IBM® Watson®
on the IBM® Cloud
CSA CAIQ V1.0
February 2018

Introduction

IBM Watson on the IBM Cloud helps to transform businesses, enhancing competitive advantage and disrupting industries by unlocking the potential within unstructured data. Fundamental to providing a strong foundation for companies wanting to leverage Watson services, IBM uses best-in-class security and compliance processes that allow for successful execution of challenging workloads.

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 IBM Watson on IBM Cloud and provides additional links where applicable on IBM and Watson security processes, procedures &/or technical controls.

IBM Watson services are ISO27001, ISO27017, and ISO27018 compliant, and are rapidly evolving to support other types of regulated workloads. Compliance of Watson services are maintained though regular reviews by both IBM internal and 3rd party auditors.

Additional information on how Watson is securely deployed on the IBM Cloud can be found below:

- Watson Trust Center: https://ibm.biz/BdjD4r
- ISO 27001 certificate: https://ibm.biz/BdjWav
- ISO 27017 certificate: https://ibm.biz/BdjWam
- ISO 27018 certificate: https://ibm.biz/BdjWaK
- Full list of IBM products covered under 27001: https://ibm.biz/BdjWab
- IBM Cloud Services data security and privacy principles: https://ibm.biz/Bdsm3x
- Additional details around IBM Cloud compliance: https://www.ibm.com/cloud/compliance
- How to secure your applications using Watson services: https://www.ibm.com/cloud/garage/content/architecture/securityArchitecture/overview

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Watson Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	x			Watson services on the IBM Cloud leverage the IBM Secure Engineering Standard which is aligned with OWASP to 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. Watson services have 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?	x			IBM Watson services utilize multiple testing, scanning & analysis techniques before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, 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?	X			IBM Watson services utilize multiple testing, scanning & analysis techniques before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, 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?			X	Development work for IBM Watson on the IBM Cloud 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?	x			IBM Watson services utilize multiple testing, scanning & analysis techniques before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, manual code reviews, and other techniques.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			IBM Watson services customers are ultimately responsible for the data integrity of their workload. IBM Watson compliance certifications demonstrate the controls in place to provide a secure platform. Additional information available here: http://www.ibm.com/watson/watson-security.html
		AIS-02.2		Are all requirements and trust levels for customers' access defined and documented?	X			Requirements and trust levels for customer access are established contractually for each IBM Watson customer.

Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	x			IBM Watson services are only available through API calls, this significantly limits an attacker's ability to interact and compromise a service. IBM Watson customers are ultimately responsible for the data integrity of their workload. ISO27001 compliance demonstrates the controls IBM Watson has in place to safeguard against the unauthorized access, destruction, loss or alteration of data. Security testing occurs prior to production rollout to ensure input & outputs from the API are secure & meets design specifications.
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			IBM Watson on the IBM Cloud Data Security Architecture is designed using industry standards and best practices aligning with ISO27001 and NIST frameworks.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	x			IBM Watson services use external and internal auditors to conduct structured, industry standard audit assertions and reports. Extensive audit planning & preparation occurs for each audit. These are performed at a minimum annually. See http://www.ibm.com/watson/watson-security.html
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	x			IBM Watson services provide relevant third-party audit attestation, certification and/or pen testing reports where a Non-Disclosure Agreement (NDA) is in place.

		AAC-02.2	annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	x			Penetration testing is performed by IBM teams against the IBM Watson services 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 the IBM Watson services production environments at least once annually. 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 any internal network vulnerabilities or weaknesses.
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	x			Penetration testing is performed by IBM teams against the IBM Watson services 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 the IBM Watson services production environments at least once annually. 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 any internal network vulnerabilities or weaknesses.
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	x			Internal audits are routine and virtually continuous for IBM Watson on the IBM Cloud. These are initiated/conducted at least once each quarter.
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	x			IBM Watson services at a minimum, use external auditors annually to conduct ISO27001 assessments & audits.
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	x			IBM Watson services provide relevant third-party pen testing attestations &/or reports where a Non-Disclosure Agreement (NDA) is in place.
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	x			IBM Watson services provide relevant third-party audit attestations to customers at their request. Executive level reports or details may be provided where a Non-Disclosure Agreement (NDA) is in place.
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	x			IBM Watson services use multiple internal entities to conduct cross functional audit assessments. IBM has a robust internal audit organization utilizing mature processes that have been developed and refined to ensure alignment of all business units and internal organizations to corporate standards.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	x			Data at rest and in transit is encrypted. Access control technologies are leveraged in all IBM Watson services delivery models to ensure customers can only access their data & workloads. Additional layers of logical segmentation are available in Premium & Dedicated models of delivery of Watson services.
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?		x		IBM Watson services customers are ultimately responsible for their data and the integrity of any workloads communicating with Watson via API. Most IBM Watson Cloud Platform Services are stateless whereby client specific data does not persist.
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	x			IBM Watson services provide customers with options to deploy their applications and data in different regions. The data will reside in the region defined in the original solution design and specified in the services contract unless customer elects to move it themselves.

