POV – Watson Privacy, Compliance, & Security

"Every organization that develops or uses AI, or hosts or processes data, must do so responsibly and transparently. Companies are being judged not just by how we use data, but by whether we are trusted stewards of other people's data. Society will decide which companies it trusts."
-Ginni Rometty, IBM Chairman, President, and CEO

Table of contents:

Scope

The scope of this document is the *IBM Watson services running on IBM Cloud*. The document does not address other IBM or client offerings with Watson in their names (e.g., Watson Health), or services that are not in the AI part of the IBM Cloud catalog. Nor does it address any third-party services showing up under AI in the IBM Catalog.

Introduction

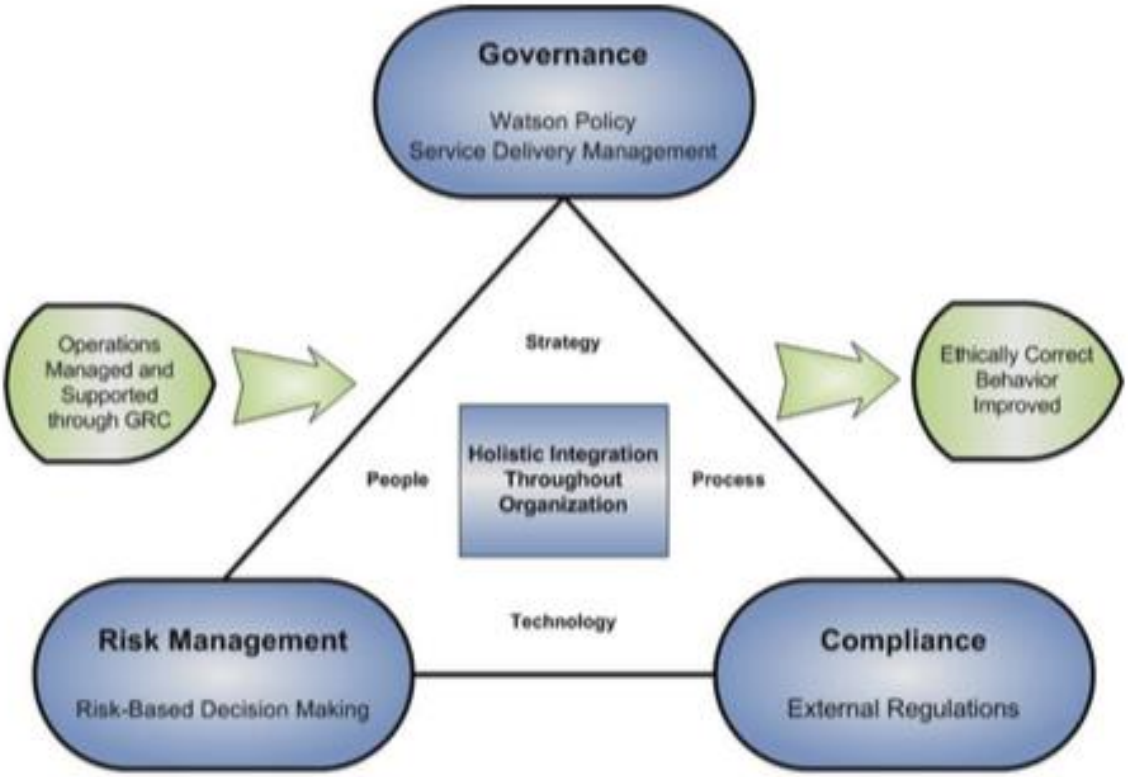
The ability of artificial intelligence (AI) to transform vast amounts of complex, ambiguous information into insights has the potential to reveal long-held secrets and solve some of the world's most enduring problems. It can help doctors treat disease, predict the weather, and manage the global economy. It is an undeniably powerful tool. And like all powerful tools, great care must be taken in its development and deployment.

