes in, and termination of employment. The IBM Bluemix access control tool queries the IBM Corporate system to detect any employee terminations on a daily basis.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	IBM Corporate HR policies provide a baseline of standards for Access to IBM Bluemix PaaS Platform is managed via IBM Bluemix User Access Management tool which ensures role based access to any Bluemix system. Approval is required from both the employee manager and the system access owner and the process includes approval/continued business need and validation/revocation on employee termination.
Human Resources *Portable / Mobile Devices*	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	IBM I.T. Security standards mandate that mobile devices are not permitted access to the customer environment. Privileged laptops are required for access to customer environments and owners of those laptops are required to install and maintain full disk encryption and other increased security controls.
Human Resources *Nondisclosure Agreements*	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	All IBM Bluemix policies and procedures are reviewed on at least an annual basis.
Human Resources *Roles / Responsibilities*	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	All roles and responsibilities relating to information security and environment operations are documented for dedicated environments.
Human Resources *Acceptable Use*	HRS-08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	Refer to IBM Privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy - privacy
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	Refer to IBM Privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy - privacy

Control Group	CID	Consensus Assessment Questions	IBM Response
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Customers can inform IBM to avoid further contact beyond fulfilling the customer request. Refer to the IBM privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy - privacy
Human Resources *Training / Awareness*	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources *User Responsibility*	HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	IBM Secure Engineering standard mandates security education for all team members on an annual basis and that security education involves a formal registration that education is complete. In addition, IBM employees regularly receive notifications on the importance of cybersecurity, asset registration and asset security via email, online resources and other. Privileged laptops are required for access to customer environments or where the user is a privileges user for a particular regulatory requirement. Owners of those laptops are required to install and maintain full disk encryption and other increased security controls to satisfy regulatory standards.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources *Workspace*	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	Tenant and service level conflicts of interest are resolved via operational and management planning.
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	IBM Bluemix customers are ultimately responsible for the data integrity of their workload. SOC2 compliance demonstrates the controls IBM Bluemix has in place to safeguard against the unauthorised access or alteration of data stored in Bluemix. Security logs for all critical operations in the IBM Bluemix Platform are logged to the IBM QRadar SIEM. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to Bluemix Platform QRadar. IBM personnel managing Bluemix Platform QRadar are distinct from those having privileged access to Bluemix Platform and this is enforced using Bluemix Platform access governance tool.
	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?	IBM Bluemix Platform deploys standard hardened VM images to deploy new images. Access to VM image repositories is managed via an IBM Bluemix User Access Management tool. Approval is required from both the employee manager and the system access owner and includes approval/continued business need and validation/revocation on employee termination. All changes must be approved by IBM Bluemix Change Management process before being pushed to production. All changes and privileged actions to VM images are logged and sent to IBM QRadar SIEM.
Identity & Access Management *Audit Tools Access*	IAM-01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	All privileged users request operating system level, network device and Bluemix PaaS Platform level access via an IBM Bluemix User Access Management tool. Approval is required from both the employee manager and the system access owner. This provides the user with role based access to the requested system. Password policy per IBM IT standards are enforced for such accounts. IBM Bluemix has daily reconciliation processes which verify that all privileged users are still valid in the IBM Employee directory. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
	IAM-01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
Identity & Access Management *User Access Policy*	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Privileged accesses to IBM Bluemix is revoked on employee termination. There is a periodic revalidation for business need and reconciliation against target systems, and password policy per IBM IT standards are enforced for such accounts.
	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?	This process is tested through our external audits, and is tested repeatedly throughout the year.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Dedicated secure networks are used for administration of IBM Bluemix systems and these networks are segregated from the public networks through which customer user traffic flows.

Control Group	CID	Consensus Assessment Questions	IBM Response
Identity & Access Management *Policies and Procedures*	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	See IAM-01.1
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	See IAM-01.1
Identity & Access Management *Segregation of Duties*	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	IBM Bluemix change management procedure defines clear lines between the groups that develop code and those that are permitted to deploy it after proper approvals. Access governance provides role based access to Bluemix production and the approval process requires a valid business.
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Access to source code repositories is managed via an IBM Bluemix User Access Management tool. Approval is required from both the employee manager and the system access owner and includes approval/continued business need and validation/revocation on employee termination. All changes must be approved by IBM Bluemix Change Management process before being pushed to production.
