CenturyLink® Business

RESOURCE GUIDE

CenturyLink Compliance

RESOURCE GUIDE

Enabling Compliance Requirements

Summary

CenturyLink’s Compliance Management and Industrial Security teams are dedicated to obtaining, continually improving, and maintaining critical compliance certifications for CenturyLink infrastructure and services. Through disciplined assessment and audit processes, CenturyLink has implemented comprehensive practices for Statement on Standards for Attestation Engagements #16 (SSAE 16) SOC 1, SOC 2, Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization (ISO 27001), Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and EU Data Protection. CenturyLink also observes regulatory controlled frameworks such as Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA) and North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP) providing custom security and compliance enabling solutions to facilitate customization to meet any organization’s compliance requirements.

CenturyLink’s IT, Cloud, and Hybrid IT solutions provide a broad array of infrastructure spanning — network, colocation, managed services, and cloud offerings — beyond on-premise data center deployments. CenturyLink’s Hybrid IT service enables companies to aggregate, unify, and scale services and their functionality, creating powerful and highly-responsive infrastructure capabilities. A growing and often key differentiator is compliance. In today’s rapidly changing IT landscape, solutions often need several compliant certifications to meet international, governmental, and industry standards. CenturyLink brings together the right people, technology, and industry best practices to create comprehensive network and Hybrid IT solutions that accelerate performance everywhere our customers do business.

United Responsibility for Compliance

Traditional IaaS Approach

The widely-used **“Shared Responsibility”** model is the baseline most Cloud and IT service providers make available to customers. Designating security as everyone's responsibility ensures that the infrastructure and everything connected to it is safe. CenturyLink is responsible for the security of everything in our infrastructure; our customers are responsible for anything built on top of, or connected to that infrastructure.

Shared Responsibility Model for Compliance

Client Responsibilities	CenturyLink Responsibilities
Software Platform	Encryption
Application Authentication / Authorization / Identity Management	Storage Hardware / SAN
	Core Network Security
Network and Firewall Configuration	Compute
	Network & Data Centers
	Physical Security & Personnel

Hybrid IT Approach

CenturyLink works with its customers to address their specific compliance needs by leveraging a “**United Responsibility**” security model depending on which services the client requires CenturyLink to manage. As a recognized leader in Hybrid IT environments, CenturyLink provides real-world experience to determine the right mix of technology and solutions based on the specific business demands, workloads, and end-user expectations — all with the built-in compliance requirements to meet most universally accepted security frameworks and standards.

United Responsibility Model for Compliance

Client Responsibilities	Optional Services	CenturyLink Responsibilities
Software Platform	Operating System	Storage Hardware / SAN
Application Authentication / Authorization / Identity Management	Network and Firewall Configuration	Core Network Security
	Encryption	Compute
		Network & Data Centers
		Physical Security & Personnel

CenturyLink works with the customer to identify and deliver the right blend of IT services — all from a single, capable, and reliable provider.

- Integrated and optimized solutions from multiple IT infrastructure models aligning technology capabilities with business needs.
- Combining the best of traditional IT with additional capabilities that internal IT teams may not be able to deliver on thier own.
- Choose from individual offerings, co-managed, or fully-managed solutions based on business priorities.
- Designed to enable customers to meet regulatory requirements from FISMA to HIPAA to PCI.

Compliance and security are top-level considerations when planning a move to a Hybrid IT model. Security concerns have long been a factor preventing companies from either experimenting with or fully embracing a cloud environment. Organizations are rapidly assessing the gaps in their current security policies against the requirements necessary to align with compliant standards. CenturyLink possesses the necessary third-party generated certifications required for its customers to become or remain aligned with relevant compliant certifications and security frameworks.

CenturyLink Reports, Certifications, Regulations, and Frameworks

The CenturyLink Compliance team is dedicated to continually improving and maintaining compliance standards and certifications that are critical to our customers. Through a disciplined assessment and audit process, CenturyLink performs annual assessments for SSAE16 SOC1,SOC2, PCI/DSS, ISO 27001, Global Risk Management, and HIPAA.

ISO 27001 and SOC Reporting

ISO 27001 Certification

ISO 27001 CERTIFIED by schellman

CenturyLink has received certification of the ISO/IEC 27001:2013 Information Security Management System (ISMS) standard for data centers located in United States, Singapore, United Kingdom, Germany, and Japan. The certificate addresses global network services and managed hosting services in Asia and EMEA, as well as colocation services (including physical security and facilities management) for data centers in Asia, EMEA, and North America. ISO 27001 is an International Standard providing a model for establishing, operating, monitoring, and improving ISMS.