To reap the societal benefits of artificial intelligence, we will first need to trust it. We have created a system of best practices that guide the management of Watson; a system that includes contracts and disclosures that help foster full transparency; a strategy that reflects our compliance efforts with existing legislation and policy; third-party certifications and security testing by third parties to validate the best practices; and a framework that provides for privacy and personal data protection.

IBM uses robust security and compliance processes that support successful execution of challenging workloads. The IBM Secure Engineering Framework reflects best practices from across the company and directs our development teams to give proper attention to security during the development lifecycle. These practices are intended to help enhance product security, protect IBM intellectual property, and support the terms of warranty of IBM products. Secure Engineering is an important element of the overall IBM security strategy. It is reflected in our internal initiative that addresses the dynamic nature of security in our development process. It is also reflected in our drive to meet the demand for high quality,

high assurance business solutions, services, and information technologies for our customers and our own operation.

The IBM Watson data privacy and security strategy is built upon industry Governance, Risk, and Compliance (GRC) principles as shown below, with ISO compliance certifications as a key part of IBM's ongoing commitment to providing a secure platform for business. This Watson on IBM Cloud security site provides further details regarding Watson security.



Data privacy

"Your data is yours, not mine to give away. If it's artificial intelligence, you own the insights, you own the algorithms."

Ginni Rometty, Chairman, President, and CEO, IBM
Dreamforce 2017, San Francisco, CA, November 8, 2017

What is data privacy on the Cloud?

POV – Watson Privacy, Compliance, & Security

Protect your insights – data is an organization's most valuable asset. It can yield unique competitive advantage coupled with the power of AI. But as data, and the models you build with it, become more and more valuable, you need to ensure you have control and choice over how it's used. When you train Watson with your data, you have the option to decide whether Watson should use your data and insights to train the Watson base models. But across the spectrum of data businesses generate, some models may gain more value if you decide to share with others whose innovations may accrue back to you.

At IBM we believe your data is yours – and yours alone. Therefore, it's essential to create a system of best practices that guide the safe management of data, including IBM Watson services on IBM Cloud and the data Watson is trained on. This includes contracts and disclosures that help foster full transparency; a strategy that reflects our compliance efforts with existing legislation and policy; and a framework that provides privacy and personal data protection.

Watson services for IBM Cloud will not share unique insights derived from your data unless you instruct us to use it. You are also not required to relinquish rights to your data in order to have the benefits of Watson services. Watson Standard clients may instruct IBM not to use their data to improve the service and base model. For Watson Premium clients, the default setting is to not use client data. When you use Watson services on the IBM Cloud, you will have the ability to combine your data sets with other IBM-owned, licensed, or permissioned public data sets to yield broader insights.

The Cloud Service Data Security and Privacy site has data sheets for each Watson service. The data sheets discuss the types of personal information used, processing activities, data protection, removal of the data at termination of the service or by request, data hosting locations, international data transfer, and more.

Watson services for IBM Cloud makes it clear when and for what purposes your data is being applied in the solutions we develop and deploy. This may include the major sources of data and expertise that inform the insights of the AI solutions we develop. Third-party or licensed data will be clearly identified.

Watson services for IBM Cloud agreements are transparent. We will not use your data unless you consent to such use, and then we will limit that use to the specific cases clearly described in the agreement. In addition, Watson services will not share unique insights derived from your data without your agreement. IBM will remove client content at the request of a client or at the end of the cloud service.

Personal data can be accepted by Watson services in the Standard, Premium, IBM Cloud Pak, or IBM Cloud Pak for Data deployment options, with the exception of regulated data types, which has separate certification recommendations.

POV – Watson Privacy, Compliance, & Security

The SLA for each IBM Watson service on IBM Cloud includes a link to a data sheet that gives details on how security and data privacy is provided for that service. The Cloud Services Data Security and Privacy site has the data sheet for each service.

Check out https://www.ibm.com/cloud/privacy for more details regarding IBM Cloud privacy policies and https://www.ibm.com/watson/data-privacy/ for the Watson privacy policies. You should also check out the resources in the Security section below.

Compliance & regulations

What is compliance & regulation in a cloud environment?