	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?	Application developers are authenticated to Bluemix PaaS Platform using IBM WebID or via SAML federation to a client provided identity provider or a client provided LDAP in the case of Dedicated Bluemix. OAuth based Cloud Foundry mechanisms to ensure each application developer only has access to the applications and service instances that they created.
Identity & Access Management *Third Party Access*	IAM-07.1	Do you provide multi-failure disaster recovery capability?	Bluemix provides a number of options to allow customers to deploy applications for high availability including high availability zones within a region and high availability across regions. There are a number of tutorials available online to assist the customer with their configurations. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html https://www.ibm.com/developerworks/cloud/library/cl-high-availability-and-disaster-recovery-in-bluemix-trs/index.html
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM-07.3	Do you have more than one provider for each service you depend on?	
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provide a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08.1	Do you document how you grant and approve access to tenant data?	IBM Bluemix customers are ultimately responsible for the data integrity of their workload. Bluemix has been audited by external auditors as part of SOC2 compliance and this includes controls IBM Bluemix has in place to safeguard against the unauthorised access or alteration of data stored in Bluemix. https://console.bluemix.net/docs/security/compliance.html - compliance
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management *User Access Authorization*	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	IBM Bluemix PaaS Platform privileged users request operating system level, network device and Bluemix PaaS Platform level access via an IBM Bluemix User Access Management tool. This access is used to deploy and manage new Bluemix environments and organizations before handing them over to customers. Customers can appoint their own administrators to manage their Bluemix organizations, spaces and user roles as described in Bluemix documentation. https://console.bluemix.net/docs/admin/orgs_spaces.html
	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?	IBM Bluemix PaaS Platform privileged users request operating system level, network device and Bluemix PaaS Platform level access via an IBM Bluemix User Access Management tool. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM. These, and other controls evaluated as part of SOC2 certification, are designed to prevent unauthorized access to Bluemix data by IBM employees or other. Customers can appoint their own administrators to manage their Bluemix organizations, spaces and user roles as described in Bluemix documentation. https://console.bluemix.net/docs/admin/orgs_spaces.html
Identity & Access Management *User Access Reviews*	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Privileged accesses to IBM Bluemix has a periodic revalidation for business need and reconciliation against target systems and access is revoked on employee termination. The process is tested by external auditors as part of SOC2 controls. https://console.bluemix.net/docs/security/compliance.html - compliance

Control Group	CID	Consensus Assessment Questions	IBM Response
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Inappropriate entitlements trigger a security defect in the Bluemix ticketing system and that tracks the actions taken on user ids and their entitlements.
	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?	Where there is suspected inappropriate access to a customer system or customer data, IBM Bluemix notifies the IBM Cybersecurity Incident Response Team (CSIRT) and the CSIRT process includes analysis, forensics and root cause analysis for the security incident IBM legal are involved and the customer is kept informed at all stages. The Bluemix status page https://developer.ibm.com/bluemix/support/ - statusis used for all client notifications including "general" security related notifications. Security notifications point to IBM security bulletins published per the IBM Product Security Incident Response Team (PSIRT) (https://www.ibm.com/security/secure-engineering/process.html) process.
Identity & Access Management *User Access Revocation*	IAM-11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Privileged accesses to IBM Bluemix has a periodic revalidation for business need and reconciliation against target systems and access is revoked on employee termination. The process is tested by external auditors as part of SOC2 controls. https://console.bluemix.net/docs/security/compliance.html - compliance
	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?	
Identity & Access Management *User ID Credentials*	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	IBMid is the IBM Identity Service, a cloud-based identity access and management solution that provides identity and single sign-on services for IBM Cloud and IBM applications IBM Bluemix supports authentication to Bluemix PaaS Platform for application developers via SAML federation to a client provided identity provider or a client provided LDAP or SAML identity provider in the case of Dedicated Bluemix. IBM Bluemix SSO services allows developers to provide SSO for their users to blue mix applications and services. Refer to the SSO section in 'Securing Workloads in IBM Cloud' white paper https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/applications/ - sso
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	IBM Bluemix (Public) supports delegation authentication to a number of social identity sources Refer to the SSO section in 'Securing Workloads in IBM Cloud' white paper https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/applications/#sso
	IAM-12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	IBM Bluemix supports authentication to Bluemix PaaS Platform for application developers via SAML federation to a client provided identity provider or a client provided LDAP or SAML identity provider in the case of Dedicated Bluemix.