		AAC-03.4	business processes are reflected.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	x			IBM Watson services management & compliance teams regularly survey changes in the regulatory environment. The IBM Legal Department also monitors regulatory requirements for their impact upon IBM security programs. Customers are ultimately responsible for their compliance and tracking any changes to their regulatory requirements.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual	Do you provide tenants with geographically resilient hosting options?	x			IBM Watson services encourage customers to take advantage of our global deployment model to accomplish geographic resiliency.
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?		x		IBM Watson services are designed, implemented & configured utilizing HA and are exclusively hosted by IBM.

			work-around, and reference information • Method for plan invocation					
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	x			Business continuity plans are regularly tested at minimum on an annual basis. The related controls have been verified by an external auditor as part of the IBM Watson services 27001 certification.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other	Do you provide tenants with documentation showing the transport route of their data between your systems?	x			IBM Watson services provide customers the option to deploy their applications and data in different regions. For stateful services or specific customer workloads, the data remains in that region unless the customer moves it. Customers have different options on how they connect to their IBM Watson services, e.g. over public network or over a dedicated VPN to a dedicated instance.
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?	x			Direct internet connectivity is the preferred solution, but other options are available for dedicated customers. All traffic in transit to IBM Watson services are encrypted.

			redundancies in the event of planned or unplanned disruptions.					
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	x			IBM Watson services provide robust documentation within each service description to assist customers with properly configuring and usage of its services. IBM Watson services have extensive documentation on the information system, this documentation is available to authorized IBM personnel. This information may also be distributed through training where applicable.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	x			IBM Watson services are hosted in IBM data centers where physical and environmental protection controls are in place. The data center security controls have been designed & implemented based on NIST-800-53, ISO27001 & other industry standard requirements. These controls are validated frequently, at a minimum annually, by both internal audits and external auditors as part of SOC and ISO27001 compliance programs.

Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		x		IBM Watson services are hosted in IBM data centers where physical and environmental protection controls are in place. The data center security controls have been designed & implemented based on NIST-800-53, ISO27001 & other industry standard requirements. These controls are validated frequently, at a minimum annually, by both internal audits and external auditors as part of SOC and ISO27001 compliance programs.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			IBM Watson services are exclusively hosted in IBM data centers. Specific hardware restore and recovery options are transparent to customers of IBM Watson services as these are provided at the underlying IaaS layer.
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	x			This can be available in IBM Watson services dedicated delivery model.
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		x		IBM Watson services are exclusively hosted in IBM data centers.
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		x		IBM Watson services are exclusively hosted in IBM data centers.
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?		x		IBM Watson services are exclusively hosted in IBM data centers.
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			IBM Data Center Physical and Environmental Protection controls are in place in all data centers. These controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Data Center SOC reports provide additional insight the security mechanisms implemented to protect against outages. The SOC3 report is available to customers and prospective customers here: https://www.ibm.com/cloud-computing/bluemix/sites/default/files/assets/docs/SoftLayer%20SOC%203%201H%202017%20

								Report_FINAL%20%281%29_0.pdf The SOC2 report is available to customers and can be requested via the customer portal or by contacting their sales team.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?		x		IBM Watson services provide 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?		x		IBM Watson services provide 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?		x		IBM Watson services provide 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

			resources required for resumption					
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			IBM Watson services follow IBM Core Security Practices covering Systems, Networking and Secure Engineering best practices. Security readiness focal points are assigned for each Platform component and service and are responsible to drive conformance to those security policies. All IBM employees are required to take security related education annually.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of	Do you have technical control capabilities to enforce tenant data retention policies?	x			Specific data retention configuration options are available to customers utilizing dedicated IBM Watson services.

		BCR-11.2	any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	x			IBM Watson services do 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 http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp, https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy , https://www-01.ibm.com/software/info/product-privacy/
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			IBM Watson services are designed with High Availability as a key requirement. The services are deployed with redundancy as part of the design. Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard.
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	x			IBM Watson services are designed, implemented & configured utilizing High availability (HA) and are exclusively hosted by IBM. Business continuity plans are regularly tested at minimum on an annual basis. The related controls have been verified by an external auditor as part of the IBM Watson services 27001 certification. Data backup is a customer retained responsibility.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			IBM Watson services have 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. 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 IBM 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?	x			Extensive documentation is available in the form of product documentation, white papers, tutorials and videos in IBM Cloud Docs and via IBM developerWorks and IBM Cloud Garage 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	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	x			Development work for the IBM Watson services is not outsourced. The IBM Secure Engineering Standard prohibits use of all 3rd party components used, e.g., libraries or open source code 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?	x			IBM Watson services utilize multiple testing, scanning & analysis techniques before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, manual code reviews, and other techniques. These tests occur on all code that makes up IBM Watson services.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you provide your tenants with documentation that describes your quality assurance process?	x			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. Additional details are available here: https://www.ibm.com/security/secure-engineering/ IBM Watson services are ISO27001 certified by external auditors. This certification is available to customers and has several control points which focus on quality assurance and risk assessment methodology.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	x			IBM Watson services provide 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?	x			IBM Watson services provide 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 https://www.ibm.com/security/secure-engineering/process.html
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	x			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	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			IBM Watson services have 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 dedicated 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.

Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	x			IBM Watson services are ISO27001 certified and this includes review of controls on change management. Reports can be made available to customers on request. For customer dedicated 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	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	x			IBM Watson services leverage namespaces, tags &/or labeling methodologies/technologies for identification of customer environments and workloads.
		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	x			Specific hardware and virtual machines are assigned to customers pursuant to their contracted specifications. This capability is provided to IBM Watson services and support teams but is transparent to the customer.

		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?	x			In dedicated IBM Watson services, 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?	x			IBM Watson services provide customers with options to select in which region instances of Watson services are deployed. Data stored as part of the service remain in that region unless the customer moves it.
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	x			IBM Watson services provide customers with options to select which region instances of Watson services are deployed in. Data stored as part of the service remains in that region unless the customer moves it.
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	x			IBM Watson services leverage namespaces, tags &/or labeling methodologies/technologies for identification of customer environments and workloads. Customers are ultimately responsible for classifying & managing their data.
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	x			IBM Watson services provide customers with options to select which region instances of Watson services are deployed in. Data stored as part of the service remains in that region unless the customer moves it.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	x			IBM Watson service utilize an extensive and detailed threat modeling process where all data flows are documented prior to major releases.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	x			IBM Watson services provide customers with options to select which region instances of Watson services are deployed in. Data stored as part of the service remains in that region unless the customer moves it.

			business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.					
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	x			IBM Watson services leverage open encryption methodologies. Data in motion and at rest is encrypted using AES encryption. Data in motion is transmitted using TLS1.2.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	x			Within IBM Watson services, all data transmitted over public networks will be encrypted per IBM policy. http://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	x			IBM Watson services follow IBM Corporate Standards which dictate a labeling and handling scheme for all assets containing IBM and customer owned data.
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			x	All customer data is considered confidential and requires data to be encrypted at rest and in motion.

Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	x			IBM Watson services have processes & procedures to afford segregated development, staging and production environments. These are deployed in different VLANs in different IaaS accounts. Each customer environment is considered to be a production environment by IBM, though the customer may have multiple environments for their purposes as well. IBM Cloud provides customers with the ability to promote Watson service instances 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	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	x			IBM Watson services support staff follows IBM Corporate Standards which dictate a labeling and handling scheme for all IBM and customer owned data. IBM Watson service customers are responsible for managing and labelling their own data within the Watson service.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	x			IBM Watson services employ 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?	x			Specific Data Sanitization options are available for customers using dedicated versions of the IBM Watson services and will be defined as part of the contractual process.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	x			IBM Watson services record all physical and virtual assets in an IBM asset inventory system that captures details including asset owner, classes of data managed, and locations of hosting infrastructure and contact details. The asset inventory process has been assessed by external auditors as part of ISO27001.
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	x			IBM Watson services document critical suppliers, along with appropriate contact information.
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	x			IBM Data centers 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/compliance See https://www.ibm.com/cloud-computing/bluemix/data-centers for more details on IBM Data center security.

Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	x			IBM Watson services manage all assets following an IBM asset inventory process and this has been assessed by external auditors as part of ISO27001 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, and replication)?		x		IBM Watson services provide customers with options to deploy their services and data in different regions. That data is remains in that region unless the customer moves it.
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	x			IBM Watson services leverage an IBM Cloud decommissioning and reclaim process for all hardware or software being reclaimed or determined to be end of life. Reclaimed hard drives are 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. IBM's asset management and repurposing processes are validated frequently by external auditors through assessments including but not limited to ISO27001/17/18, SOC, and HIPAA.
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business	Can you provide evidence that policies, standards, and procedures have been established for maintaining a	x			IBM Watson services engage third party auditors to validate our compliance with many different frameworks including but not limited to ISO27001. The additional layers of the cloud underlying IBM Watson services also go through extensive third-party audits throughout each year. These include, but are not limited to, ISO27001/17/18, SOC, and HIPAA.

			processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	safe and secure working environment in offices, rooms, facilities, and secure areas?				
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	x			IBM Watson service employees complete annual required IBM security awareness training which includes training on policies, standards &/or procedures. Security awareness training is included as part of external and internal audits for verification & validation.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	x			IBM Watson services provide customers with options to select in which region instances of Watson services are deployed. Data stored as part of the service remains in that region unless the customer moves it. This is performed during the ordering & contract negotiation process.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	x			IBM Data Center 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 and external audits. https://www.ibm.com/cloud-computing/bluemix/compliance
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	x			IBM Data Center 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 and external audits. https://www.ibm.com/cloud-computing/bluemix/compliance

Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?			x	IBM has defined a Key Management policy to support encryption of data at rest and in transit for all Watson platform components. Encryption is managed at the disk level and keys are not tied to clients.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	x			This is available for customers using IBM Watson services dedicated service delivery models.
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			Encryption keys on the back end of the IBM Watson services are managed & maintained by IBM.
		EKM-02.3		Do you maintain key management procedures?		X		IBM Watson services have a robust Key Management solution to ensure security throughout the key lifecycle, including key access, strength, rotation, & revocability. Key management procedures are in the process of being documented.
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			IBM Watson services have a robust Key Management solution to ensure security throughout the key lifecycle, including key ownership at each stage of the lifecycle.
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			IBM Watson services have implemented a robust Key Management solution that leverages open source, 3rd party & proprietary components.
Encryption & Key	EKM-03	EKM-03.1	Policies and procedures shall be established, and	Do you encrypt tenant data at rest (on disk/storage) within your environment?	x			IBM Watson services encrypt data with AES & TLS1.2 encryption technologies.