As a business, it is your responsibility to protect your customers' data. The cloud provider you choose must place a premium on security and transparency in how they will use the data you share. After all, if your customers' data is compromised, your company may be held accountable.

To choose a cloud provider that will help you meet your required compliance standards, you must understand the types of data you have. Different types of data have their own compliance standards. Compliance standards exist for many industries and may vary by country or region. Here are several examples:

- If you store health information for U.S. patients, U.S. Health Insurance Portability and Accountability Act (HIPAA) compliance is important.
- If your data pertains to European data subjects or your data is processed within the European Union, then General Data Protection Regulation (GDPR) compliance is critical.
- To ensure consistent standards for merchants, the Payment Card Industry Security Standards Council established Payment Card Industry (PCI) data security standards.

How to do it

ISO compliance certifications obtained by IBM Cloud are another confirmation of our strong commitment to protecting your data and your cloud.

Check out http://www.ibm.com/cloud/compliance for more details on IBM Cloud compliance. See the table below for details on Watson services.

POV – Watson Privacy, Compliance, & Security

Compliance Standard	Description	Watson Standard	Watson Premium
ISO27001	ISO 27001 is a widely adopted global security standard outlining the requirements for information-security management systems and provides a systematic approach to managing company and customer information based on periodic risk assessments. ISO 27001 certificate: https://ibm.biz/BdjWav Full list of IBM products covered under 27001: https://ibm.biz/BdjWab. Compliance for both IBM Cloud and Watson services.	Yes	Yes
ISO 27017	ISO 27017 gives guidelines for information-security controls applicable to the provisioning and use of cloud services, as well as implementation guidance for both cloud service providers and cloud service customers. ISO 27017 certificate: https://ibm.biz/BdjWam Compliance for both IBM Cloud and Watson services.	Yes	Yes
ISO 27018	ISO 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personal Data in accordance with the privacy principles in ISO 29100 for the public cloud computing environment.	Yes	Yes

	ISO 27018 certificate: https://ibm.biz/BdjWaK Compliance for both IBM Cloud and Watson services.		

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for European Union data subjects, wherever the data is processed. See this site documenting IBM's commitment to GDPR and IBM's Journey to GDPR Readiness eBook. The three Watson deployment models above are GDPR-ready.

The Cloud Security Alliance CSA is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing. One of the mechanisms the CSA uses in pursuit of its mission is the Security, Trust, and Assurance Registry (STAR) — a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings. For those looking for detailed answers to specific cloud security questions, the CSA assessment is an excellent source of answers. IBM Cloud's CSA STARS CAIQ assessment is here. Scroll down on that site and you will see the Watson self-assessment.

Security

What is Cloud security?

The growth of cloud and mobile computing and Internet of Things (IoT) technologies is accelerating the shift in IT services away from "on-premises" and towards cloud. Every member of your company, every device, and every piece of software is vulnerable to attacks, for which your leadership may be held accountable. Your data security and privacy considerations are only as strong as those of your cloud provider, so it is critical to choose a provider that is both secure and transparent with their security processes. The provider must be able to detect and react to threats, as well as proactively take actions to prevent them from occurring. Otherwise, your brand and corporate reputation may be at risk.

In spite of the risk, companies are moving more sensitive data to the cloud, including personal data (e.g., health and financial dara) and intellectual property (e.g., source code and product plans). A breach of this type of sensitive data could disrupt company operations, negatively affect market and customer perception, and lead to a loss in revenue and trust.

How to do it

POV – Watson Privacy, Compliance, & Security

In the era of ever-present attacks and breaches, IBM Cloud Security's scalable suite of technologies and solutions are made more robust and complete through pervasive encryption, AI with automation, and integration. When you partner with IBM, you gain access not only to a full stack of IBM Cloud security services, but also to an IBM security team supporting more than 12,000 customers in 133 countries.

No matter which IBM Cloud service you subscribe to, you can be confident your content is protected by IBM security. Every IBM Cloud service is designed, developed, and managed according to IBM's own strict security policies and implementation guidelines, and provided to you under the commitments of the IBM Data Security and Privacy Principles.