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	This can be enforced for Bluemix Dedicated tenants at tenant requests.
	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?	Role based identity management can be provided via SAML federation to a client provided identity provider Bluemix PaaS Platform provides role based access to organisations, spaces and applications which is enforced using Oauth. Organisation administrators for a customer can configure which roles and access different people within their organisation(s) have. https://console.bluemix.net/docs/iam/iamusermanage.html - iamusermanage
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	IBM Bluemix supports authentication to Bluemix PaaS Platform for application developers via SAML federation to a client provided identity provider. That identity provider may support any type of authentication including multi-factor.
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	IBM Bluemix supports authentication to Bluemix PaaS Platform for application developers via SAML federation to a client provided identity provider which can provide third-party identity assurance services.
	IAM-12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	IBMid supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Bluemix Customers can enforce any password policy they choose by using saml federation.
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	IBM Bluemix Customers can enforce any password policy they choose by using saml federation.
	IAM-12.10	Do you support the ability to force password changes upon first logon?	IBM Bluemix Customers can enforce any password policy they choose by using saml federation.

Control Group	CID	Consensus Assessment Questions	IBM Response
	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)?	IBMid supports password reset and unlocking accounts. https://www.ibm.com/ibmid/password1.html?
Identity & Access Management *Utility Programs Access*	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	IBM IaaS and IBM Bluemix PaaS Platform restrict access to administrative tools and utilities via an IBM Bluemix User Access Management tool and access is based on least privilege and best practices. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
	IAM-13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	Access to Virtual Infrastructure is restricted to only personnel who require access and all access is logged. Monitoring and controls have been reviewed by independent auditors as part of SOC2 audits. https://console.bluemix.net/docs/security/compliance.html - compliance
	IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	All IBM Bluemix systems are security hardened which includes File Integrity Monitoring to detect changes on critical files. Dedicated Bluemix with direct internet facing endpoints includes IPS which examines incoming traffic and detects known malware signatures. Those signatures are updated automatically from the IPS vendor. All logs are delivered to IBM QRadar SIEM and rules are enabled for malware detection and generation of security alerts.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Security logs for all critical operations in the IBM Bluemix PaaS Platform are logged to the IBM QRadar SIEM. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to Bluemix PaaS Platform QRadar. IBM personnel managing Bluemix PaaS Platform QRadar are distinct from those having privileged access to Bluemix PaaS Platform and this is enforced using Bluemix PaaS Platform access governance tool.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	External auditors have affirmed that IBM Bluemix controls are operating effectively against a number of standards including ISO27001/2, SSAE16 SOC2 and others. https://console.bluemix.net/docs/security/compliance.html - compliance
	IVS-01.4	Are audit logs centrally stored and retained?	Security logs for all critical operations in the IBM Bluemix PaaS Platform are logged to the IBM QRadar SIEM. Security logs are retained for one year.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	BM QRadar SIEM is configured with a set of rules which trigger offences based on incoming log events. Those offences trigger pager duty alerts to the IBM Bluemix SOC team on a 24x7 basis. Refer to the IBM QRadar documentation for more details. https://www.ibm.com/security/security-intelligence/QRadar/
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	IBM Bluemix PaaS Platform deploys standard hardened VM images to deploy new images. All changes and privileged actions to VM images are logged and sent to IBM QRadar SIEM.
	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)?	
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	IBM IaaS provides a NTP service which IBM Bluemix PaaS Platform uses. It uses dedicated radio receivers to pick up signal directly from a stratum 0 source. In turn, that means these servers feed off a stratum 1 source (our internal servers).
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	System capacity requirements for Dedicated customers are negotiated contractually.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	IBM IaaS maintains capacity and resource planning in alignment with ISO27001 and these efforts are validated by external auditors. IBM Bluemix PaaS Platform deploys applications in cloud foundry containers which are limited in terms of CPU, memory and other resource usage. The number of containers per host machine is limited.