Management *Encryption*		EKM-03.2	supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	x			IBM Watson services encrypt data with AES & TLS1.2 encryption technologies.
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?		x		IBM recognizes that Bring Your Own Key (BYOK) is important for some customers and will work with them to determine a mutually agreeable solution.
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	x			This is included as part of the Data Security and Privacy Principles that is included as standard contract language. Documentation is available here: http://www.ibm.com/cloud/data-security & https://www-05.ibm.com/support/operations/files/pdf/csa_us.pdf
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	x			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. By default, all connections start at TLS 1.2 and data at rest is AES 128 or better.
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	x			IBM Watson keys are owned and managed by IBM Watson.
		EKM-04.3		Do you store encryption keys in the cloud?	x			Yes, keys are stored within the IBM Cloud environment.
		EKM-04.4		Do you have separate key management and key usage duties?		x		IBM recognizes that Bring Your Own Key (BYOK) is important for some customers and will work with them to determine a mutually agreeable solution.
Governance and Risk Management	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors,	x			IBM maintains system baselines for all critical components and this had been verified by an independent auditor as part of ISO 27001 certification.

Baseline Requirements			acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	operating systems, routers, DNS servers, etc.)?				
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	x			End points are routinely monitored at the OS level to ensure compliance with a set of security standards. Those security standards follow the IBM 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?			x	IBM Watson services are only available as a service provided by IBM.
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	x			Security logs are created for all critical operations in IBM Watson services e.g. authentication, privileged operations, etc. These are available on request to Watson dedicated customers for their environment. ISO27001 reports are available on request and demonstrate the use of security controls in IBM Watson services. Customers may leverage the IBM Cloud Console to monitor for health of services. https://console.bluemix.net/status

		GRM-02.2	is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you conduct risk assessments associated with data governance requirements at least once a year?	x			IBM Watson services are ISO27001 certified by external auditors. Part of the certification requires an ISMS (Information and Security Management System) and risk management process be in place and approved by IBM senior management. Additionally, regular penetration testing is performed by both IBM internal and external teams as well as regular network and application scanning. 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/
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	x			IBM Security standards require managers to own the security and risks for their services, each must appoint a security focal to manage security and compliance for all aspects of the service. IBM Secure Engineering standard requires all employees to take security education on an annual basis. This area is reviewed annually as part of the IS027001 certification for IBM Watson services.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	x			IBM Watson services are ISO27001 certified by external auditors and available for review by customers. ISO27001 is focused on security management processes and validates that IBM Watson services security processes conform to the ISO27001 control standards. IBM Security Principles are available here: http://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	x			IBM ISMS & its specification in regard to IBM Watson services are reviewed at least annually.

			be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance					
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	x			IBM Watson services are 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.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	x			IBM information security and privacy policies are based on & align with industry standards such as NIST 800-53 and ISO27001. IBM Watson services are ISO27001 certified by external auditors with that certification being available to customers.
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	x			Agreements are in place to verify and monitor supplier compliance with industry standards. IBM Watson services are 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.

		GRM-06.3	organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	x			This effort with the CSA CAIQ reflects a mapping to regulations and standards. IBM Watson services are 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.
		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	x			This effort with the CSA CAIQ reflects a mapping to regulations and standards. IBM Watson services are ISO27001/17/18 certified by external auditors with that certification being available to customers. For additional details refer to https://www.ibm.com/watson/watson-security.html
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	x			Yes, this is established by IBM Corporate HR policies, standards, training, and processes & adhered to within IBM Watson services on the IBM Cloud.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	x			Yes, this is established by IBM Corporate HR policies, standards, training, and processes & adhered to within IBM Watson services on the IBM Cloud.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x			IBM Watson services ensure risk assessments are conducted at least quarterly. Policies, procedures and standards are subject to revision as an outcome of these assessments.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	x			IBM Watson services dedicated tenants are notified of changes to their environment including those resulting from modified security policies. All deployments are controlled via the Change Management Policy and customers are approvers for any changes that happen outside agreed maintenance windows.

		GRM-09.2	business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you perform, at minimum, annual reviews to your privacy and security policies?	x			Security policies are reviewed at least annually. The privacy policy is updated and reviewed by the IBM Corporate Privacy Office. For more details on privacy & data security policies see http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp and https://www-01.ibm.com/software/info/product-privacy/
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	x			Regular risk assessments are conducted quarterly and documented as part of the ISMS. 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)?	x			Results from regular 3rd party audits/assessments and penetration testing are one of the many feeds into the overall risk management program. Additionally, independent internal IBM compliance teams perform quarterly reviews to ensure ongoing risk identification & compliance. Threat modeling is also required for each of the Watson services.

Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	x			IBM recognizes risk assessment to be an important factor in security and has established a periodic risk assessment process that is applicable to the systems that host Watson as a Service. Assessments are entered into the IBM Governance, Risk, and Compliance program to determine & manage the current risk posture. IBM has a well-established risk management program in place that is validated as part of the annual ISO27001 audit and assessment.
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	x			Various documents are published externally regarding IBM Risk Management programs, services, & solutions. Risks identified that require customers to take an action are released as part of the PSIRT process. Additional program information available here: https://www.ibm.com/security/secure-engineering/process.html
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	x			IBM Watson services have 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 or privacy incident involving any Watson or Customer system or data. Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper and IBM incident response process here: https://www.ibm.com/security/secure-engineering/process.html https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	x			IBM privacy policies are aligned with industry and country requirements and is continuously monitored for updates See these links for more information: https://www.ibm.com/cloud/privacy http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp https://www-01.ibm.com/software/info/product-privacy/
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	x			IBM Corporate HR policies dictate that all employment candidates are subject to background verification.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x			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 IBM Watson services 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	to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you document employee acknowledgment of training they have completed?	x			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?	x			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?	x			Timely completion of the training program is a prerequisite to gaining/maintaining access to IBM computing resources, which may include sensitive systems & customer data.
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	x			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	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	x			IBM Corporate HR policies provide a baseline of standards for changes in, and termination of employment. The IBM Cloud access control solution 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?	x			IBM Corporate HR policies provide a baseline of standards to ensure all employee system access is terminated and assets are collected at time of termination. IBM Watson services are managed via an IBM Cloud IAM solution which ensures role-based access to any Watson 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	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	x			IBM IT Security standards mandate that mobile devices are not permitted access to customer environments. 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. This is managed with extensive access security controls which are validated at least annually buy 3rd party auditors.
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	x			All IBM policies and procedures are reviewed on at least an annual basis. 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 a minimum of once annually.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x			All roles and responsibilities relating to information security and environment operations are documented for dedicated environments.

Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may access tenant data and metadata?	x			Refer to IBM Privacy & Data security sites for more information. https://www.ibm.com/cloud/privacy http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp https://www-01.ibm.com/software/info/product-privacy/
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	x			This is enabled by default for all standard IBM Watson services. Customers may opt out of data usage if they chose. By default, this is disabled for Premium and Dedicated customers.
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	x			This is enabled by default for all standard IBM Watson services. Customers may opt out of data usage if they chose. By default, this is disabled for Premium and Dedicated customers.
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	x			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	access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			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/
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	x			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-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	x			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-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	x			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/
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	x			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?	x			Security logs for all critical operations are collected and sent to IBM QRadar SIEM (Security Information and Event Management) which is monitored 24x7 by the IBM SOC. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to QRadar. IBM personnel managing Watson Cloud Platform Services QRadar are distinct from those having privileged access to the Watson Platform and this is enforced using the IBM IAM (Identity and Access Management) governance solution.
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	x			Security logs for all critical operations are collected and sent to IBM QRadar SIEM which is monitored 24x7 by the IBM SOC (Security Operations Center). Tampering of logging configuration and security logs are logged themselves and such logs are delivered to QRadar. IBM personnel managing IBM Watson services QRadar are distinct from those having privileged access to the Watson Platform and this is enforced using the IBM IAM governance solution.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			All access requires approval from both the employee manager and the system access owner. This provides the user with role-based access to the requested system. 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 (e.g., administrator level) to information security management systems?	x			All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
Identity & Access Management	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			Internal access to IBM Watson services are revoked on employee termination. Routine verification of access is also performed with user's management to ensure business purposes align with existing access.

User Access Policy		IAM-02.2	processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		x		Management of IBM ID's is an IBM retained responsibility. This internal process is automated and tested through our external audits repeatedly throughout the year. Client ID's are managed by client and are client responsibility.

			assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions				

			(e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements					
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	x			IBM Cloud management network traffic is processed using management control plane with strict access control. VPNs are utilized where needed to provide additional layer of security for sensitive networks within IBM.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			IBM Watson services leverage IBM IAM services to manage and maintain identity and access control.
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	x			IBM Watson services leverage IBM IAM services to manage and maintain identity and access control.

Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	x			IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. Secondary controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification. Access to systems that host the Watson as a Service offering is granted by management and is based on role requirements. Access is decided by using the principle of least privilege as a guide. Management ensures appropriate levels of segregation of duties when approving access.
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	x			IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. Secondary controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification. Access to systems that host the Watson as a Service offering is granted by management and is based on role requirements. Access is decided by using the principle of least privilege as a guide. Management ensures appropriate levels of segregation of duties when approving access.

		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	x			IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. Secondary controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification. Access to systems that host the Watson as a Service offering is granted by management and is based on role requirements. Access is decided by using the principle of least privilege as a guide. Management ensures appropriate levels of segregation of duties when approving access.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate	Do you provide multi-failure disaster recovery capability?		X		N/A. Customers desiring multi-failure disaster recovery should consider designs leveraging multiple regions across the IBM Global Cloud infrastructure.