Watson services on the IBM Cloud can help 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 robust security and compliance processes that allow for execution of challenging workloads.

IBM employs robust security procedures to safeguard the data with which Watson interacts. This includes use of encryption and access control methodologies which allow us to code or move data to restrict access to authorized users and to de-identify and use data in accordance with applicable permissions.

The security policy for Watson services on IBM Cloud requires that all services include network and storage encryption, circuit and application level firewalls, security information and event management, intrusion detection, application source code scanning, third-party penetration testing, and regular vulnerability scanning.

Watson services are governed by the IBM Cloud Services data security and privacy principles. The technical and organizational measures apply to IBM Cloud, including any underlying applications, platforms, and infrastructure components operated and managed by IBM. See the Cloud Service Data Security and Privacy site for data sheets on the individual IBM Cloud services. The data sheet for each service discusses the types of personal information used, processing activities, data protection, removal of the data at termination of the service or by request, data hosting locations, international data transfer, and more.

IBM Watson has a policy of end-to-end encryption and employs the latest cryptographic technologies to protect client data. The IBM platform ensures:

- that end-to-end security for data in transit is implemented using TLS Version 1.2;
- an optional mutual authentication certificate and/or username and password for added measure via mutually authenticated SSL;
- and that data in transit and at rest is secured using AES 256-bit encryption

POV – Watson Privacy, Compliance, & Security

Check out https://www.ibm.com/cloud/security for more details on the IBM Cloud Security policies.

Additional security resources:

- IBM Watson on IBM Cloud Security overview - This site goes into detail on how IBM Watson provides security on the IBM Cloud. Encryption, network security, authentication, authorization, and more are topics covered.
- IBM Watson Data perspective - Provides the IBM Data Responsibility Perspective for Watson Data and AI.
- IBM Cloud Services data security and privacy principles - This site has documents related to data security & privacy for IBM Cloud Services offerings.
- Cloud Services data security and privacy - This site describes overarching policies and practices that are incorporated into each service description by reference.
- IBM Charter of Trust for Cybersecurity - This February 16, 2018 blog describes the Charter of Trust for a secure digital world. Launched at the Munich Security Conference, this Charter established 10 key cybersecurity principles that IBM, Siemens, Airbus, Allianz, Daimler, and others are adopting to strengthen trust in the security of the digital economy.
- IBM Principles for Trust & Transparency - Describes how Data Responsibility and Privacy is handled for AI.
- IBM Cloud security - This site is part of the DOCS associated with IBM Cloud. Note that this site also links to the IBM Cloud Security architecture.
- Resources on AI bias:
  - Think Policy Blog- Bias in AI: How we Build Fair AI Systems and Less-Biased Humans
  - White paper - Mitigating Bias in AI Models by Ruchir Puri
  - Think 2018 conference 5 in 5 presentation, Las Vegas - Unbiased AI, Francesca Ross

Frequently asked questions

Data privacy

1. How does Watson services on IBM Cloud handle personal data, including regulated personal data like health and credit card information?
   - IBM Cloud handles non-regulated personal data, or sensitive personal data, in accordance with the ISO 27107 and 27108 standards.

2. Is Watson learning from my data? Does Watson train other client's models with my data?
   - The default for Watson Standard is that client training data is used for continued development of the general models, where there is a direct benefit to the client.

- A Watson Standard client can instruct IBM not to use the client data to improve the model on the transaction, service, or account level.
- The default for Watson Premium is that no client training data is used for the development or enhancement of the general models or other clients' models.

3. We hear the "your data is your data" message from many cloud providers. Why is IBM different?
    - A client can direct Watson not to use their client training data to update the Watson base models. In that case, their data will not be used for the development or enhancement of the general models, or other to help build clients' models. The best way to determine how other cloud providers handle your data is to check their terms & conditions. See the IBM Principles for Trust & Transparency.