	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?	IBM Bluemix PaaS Platform projects the anticipated capacity for the platform and ensures there is enough hardware, memory and other resources to meet that anticipated capacity. Based on the current and anticipated capacity, warning limits are in place which trigger alerts to operations when breached. That triggers another cycle of capacity planning and new warning limits. For Bluemix Dedicated, details of the current capacity usage are made available to the customer via the Bluemix Operations console.
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all	

Control Group	CID	Consensus Assessment Questions	IBM Response
		the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	The IBM Secure Engineering standard dictates multiple scanning techniques be used against production systems. These include automated dynamic scans, manual penetration tests and threat modelling. These activities both the virtualization technologies and all Virtual machines and containers deployed on those virtualization technologies. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	IBM Bluemix PaaS Platform does not offer IaaS. However, IBM Cloud does provide guidance on how to create a layered security architecture equivalence using your virtualized solution. Refer to this white paper on securing workloads in IBM Cloud. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Network architectures are regularly reviewed and updates are made after any significant change.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	IBM Bluemix PaaS Platform conducts reviews on all firewalls on a quarterly basis. These reviews check for appropriateness of access and any unauthorized changes made outside of the Bluemix PaaS Platform change control process. These firewall reviews have been assessed by external auditors as part of SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance IBM I.T. standard mandates an annual review of Bluemix network architecture. This is performed by an independent team from IBM CISO office and includes checks for appropriateness of access.
	IVS-06.4	Are all firewall access control lists documented with business justification?	All changes to IBM Bluemix firewalls must follow the Bluemix change controls process which requires business justification and multiple levels of review and approval before deployment. IBM Bluemix platform conducts reviews on all firewalls on a quarterly basis which check for any unauthorized changes made outside of the Bluemix Platform change control process.
Infrastructure & Virtualization Security *OS Hardening and Base Conrols*	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	All host machines in IBM Bluemix PaaS Platform are deployed as standard builds which remove unnecessary ports, protocols, and services. Agents deployed to all machines hosting customer traffic check for compliance with a set of hardening rules on a daily basis.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Dedicated Bluemix tenants can provision production and non-production environments via requests, as limited by their contracts.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	IBM Bluemix does not offer IaaS.
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	IBM Bluemix PaaS Platform has a non-production environment for both Public and Dedicated Bluemix used to perform any testing pre-deployment to production environment. The non-production environments are logically segregated from production environments All Bluemix dedicated environment are logically segregated and are deployed on dedicated hardware.
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	All systems and resources are protected by at least one firewall.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	All systems and resources are protected by at least one firewall. Firewall configurations and firewall reviews are assessed by external auditors as part of the applicable compliance. standard. https://console.bluemix.net/docs/security/compliance.html#compliance
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	In a dedicated environment, the customer has the option to create separate production and non-production environments and would have the responsibility to manage the firewall between them.
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	All systems and resources are protected by at least one firewall.
Infrastructure & Virtualization	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	All IBM Bluemix PaaS Platform data is encrypted in transit. IBM Bluemix does not manage any physical servers. IBM Bluemix customers are responsible for any transfer of their data and ensuring it is encrypted.

Control Group	CID	Consensus Assessment Questions	IBM Response
Security *VM Security - vMotion Data Protection*	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	IBM Bluemix PaaS Platform privileged users request access to Bluemix environments, including administrative tools, hypervisors and virtual machines, via an IBM Bluemix User Access Management tool. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM. These, and other controls evaluated as part of SOC2 certification, are designed to prevent unauthorized access to Bluemix data by IBM employees or other. All systems and resources are protected and isolated by at least one firewall. All access to administrative consoles, hypervisors and Virtual Machines is over TLS and all IBM Bluemix PaaS Platform data is encrypted in transit.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	IBM Bluemix does not have access to physical Ethernet ports, and does not have the ability to implement wireless in the environment. IBM IaaS does not permit the use of wireless networks and scans for and rogue devices are conducted routinely. These controls have been accessed by and independent auditor as part of PCI DSS AoC and can be made available to customers upon request.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	IBM Bluemix network diagrams clearly document the boundaries of different environments and systems including the Bluemix platform data flows across boundaries. IBM Bluemix customers are responsible for their own data including any compliance with any legal standards for that data. The IBM CISO office conduct an annual review of the Bluemix network architecture which includes checks on classification of Bluemix platform data, network zones and protections between zones.