		IAM-07.2	access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you monitor service continuity with upstream providers in the event of provider failure?	x			IBM Watson services availability is monitored and published using the IBM Cloud console. Upstream providers are monitored for service continuity and availability at the IBM Cloud IaaS layer.
		IAM-07.3		Do you have more than one provider for each service you depend on?	x			There are multiple ISP providers within the IBM Cloud datacenters which support IBM Watson services.
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	x			As published within the externally available audit reports.
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	x			This can be available in IBM Watson services dedicated deployment models. As documented within the solution design and contractual agreement.
		IAM-07.6		Do you provide a tenant-triggered failover option?	x			This can be available in IBM Watson services dedicated deployment models. As documented within the solution design and contractual agreement.
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	x			As published within the externally available audit reports and as required by contract.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	x			This is on a need-to-know basis only and is only ever leveraged in the need to support a client support request or requirement. IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow.
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	x			All customer data is rated as sensitive. Depending on IBM Watson services deployment model, tenant data is isolated based on solution design and contractual agreement.

Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	x			IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. Secondary controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification. Access to systems that host the Watson as a Service offering is granted by management and is based on role requirements. Tenants retain responsibility for their user's authorization and user access via IBM IAM services.

		IAM-09.2	appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?		x		IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. Secondary controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification. Access to systems that host the Watson as a Service offering is granted by management and is based on role requirements. Tenants retain responsibility for their user's authorization and user access via IBM IAM services. Backend system access is restricted to IBM employees with business need only.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	x			IBM user accounts are revalidated in accordance with IBM policy. Controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification.
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	x			IBM user accounts are revalidated in accordance with IBM policy. Controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification.

		IAM-10.3	function. For identified access violations, remediation must follow established user access policies and procedures.	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?		x		Revalidation reports are for IBM access & use only.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	x			IBM user accounts are revalidated, revoked, modified and/or updated in accordance with IBM policy. Controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	x			IBM user accounts are revalidated, revoked, modified and/or updated in accordance with IBM policy. Controls are used to enforce periodic revalidation of users that are based on continued business need and employment verification.
Identity & Access Management	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	x			Customer integration & federated access is managed and supported using the IBM Cloud IAM services control points. This integration with customer directory services allows for SSO (Single Sign On) capabilities.

User ID Credentials		IAM-12.2	restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you use open standards to delegate authentication capabilities to your tenants?	x			Customer integration & federated access is managed and supported using the IBM Cloud IAM services which leverages open standards to allow for delegation of authentication capabilities to IBM Watson services tenants.
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	x			Customer integration & SAML (Security Assertion Markup Language) federated access is managed and supported using the IBM Cloud IAM services.
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	x			Customer integration & federated access is managed and supported using the IBM Cloud IAM services control points.
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	x			Customer integration access is managed and supported using the IBM Cloud IAM services control points.
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	x			Customer integration & federated access is managed and supported using the IBM Cloud IAM services. This integration allows for clients to leverage existing MFA (Multifactor Authentication) options as established within their organization and directory services.
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	x			Customer integration & federated access is managed and supported using the IBM Cloud IAM services. This integration allows for clients to leverage third-party identity assurance services. Also, this is often accomplished using third-party certificate/key authorization services.
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	x			IBM Cloud IAM services supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Cloud customers may 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?	x			IBM Cloud IAM services supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Cloud customers may 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?	x			IBM Cloud IAM services supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Cloud customers may enforce any password policy they choose by using SAML federation.
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	x			IBM Cloud IAM services supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Cloud customers may enforce any password policy they choose by using SAML federation.

Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	x			IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow. This would include permissions and access to utilities that can manage virtualized partitions. Privileged access utilizing such utilities would be logged and sent in near real-time to IBM QRadar SIEM.
		IAM-13.2		Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	x			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 ISO audits.
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	x			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 ISO audits.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?		x		This is an ongoing project and compensating controls exist using advanced logging and SIEM monitoring.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	x			Audit logs are secured and encrypted using the QRadar tool. Access to these logs would follow the IBM Access control policies & procedures. IBM Watson services use a provisioning system with robust security attributes that is used to manage access for IBM administrators and to retain audit trails of access control workflow.
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	x			This is accomplished via IBM Compliance teams leveraging the IBM ISO27001 based ISMS (Information Security Management System) & also CSA (Cloud Service Alliance) Cloud Control Matrix. IBM Watson services are ISO27001/17/18 certified by external auditors with those certifications being available to customers. As part of ISO27001 audits and assessments, due diligence mapping to regulations and standards is reviewed.
		IVS-01.4		Are audit logs centrally stored and retained?	x			IBM Watson services security logs feed into a SELM (Security Event Log Monitor) service (IBM QRadar) and are monitored and managed via a SOC. Logs are retained a minimum of 90 days.
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	x			IBM Watson services security logs feed into a SELM service and monitored utilizing QRadar SIEM and managed via a SOC.
Infrastructure & Virtualization Security	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times.	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	x			All changes and privileged actions to VM (Virtual Machine) images are logged and sent to IBM QRadar SIEM for monitoring and alerting.

Change Detection		IVS-02.2	Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		x		IBM Cloud manages the backend IaaS supporting/providing all virtual infrastructure for the customer such that all changes to VMs are transparent to the IBM Watson services being provided.
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			IBM Cloud provides centralized, synchronized NTP (Network Time Protocol) services for IBM Watson services.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	x			For IBM Watson services this should be transparent to the end user. SLAs will be met as agreed to in the customer contract. Specific capacity requirements can be negotiated and documented in Dedicated service delivery models.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	x			This is provided by IBM Cloud IaaS.