4. Which Watson services are stateful, rather than stateless?
    - A **stateless** service treats each request as an independent transaction that is unrelated to any previous request. A **stateful** service may store data to correlate a prior request with the request it is currently processing. The following Watson services are stateful:
        - Watson Assistant
        - Watson Discovery
        - Watson Knowledge Studio
        - Watson Language Translator
        - Watson Machine Learning
        - Watson Speech-to-Text for custom models; otherwise stateless
        - Watson Text-to-Speech for custom models; otherwise stateless

Compliance & Regulations

1. Which regulations do IBM Cloud & Watson services support? For example: PCI (credit cards), HIPAA (U.S. healthcare), FFIEC and FISC (financial), FISMA and FedRAMP (U.S. Federal). Country-specific directives like the NIS Directive, and GDPR (European Union)?
    - As of May 25, 2018, both Watson and IBM Cloud were GDPR-ready.

2. As a client, can I request your SOC 2 / SOC 3 reports, and CAIQ assessment?
    - A SOC 1 report focuses on controls at the service organization that would be useful to user entities and their auditors for planning a financial statement audit of the user entity and evaluating internal control over financial reporting at the user entity.

    - Request the SOC 1 and SOC 2 certificates through our customer portal (link resides outside ibm.com) or contact your IBM representative.
- SOC 2 and SOC 3 reports focus on the service organization's system description and controls in accordance with specific criteria related to availability, security and confidentiality. SOC 2 includes auditor testing and results, while SOC 3 is a summary of the SOC 2 report that is available for public use.
    - The SOC 3 report is on the IBM Cloud Compliance site.
- The Cloud Security Alliance CSA (link resides outside ibm.com) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing. One of the mechanisms the CSA uses in pursuit of its mission is the Security, Trust and Assurance Registry (STAR) — a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.
    - IBM Cloud's CSA STARS CAIQ assessment is here. Scroll down on the IBM Cloud Compliance site to see the Watson self-assessment.

3. How does Watson use Privacy Shield or the EU model Clauses, or Safe Harbor?
    - Watson and IBM Cloud are Privacy Shield certified.
    - IBM uses EU Model Clauses in contracts.
    - Safe Harbor was used to govern the transfer of data between the EU and the United States. Safe Harbor was replaced with a choice of either Privacy Shield or EU Model Clauses.

4. How do Watson services on IBM Cloud handle "right to erasure" in GDPR?
    - Clients that require this control for Watson services for IBM Cloud must label their data, and then use a web site to indicate that their labelled data should be deleted everywhere.

- Is IBM Cloud certified for the following?
    - ISO 20000-1 – Yes, demonstrated with an ISO 27001 Certification.
    - SSAE 16 – Yes, demonstrated with a SOC1 Type 1 or Type 2 report.
    - ISAE 3402 – Our auditors include this attestation as part of the SOC1 report.
    - EU Directive 95/46/EC – Superseded by GDPR. IBM Cloud & Watson are GDPR-ready.
    - German Bundesdatenschutzgesetz (BDSG) – IBM Cloud IaaS is certified for the BSI C5 standard to meet the requirements. See https://www.trusted-cloud.de/en/standards.

Security

Securing my data

POV – Watson Privacy, Compliance, & Security

1. How is access management handled?
   - See the Authentication & Authorization and Identity & Access Management sections in the IBM Watson on IBM Cloud Security Overview for details.

2. Do you provide fine-grained access management (e.g., edit rights to some, read rights to others)?
   - Users of a Watson service get an access key, but no tiered levels of access are currently provided.

3. What do you offer a client that wants data isolation (e.g., for PHI)?
   - There are multiple deployment models: IBM Watson public cloud (Watson Standard), Premium plans that provide additional data isolation within the public cloud, IBM Cloud Pak for Data cloud environment if you need an infrastructure that runs within your environment. Each environment offers the same service functionality and the security architecture remains consistent. All IBM deployments reside within hardened enterprise-class IBM Cloud data centers that are ISO27001 and SOC2 certified. See Securing Cognitive Apps in Watson on IBM Cloud Security for details behind the three Watson deployment models.