	IVS-13.2	Do you implement technical measures and apply defence-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?	Firewalls restrict traffic from the internet to ports 80 and 443. Bluemix dedicated customers are responsible for specifying firewall rules in their environment and may request changes to lock down that outbound access either to the internet or via a VPN to their enterprise network. Bluemix PaaS Platform intrusion detection is provided by a combination of IBM IaaS provided capabilities (for Public and Dedicated Bluemix environments that run on IBM IaaS), capabilities at the perimeter level within firewall/DataPower and by monitoring of security logs that are consolidated within the IBM QRadar SIEM tool. Periodic scanning to detect OWASP issues are done for the Bluemix PaaS Platform endpoints.
Interoperability & Portability *APIs*	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	A list of APIs available is published at https://www.ibm.com/cloud-computing/Bluemix
Interoperability & Portability *Data Request*	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	IBM Bluemix customers are responsible for the data including the format of that data and how and when it is accessed.
Interoperability & Portability *Policy & Legal*	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Policies and procedures are in place governing the use of APIs between IBM Bluemix and third party applications.
	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?	IBM Bluemix customers are responsible for the data including how and when that data is migrated. Refer to the Bluemix Data Services documents to understand how these can assist with data migration https://console.bluemix.net/docs/
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	All IBM Bluemix PaaS Platform data is encrypted in transit. See AIS04.1
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Tenants can receive this data upon request.

Control Group	CID	Consensus Assessment Questions	IBM Response
Interoperability & Portability *Virtualization*	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	IBM Bluemix uses industry standard virtualization formats to help ensure interoperability, such as Docker Containers, Cloud Foundry and VMWare.
	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?	IBM IaaS do not have solution specific virtualisation hooks.
Mobile Security *Anti-Malware*	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role. Anti-malware awareness training, specific to mobile devices, is included in that training.
Mobile Security *Application Stores*	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	A list of approved application stores is available and has been communicated to users.
Mobile Security *Approved Applications*	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	IBM Corporate Security mandates the installation of a Mobile Device Management client on all BYODs used for IBM business. That client ensures compliance with IBM Corporate security standards including ensuring that only approved application stores can be used.
Mobile Security *Approved Software for BYOD*	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	The IBM Corporate security policy clearly states which applications and application stores are approved. Mobile Device Management is in place to block risky extensions and plugins.
Mobile Security *Awareness and Training*	MOS-05	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?	IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Cloud Based Services*	MOS-06	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?	IBM Corporate security policy defines the pre-approved vendor(s) for cloud storage on mobile devices with regards to company business data.
Mobile Security *Compatibility*	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Device Eligibility*	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	IBM Corporate security policies define the eligibility requirements to allow for BYOD usage. BYOD is not permitted to connect to customer environments or to store customer data.
Mobile Security *Device Inventory*	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	Mobile devices are not permitted to connect to customer environments or to store customer data. IBM Corporate retains control of inventories, forced patching, etc., of mobile devices.
Mobile Security *Device Management*	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	Mobile devices are required to install a mobile device management tool. No mobile devices are permitted to store, transmit or process customer data.
Mobile Security *Encryption*	MOS-11	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?	IBM Corporate security policies require full device encryption on mobile devices as well as BYOD. Sensitive data is not permitted on mobile devices or on BYOD.
Mobile Security *Jailbreaking and Rooting*	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Mobile devices are required to install a mobile device management tool. Jailbreaking or rooting is prevented and reported on.
	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?	Mobile devices are required to install a mobile device management tool. Jailbreaking, rooting, or circumventing required controls is prevented and reported on.
Mobile Security *Legal*	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	IBM Corporate Security Policies define these elements for BYOD.
	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?	BYOD are required to install a mobile device management tool. Jailbreaking, rooting, or circumventing required controls is prevented and reported on.
Mobile Security *Lockout Screen*	MOS-14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Automatic lockouts are configured for BYOD and mobile devices.

Control Group	CID	Consensus Assessment Questions	IBM Response
Mobile Security *Operating Systems*	MOS-15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	IBM Bluemix does not develop, approve or deploy mobile device operating systems or applications. IBM Corporate manages these items through change management processes and enforces them through a mobile device management tool.
Mobile Security *Passwords*	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	All mobile devices and BYOD have required passwords.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	Passwords are enforced through a mobile device management tool.