The ISO 27001 certification allows CenturyLink to demonstrate effective information security processes are defined and implemented. ISO 27001 conducts interim audits annually to support a three-year renewal cycle. The most recent renewal certification audit was completed in 2013.

ISO 27001 key benefits:

- Includes security as part of the current quality system.
- Provides an opportunity to identify and manage risks to key information and systems assets.
- Provides confidence and assurance to both partners and clients.
- Allows for an independent review and assurance of information security practices to customers.

CenturyLink adopted ISO 27001 for a variety of reasons including:

- Protecting critical and sensitive information.
- Providing a holistic approach to secure information and compliance.
- Credibility, trust, satisfaction, and confidence with stakeholders, partners, citizens, and customers.
- Security status according to internationally accepted criteria.
- Market differentiation due to prestige, image, and external goodwill.
- Globally accepted certification.

SOC Reports (CenturyLink and CenturyLink Cloud)

CenturyLink provides an annual combined examination of Statement on Standards for Attestation Engagements (SSAE) No. 16 and International Standard on Assurance Engagements (ISAE) 3402. The certification validates CenturyLink's commitment to operational excellence and customer satisfaction. The SSAE 16 (SOC1) Type II report covers October 1 to September 30 annually. A Type II examination means that an independent service auditor formally evaluated and issued an opinion on the description of selected CenturyLink systems along with the suitability of the design and operating effectiveness of the applicable controls. This audit report includes controls related to managed security services, change management, service delivery, support services, environmental services, physical security, facilities management, managed hosting services, managed storage, and backup services in CenturyLink's data centers in Asia, EMEA, and North America.

The SOC 2 report meets the requirements of a broad range of users that must understand internal controls at a service organization as it relates to the Trust Service Principles framework. The SOC 2 Type II reports covers October 1 to September 30. The report is relevant to the non-financial reporting controls related to the security and availability principles modeled around four broad areas: Policies, Communications, Procedures, and Monitoring.

This audit report includes: managed security services, change management, service delivery, support services, environmental services, logical and physical security, managed hosting services, managed storage and backup services controls in data centers in Asia, EMEA, and North America. CenturyLink will provide report copies upon request, subject to CenturyLink's non-disclosure agreements in place.

Products and Services Included in ISO 27001 and SOC Reports

A variety of products and services are included in ISO 27001 and SOC reports including:

Cloud Services
Hybrid-ready public cloud provides the agility, scalability, and security expected from an enterprise-class cloud backed by an industry leading global network.

Managed Services
Managed Services secure and optimize your network, applications, and infrastructure so you can compete at the speed of business.

Managed Security
CenturyLink Managed Security Services provide a full complement of threat prevention, threat management, incident response and analysis services to support our hosted or on-premise enterprise security environments.

Managed Hosting
Maintain complex IT infrastructure and applications with CenturyLink's comprehensive portfolio of Managed Hosting services including fully managed networks, servers, storage, operating systems, and security.

Managed Storage and Backups
Gives a range of storage options including data replication and backup/archiving. CenturyLink solutions are secure, affordable and can provide data resilience up to five nines.

PCI-DSS Certification

The Payment Card Industry Data Security Standard (PCI-DSS) Version 3.1 is the security certification that applies to organizations and merchants that accept, transmit, or store any credit card-holder data. If any customer of an organization directly pays the merchant using a credit or debit card, the PCI DSS applies.

CenturyLink is currently listed on the VISA list of PCI compliance service providers. CenturyLink obtained the following passing Report On Compliance (ROC):

- Managed Firewalls and NIDS Services (not location specific) Cisco ASA and Check Point firewalls, and Network Intrusion Detection Systems (NIDS).
- iO Private Port (not location specific): MPLS based on WAN platform for customer provisioning and management on the network.
- Network Integrated Cloud Contact Center Solutions: Hosted Interactive Voice Response and Network Common Areas contact center solutions.
- Data Center Services with physical and administrative security controls in the majority of CenturyLink branded data centers.

CenturyLink's auditors provide a "ROC Letter" that confirms CenturyLink's compliance with specific PCI controls and the applicable locations and services. This ROC Letter is available upon request, subject to CenturyLink's non-disclosure agreement. In addition to having PCI-compliant solutions, CenturyLink has developed a detailed matrix of PCI controls for organizations that have broader requirements. The matrix specifies the responsible party for each PCI control and is customized for the solution sold to the customer. Additionally, it is appended to a PCI Addendum, which defines CenturyLink's commitment to the PCI controls.