4. What are the different levels of isolation that I can get around storage and data?
   - There are several deployment models: IBM Watson public cloud (Watson Standard), Premium plans that provide additional data isolation within the public cloud, and IBM Cloud Private or IBM Cloud Pak for Data. Watson Standard is multi-tenant. Watson Premium provides Data isolation, while IBM Cloud Private and IBM Cloud Private for Data provide complete isolation since they are running in the client's environment. Each deployment model provides isolation. See Securing Cognitive Apps in Watson on IBM Cloud Security for details behind the Watson deployment models.

5. If Watson transfers my data to process it, how does Watson ensure it gets deleted (the verification processes)? Is this process auditable so I can know my data has been deleted?
   - Most of the Watson services are stateless, which means that Watson does not store client data if a client instructs IBM not to use client data to train the base model. Audits are performed internally, but to protect the security and privacy of our clients, we don't share the processes.

6. How is data erasure handled when the client terminates their contract - either at the end of the contract or at any point before? How soon after the contract ends is the data erased?

- IBM will remove client content 1) at request of the client within 30 days, or 2) at the end of the cloud service within 90 days after termination of the service.

7. Can I keep my data local (on-premises) and yet still process it through the Watson services? In other words, connect to my data from the cloud, but not transfer the data?
   - Your data needs to be transferred to the cloud to be processed by the Watson services. For stateless services, the data is only on the platform transitorily. For stateful services like Watson Assistant and Watson Discovery, data a client sends to the service is sent by the client, used to train a model, and then deleted.
   - When your business is using an IBM Cloud Private or IBM Cloud Pak for Data environment, your data remains within your private cloud.

8. What is your management system around data isolation that would lead to data privacy?
   - Watson services have four levels of data isolation: Standard, Premium, IBM Cloud Private, and IBM Cloud Private for Data. See earlier descriptions of the four deployment models in earlier FAQs. In addition, the EU Cloud provision stops data from leaving the European Union, without it being transparent to the client.

9. Does IBM allow a private, secure connection from the customer's data center to an IBM Cloud data center?
   - To get to a Watson service, a client would need an IBM Cloud Infrastructure (SoftLayer) account and use that network to establish a TLS encrypted connection.

10. How do the Watson services handle backup and recovery of my data?
    - See the data sheets associated with each Watson service as well as the associated Service Descriptions which address backup and storage [Retention and Destruction] policies. As an example, here are links to the IBM Watson Discovery data sheet and IBM Watson Discovery Service Description.

11. What insight do I have to your logs and processes? Can I get a log feed?
    - For the security and privacy of the IBM Cloud users, we don't share our logs with partners or clients. If information were required from the logs for a legitimate reason (such as an investigation), then IBM would work in a secure way with the client to ensure that we shared the relevant information.

Encryption

1. Do you provide encryption-at-rest and encryption-in-motion?

- Yes. See the Encryption & Data Privacy section in the IBM Watson on IBM Cloud Security Overview for details.

2. What kinds of encryption does Watson handle, and when?
   - IBM Security Policy requires that all services include network and storage encryption. IBM employs the latest technically feasible cryptography technologies to protect customer data at rest and in motion. See the IBM Watson on IBM Cloud Security Overview for details.

3. How can I build a secure Watson application?
   - See How to secure your applications when using Watson services and Improve the effectiveness of your application security.

4. What is the management process around encryption keys: Access, alerts, audits, management?
   - See the Encryption & Data Protection, and Authentication & Authorization sections in the IBM Watson on IBM Cloud Security Overview for details. The is also information on vulnerability management.

5. Does IBM Cloud support Bring Your Own Key (BYOK) so I can supply the key for encryption-at-rest and encryption-in-motion?
   - IBM Cloud supports encryption-at-rest and encryption-in-motion. Currently, everything is encrypted using IBM managed keys. BYOK means customers can bring and manage their own encryption keys; this is currently targeted for later in 2018.