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Authentication requirements for passwords residing on the device, e.g. screen pin, can't be changed and this is enforced by a mobile device management tool.
Mobile Security *Policy*	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Data is stored on the cloud thus the corporate data is backed up. There is no device resident data except for authentication keys.
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	BYOD mobile devices are not permitted to use unapproved application stores.
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Anti-malware is required on BYOD and enforced via management tools.
Mobile Security *Remote Wipe*	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	All mobile devices have remote wipe configured through the required mobile device management tools.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	All mobile devices have remote wipe configured through the required mobile device management tools.
Mobile Security *Security Patches*	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	All mobile devices are configured to force installation of security patches deemed critical by the IBM Office of the CIO.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	All mobile devices are configured to force installation of security patches deemed critical by the IBM Office of the CIO, through the Mobile Device Management Tool.
Mobile Security *Users*	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	The policy clearly states mobile devices and BYOD systems are not permitted to access customer environments.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	The policy clearly states mobile devices and BYOD systems are not permitted to access customer environments. Users whose primary role is accessing or maintaining customer devices must use a company provided privileged workstation.
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	IBM Cybersecurity and IBM Legal maintain relationships with the proper local authorities.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	IBM Bluemix has a security incident response plan which aligns with IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected security incident involving any Bluemix or Customer system or data. Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	The IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected a suspected security incident involving any Bluemix or Customer system or data. One of their responsibilities is to engage with the customer and keep them informed on the investigation, findings and any root cause analysis actions.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/

Control Group	CID	Consensus Assessment Questions	IBM Response
	SEF-02.4	Have you tested your security incident response plans in the last year?	The Security incident response plan is reviewed and tested at least annually.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	Security logs for all successful and failed login attempts and all critical operations in the IBM Bluemix PaaS Platform, including network devices, host machines and IDS logs, are logged to IBM QRadar SIEM. IBM QRadar SIEM is configured with a set of rules which trigger offences based on incoming events across all log sources. Those offences trigger pager duty alerts to the IBM Bluemix SOC team on a 24x7 basis. Refer to the IBM QRadar documentation for more details. https://www.ibm.com/security/security-intelligence/QRadar/
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	For Bluemix dedicated environments, the potential incident activities are always attributed to a specific environment belonging to a customer. For Public Bluemix, investigation of the incident may be required to determine which customer(s) was involved.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Specific details regarding chain of custody, forensics, and litigation holds are addressed by IBM Legal and the IBM Cybersecurity Incident Response Team (CSIRT).
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Security logs for all successful and failed login attempts and all critical operations in the IBM Bluemix PaaS Platform, including network devices, host machines and IDS logs, are logged to IBM QRadar SIEM. IBM QRadar SIEM provides reports on the types and volumes of all security events and all offences triggered based on QRadar rules. All security incidents triggering the IBM Bluemix Security incident response plan have a root cause analysis which record impact and trigger actions to mitigate in future.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	For Bluemix dedicated environments, details of those offences can be shared upon request via reports delivered to their IBM operations console. The Bluemix status page is used for all client notifications including "general" security related notifications: https://developer.ibm.com/bluemix/support/ - status. Security notifications point to IBM security bulletins published per the IBM Product Security Incident Response Team (PSIRT) process. https://www.ibm.com/security/secure-engineering/process.html
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	IBM Bluemix customers are ultimately responsible for the data integrity of their workload. IBM Bluemix compliance certifications demonstrate the controls Bluemix has in place to provide a secure platform including controls related to supply chain. https://console.bluemix.net/docs/security/compliance.html - compliance
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	Refer to IAM 10.3
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	IBM Bluemix PaaS Platform projects the anticipated capacity for the platform and ensures there is enough hardware, memory and other resources to meet that anticipated capacity. Based on the current and anticipated capacity, warning limits are in place which trigger alerts to operations when breached. That triggers another cycle of capacity planning and new warning limits.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	For Bluemix Dedicated, details of the current capacity usage are made available to the customer via the Bluemix Operations console.

Control Group	CID	Consensus Assessment Questions	IBM Response
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Internal audits are conducted on at least an annual basis and check conformance and effectiveness of Bluemix Platform policies, procedures, and supporting measures and metrics.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.3	Does legal counsel review all third-party agreements?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	IBM maintains all required subprocessing agreements and makes them available as required to clients upon request.