		IVS-04.3	capacity requirements shall be made to mitigate the risk of system overload.	Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	x			IBM Cloud Platform services projects the anticipated capacity for the platform and ensures there is enough hardware, network, 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. This is also addressed when building out additional clients and services within IBM Watson services as needed.
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	x			IBM Cloud Platform services projects the anticipated capacity for the platform and ensures there is enough hardware, network, 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. This is also addressed when building out additional clients and services within IBM Watson services as needed.
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			The 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 include 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. Vulnerability tools, processes, & procedures are assessed & audited annually with internal and third-party auditors.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			x	IBM Watson services do not provide IaaS capabilities directly to clients. IBM Cloud manages the Infrastructure entirely for IBM Watson services customers.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	x			IBM Watson services architectures are reviewed as part of a threat modeling processes, procedures & exercise which are mandated prior to services going to general availability and then with major releases. These include documenting data flows and data maps.
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	x			IBM Watson services conduct reviews on all firewalls on an annual basis.
		IVS-06.4		Are all firewall access control lists documented with business justification?	x			All changes to IBM firewalls must follow the change management process which requires business justification and multiple levels of review and approval before deployment.

Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	x			All host machines in IBM Watson services are deployed as standard builds which remove unnecessary ports, protocols, and services. Authenticated scanning is performed on all machines to validate compliance with a set of hardening rules on a at least a monthly basis.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	x			Customers can choose to provision multiple instances of a service and implement access controls through IBM Cloud Platform that will support this process.
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			x	IBM Watson services are SaaS, IBM manages the architecture exclusively.
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	x			IBM Watson services have multiple non-production environments that support development and staging for both Public and Dedicated solutions. These environments are used to perform any testing pre-deployment prior to pushing to production environments. The non-production environments are logically segregated from production environments.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	x			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?	x			All systems and resources are protected by at least one firewall.

		IVS-09.3	configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	x			There are dedicated development, staging, and production cloud environments. Each environment contains at least one firewall to ensure isolation.
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	x			All systems and resources are protected by at least one firewall.
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	x			Per IBM policy data is encrypted in transit. IBM Watson services are built & deployed in virtualized environments.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	x			There are dedicated development, staging, and production cloud environments. Each environment contains at least one firewall to ensure isolation.

Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	x			IBM Watson services privileged users request access to IBM Cloud environments, including administrative tools, hypervisors and virtual machines, via an IBM 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 to prevent unauthorized access to data by IBM employees. 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 Cloud PaaS Platform data is encrypted in transit.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys,	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	IBM Watson services team 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 rogue devices are conducted routinely. These controls are accessed by an independent auditor as part of ISO27001 and SOC reviews 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)?			x	IBM IaaS does not permit the use of wireless networks and scans for and rogue devices are conducted routinely. These controls are accessed by an independent auditor as part of ISO27001 and SOC reviews and can be made available to customers upon request.
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			x	IBM IaaS does not permit the use of wireless networks and scans for and rogue devices are conducted routinely. These controls are accessed by an independent auditor as part of ISO27001 and SOC reviews and can be made available to customers upon request.

			passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network					
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	x			IBM Watson services network diagrams and threat models clearly document the boundaries of different environments and systems including the data flows across boundaries and data stores.
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	x			At the IaaS layer a clean pipe solution is implemented to ensure only appropriate traffic is passed through to the FWs which then passes the traffic back to an application proxy to authenticate the traffic before allowing it to reach any of the Watson services. IBM Watson services have implemented a DDoS (Distributed Denial of Service) solution to mitigate DDoS attacks.

Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			A list of all available APIs is published within each services description page. Additional details available here: https://www.ibm.com/watson/products-services/
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?			x	Customers may elect to provide additional training information to customize their Watson service. This data is typically provided by the customer and is their responsibility to manage. Some services, such as Watson Knowledge Studio, do allow customers to export the customized training models they have created.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	x			Policies and procedures are in place governing the use of APIs between IBM Watson services and third-party applications as part of the standard contract language.
		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?	x			IBM Watson services customers are responsible for the data including how and when that data is migrated. Please check the service descriptions for additional details.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	x			Per IBM policy data is encrypted in transit.

		IPY-04.2	export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	x			Tenants can receive this data upon request. Please check the service descriptions for additional details.
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	x			IBM Watson services use industry standard virtualization formats and technologies to help ensure interoperability, such as Kubernetes, Docker Containers, 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?			x	IBM Watson services IaaS does not have solution-specific virtualization hooks.
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	x			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	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	x			A list of approved application stores is available and has been communicated to users.

Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	x			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	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	x			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	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	x			IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	x			IBM Corporate security policy defines the pre-approved vendor(s) for cloud storage on mobile devices with regards to company business data.

			company business data.					
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	x			IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	x			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	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	x			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	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	x			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	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	x			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	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	x			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?	x			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	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	x			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?	x			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	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	x			Automatic lockouts are configured for BYOD and mobile devices.
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	x			IBM Corporate retains control of inventories, forced patching, etc., of mobile devices. Changes are implemented per policy and with mobile device change management processes.
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	x			All mobile devices and BYOD have required passwords.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	x			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?	x			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	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?		x		Data is stored on the cloud and enforced via a mobile device management solution where needed, 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?	x			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)?	x			Anti-malware is required on BYOD and enforced via management tools.

Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	x			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?	x			All mobile devices have remote wipe configured through the required mobile device management tools.
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	x			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?	x			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	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	x			The policy 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?	x			The policy 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	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			IBM Cybersecurity and IBM Legal maintain relationships with the proper local authorities.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	x			IBM Watson services have 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 IBM Watson or Customer system or data. https://www.ibm.com/security/secure-engineering/process.html 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?			x	The IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected a suspected security incident involving any IBM 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?	x			Refer to Security Incident Response and Support in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
		SEF-02.4		Have you tested your security incident response plans in the last year?	x			The Security incident response plan is reviewed and tested at least annually.
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	x			Security logs for all successful and failed login attempts and all critical operations in the IBM Watson services, including network devices and host machines, 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 SOC team on a 24x7 basis.

Incident Reporting			required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.					Refer to the IBM Security Intelligence 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?	x			For IBM Watson services dedicated environments, the potential incident activities are always attributed to a specific environment belonging to a customer. For Public, investigation of the incident may be required to determine which customer(s) was (were) impacted.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	x			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?	x			This is available where technologically possible when it has been deemed necessary to collect and manage evidence.
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	x			This is available in both Premium and Dedicated delivery models.
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			This is available in both Premium and Dedicated delivery models.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	x			Security logs for all successful and failed login attempts and all critical operations in the IBM Watson services stack including network devices, host machines, 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 Watson services Security incident response plan have a root cause analysis which record impact and trigger actions to mitigate in future.

Response Metrics		SEF-05.2	of information security incidents.	Will you share statistical information for security incident data with your tenants upon request?	x			Reports will be generated where technically possible upon request should a security incident occur.
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	x			IBM Watson services customers are ultimately responsible for the data integrity of their workload. IBM Watson services compliance certifications demonstrate the controls are in place to provide a secure platform including controls related to supply chain.
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	x			Access management processes are in place to ensure only users with a business need have access and that appropriate roles have been defined to ensure the principle of least privilege.
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	x			Customer will be notified via the IBM Cloud dash board if an issue has been identified that requires action on their part. Depending on the severity of the incident individual customers may be contacted directly. Customers may also subscribe to vulnerability notifications as described at https://www.ibm.com/security/secure-engineering/bulletins.html
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with	Do you collect capacity and use data for all relevant components of your cloud service offering?	x			IBM Cloud and the Watson services teams project 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?	x			Usage reports of the IBM Watson services are available on the IBM Cloud console.

			mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.					
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	x			IBM has a mature Internal Audit & assessment program which performs audits & assessments at least annually.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships,	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	x			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?	x			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?	x			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?	x			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?	x			IBM maintains all required sub-processing agreements and makes them available as required to clients upon request.

			physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up-					

			and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence					

Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	x			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 ISO27001.
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	x			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 ISO27001.
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	x			This is addressed via contract language maintained and managed by IBM Legal and Procurement for maintenance of supplier relationships.
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	x			This is addressed via contract language maintained and managed by IBM Legal and Procurement for maintenance of supplier relationships.
		STA-07.4		Do you review all agreements, policies, and processes at least annually?	x			IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all	Do you assure reasonable information security across your information supply chain by performing an annual review?	x			External audit assurance reports are reviewed for key suppliers on at least an annual basis.
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	x			External audit assurance reports are reviewed for key suppliers on at least an annual basis.

			partners/third party providers upon which their information supply chain depends on.					
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?	x			Penetration testing is allowed by IBM Watson services 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?	x			Penetration testing for IBM Watson services environments is performed on an annual basis using a 3rd party vendor.
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	x			Antivirus Antimalware protection is deployed on all Windows systems at the host level and logs are sent to IBM QRadar SIEM. Automated updates are in place for new malware or virus signatures.
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	x			Automated updates are in place for new malware or virus signatures.

Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant)	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	x			Network scanning is conducted at a minimum on a monthly basis. Findings are reported on and managed though normal operational vulnerability and risk management processes and procedures.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	x			The IBM Secure Engineering Standard mandates vulnerability assessment which requires automated code and application scanning at least on a monthly basis. Dynamic and static code scanning is performed using IBM Appscan on a monthly basis or whenever there is a major change.
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	x			OS scanning is conducted at minimum once a month. Findings are reported on and managed through normal operational processes.
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	x			Customers of IBM Watson dedicated services can request a Vulnerability assessment report for their environments.
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	x			IBM Watson services automating rapid patching across the environment. This provides full visibility on what is patched in addition to providing the automation to push out the patches to all machines across all Watson environments.
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?	x			Dedicated customers will be included in the change management process required to distribute patches within their environment.

			data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.					
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	x			IBM Watson services have a Change Control process to manage and track changes to any portion of the Watson infrastructure, regardless of its maturity level (Experimental, Beta or GA). The change control process requires multiple levels of review approval including component owners and management.
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	X			Within the IBM Watson services environment all mobile code in the form of scripts or executables must be tested and approved for deployment. End users and consumers of Watson APIs should provide for their own unauthorized mobile code prevention solution as that is not within scope for IBM Watson services on the IBM Cloud.

© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ Version 3.0.1" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 (2014). If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.