Vulnerability management

1. What is your vulnerability management process?
   - The IBM Product Security Incident Response Team (PSIRT) manages the security vulnerability management process, providing identification and remediation of security vulnerabilities. All IBM Watson services participate in this system. See the IBM Secure Engineering and Product Vulnerability Management site for details.

2. What is the procedure in case of a data breach? How is the client notified and how soon after the breach? Where does IBM document the details of the breach? Can I get a Root Cause Analysis Report?
   - See the IBM Secure Engineering and Product Vulnerability Management site for process details regarding data breaches.

Security management

POV – Watson Privacy, Compliance, & Security

1. What is your health check posture for scanning devices and code for vulnerabilities? How often do you run the scan and how is remediation handled?
   - See the Application Security sections in the IBM Watson on IBM Cloud Security Overview for details.
   - See Securing Cognitive Apps in Watson on IBM Cloud Security for details on the three Watson deployment models.

2. When was your last penetration test? How often do you run the test? What are the results of the last test, as well as your remediation plan for any identified gaps?
   - Penetration testing involves skilled practitioners using a wide array of automated tools and manual methods in an attempt to compromise a system. All services regularly undergo penetration testing, using both IBM teams and external vendors. Each service is tested at least annually by a certified external vendor. Different services are tested each quarter, as opposed to all IBM Cloud services being tested at once.
   - Any critical or high priority issues are addressed immediately. IBM does not share the results of the penetration test with clients because making gaps public could expose the security and privacy of our clients. IBM will share an executive summary from the third-party report with clients or partners upon request.

3. Am I allowed to conduct a walk-through at one of your data centers to see how you handle physical security, badging, logs, etc.?
   - Clients and partners are not permitted to conduct a walk-through of an IBM Cloud data center. This is to protect the security and privacy of other clients using the IBM Cloud.

4. Can I see your ITS policy document? How did Watson and IBM Cloud do on the last audits?
   - Here are the Data Security and Privacy Principles for the IBM Cloud: https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp. This document is effectively IBM's ITS policy document for IBM Cloud. IBM does not share the results of tests and audits with clients because making gaps public could expose the security and privacy of our clients.

5. What is your end-of-life policy for hardware in your cloud data centers (e.g., router no longer supported by vendor, so no patches available) as well as for software?
   - Here is the end-of-life management procedure for the IBM Cloud data centers:
     - Networking manages system's life cycles proactively with device manufacturers and/or vendors to remain compliant with FFIEC

guidelines. The scope of our efforts is for device installation and maintenance only. While Networking does make decisions on which make and model to replace EOL devices, they must align with current architecture standards. Our procedures include:

- Maintaining an inventory of device model, manufacturer, and firmware version in IMS Tracking changes to the inventory of devices in IMS.
- Proactively monitor manufacturer end-of-life product pages at a minimum of once per quarter.
- Discussing aging devices regularly as part of business reviews with our vendors monthly.
- Planning for the replacement of devices through our maintenance team.
- Secure disposal of assets.

6. I'm a partner and I sell my application to 100 clients. I could have 100 instances on IBM Cloud Premium.
   - How can I get usage information for an individual client instance?
     - You can see an individual offering's usage by going to: Manage -> Billing and Usage -> Usage. This will bring users to a dashboard for all of the instances of the offerings they've purchased, and the aggregated usage associated with them. By clicking 'View Instances,' users should be able to see granular details for the particular instances they are interested in.
   - Are there capabilities to provide fine-grained security and authorization for a single instance?
     - The client's admin sets up instances, orgs, and spaces in IBM Cloud. They control the access for individual instances. Currently there is no vehicle to provide fine-grained security and authorization within a single instance.
   - How would a client know if a disgruntled employee deleted a production instance?
     - The information is logged, but the client has to call IBM Support to find the disgruntled employee's name.
     - If a disgruntled employee takes malicious actions, the client could rotate or change the employee keys and then the disgruntled employee can do nothing further.
   - If an instance goes down, how would the client know?
     - Either IBM Cloud will communicate that the service instance is down, or the client will have to check the status page described earlier in this response.