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	IBM has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements. IBM supplier management processes are validated by external auditors as part of compliance with SOC and ISO27001.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	IBM maintains formal agreements with third party suppliers and those agreements are reviewed on an annual basis. Supplier relationships and processes are reviewed by an independent auditor as part of SOC2 compliance.
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	External audit assurance reports are reviewed for key suppliers on at least an annual basis.
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	External audit assurance reports are reviewed for key suppliers on at least an annual basis.
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Penetration testing is allowed by IBM Bluemix PaaS Platform on their own Dedicated environments with approval of IBM Cloud CISO.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Pen testing for Public and Dedicated Bluemix PaaS Platform is performed on an annual basis using a 3rd party vendor. Penetration testing for Dedicated Bluemix will only be performed and scheduled with the approval of the customer and penetration test and vulnerability scan reports can be made available upon request for their own Dedicated Bluemix environments.
Threat and Vulnerbility Management *Antivirus / Malicious Software*	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Antivirus Antimalware protection is deployed on all Windows systems at the host level and reports back to a central console managing Antivirus Antimalware. Automated updates are in place for new malware or virus signatures. All Linux systems are deployed using a pre-hardened image that is patched to the latest operating system level patches using BigFix, and they are hardened per the operating system hardening specification. The IBM GSSD team guidelines are used to determine severity of operating systems patches so they can be applied in a timely manner per our patch management policy.
	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?	

Control Group	CID	Consensus Assessment Questions	IBM Response
			The following secondary controls are in place to protect against malware 1. All systems are security hardened which includes File Integrity Monitoring to detect changes on critical files. 2. Dedicated Bluemix with direct internet facing endpoints includes IPS which examines incoming traffic and detects known malware signatures. Those signatures are updated automatically from the IPS vendor. 3. All privileged access is approved by a user's manager and an access approver, is periodically revalidated, and is revoked on user transfer or employee termination. 4. Change Management: All changes to software on systems must be approved by a reviewer and a manager. 5. Patch management is fully automated using IBM BigFix. 6. QRadar: rules on security logs from systems are enabled for malware detection and generation of security alerts. 7. PSIRT: processes enforced to update any systems or software with potential malware vulnerabilities. 8. NESSUS: vulnerability scans are run periodically.
Threat and Vulnerbility Management *Vulnerability / Patch Management*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Secure Engineering Standard ensure security as part of our SDLC. Those standards include processes for secure coding, vulnerability assessment, vulnerability scanning, penetration testing, education, processes for 3rd party code approval and threat modelling. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/ Network based vulnerability scans are run periodically using Nessus.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Secure Engineering Standard mandates vulnerability assessment which requires automated code and application scanning in addition to manual testing. Dynamic and static code scanning is performed using IBM Appscan on a monthly basis or whenever there is a major change. Manual reviews are performed for security related code and reviews check against OWASP top ten vulnerabilities.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Product Security Incident Response Team (PSIRT) process is followed for security incident management (https://www.ibm.com/security/secure-engineering/process.html). The PSIRT team monitor and alert on any vulnerabilities discovered in any IBM system including at OS level and each Bluemix Platform and Service has assigned PSIRT Responders to act on those vulnerabilities. SLAs are in place to ensure timely assessment on whether each component is vulnerable and subsequent patching, with the SLAs varying depending on the CVSS score. Nessus scans are run periodically and check for any OS level vulnerabilities detected from network scans.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	Bluemix dedicated customers can request details of Vulnerability scans for their dedicated environments. These are provided via the IBM operations console.
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	IBM Bigfix is used for managing and automating patching across Bluemix. This provides full visibility on what is patched in addition to providing the automation to push out the patches to all machines across all Bluemix environments. Refer to these public docs. https://www.ibm.com/marketplace/bigfix-patch-management
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	Bluemix dedicated customers can be provided with details of risk-based systems patching time frames upon request.
Threat and Vulnerbility Management *Mobile Code*	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	IBM Bluemix has a Change Control process to manage and track changes to any portion of the system, regardless of its maturity level (Experimental, Beta or GA). The change control process requires multiple levels of review approval including component owners and management. For customer private clouds, the changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance. File integrity monitoring runs on all VMs in customer environments and tracks any unauthorized changes to that VM such as identity management, networking, system management and OS configuration.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	