Products and Services Related to PCI-DSS Compliance

A variety of services may be deployed to build-out a comprehensive PCI-DSS compliant solution including:

Colocation
Recognized as a trusted colocation provider by many of the world's largest companies, our global footprint includes over 70 data centers built to Tier III, Concurrent Maintainable specifications.

Data Centers
The freedom to choose the best location to comply with business, regulatory, or data sovereignty considerations.

FISMA – The Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) is a comprehensive framework for securing the federal government's information technology (IT). FISMA provides a set of specific guidelines for federal agencies on how to plan for, budget, implement, and maintain secure systems.

Each federal agency must develop, document, and implement a program to provide security for the data and IT systems that support its operations and assets — including both its own systems as well as those belonging to other agencies, contractors, and others supporting its mission to achieve FISMA compliance. The agency must:

- Plan for security.
- Ensure that appropriate officials are assigned security responsibility.
- Periodically review IT security controls.
- Authorize system processing prior to operations and periodically, thereafter.

Not only do all federal agencies receive an annual "grade" for their FISMA compliance programs, but these grades are also made public. A high grade on the FISMA report card indicates that the agency's systems are secure; its data is locked down, and provides a public verification of that fact.

In today's environment, security and risk management have become critical to the over all security of our nation. The CenturyLink Government team has been — and will continue to be — an industry leader in working with our federal government agencies and departments to meet this national priority. We have implemented a hierarchy of controls and management tools in the areas of personnel, systems and facility security, each of which are governed by a comprehensive set of security policies, standards, and guidelines.

CenturyLink's extensive experience has shown that, in light of today's ever-changing climate of threats and vulnerabilities, a sound security position is best maintained by adopting a holistic view of risk management. This enterprise-wide approach to risk management, and more specifically, security practices, calls for:

- Centralized authority and policymaking
- Clear lines of communication
- Well-defined expectations
- Close collaboration among all parties

The Collaboration Model

CenturyLink’s collaboration model, which provides the backbone for rapid identification of new threats and vulnerabilities, creates an action-oriented platform for reducing risks and managing security events. As the cyber threat for federal customers has grown, so has the need for demonstrated security practices to comply with obligations such as FISMA.

To meet these demands, CenturyLink has evolved our security- and technology-related functions to ensure close organizational alignment and collaboration with more traditional industrial security programs.

FedRAMP – The Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

This approach uses a “do once, use many times” framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cyber security and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

Goals

- Accelerate the adoption of secure cloud solutions through the reuse of assessments and authorizations.
- Increase confidence in security of cloud solutions to achieve consistent security authorizations using a baseline set of agreed upon standards to be used for cloud product approval in or outside of FedRAMP.
- Ensure consistent application of existing security practice and increase confidence in security assessments.
- Increase automation and near real-time data for continuous monitoring.

Benefits

- Increase reuse of existing security assessments across agencies.
- Save significant cost, time, and resources – “do once, use many times”.
- Improve real-time security visibility.
- Provide a uniform approach to risk-based management.
- Enhance transparency between government and Cloud Service Providers (CSPs).

CenturyLink Government Cloud

CenturyLink Government Cloud is an enterprise-class FedRAMP compliant service deployed in conjunction with VMware's industry recognized vCloud Government Community platform, based on vSphere. This allows customers to stretch their data center to the cloud (often referred to as a "Hybrid Cloud") using familiar tools and processes. A common vSphere foundation makes cloud adoption simpler and less risky.

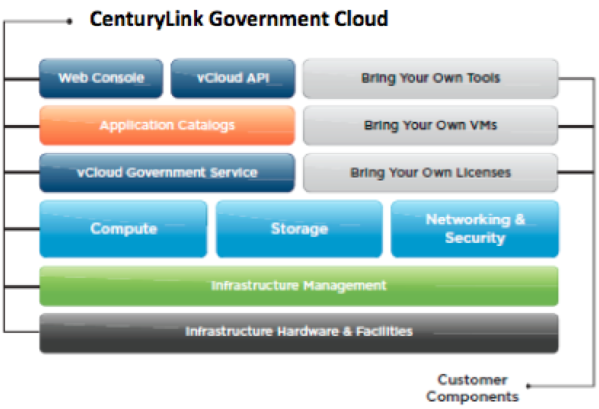
CenturyLink brings together the best of public, private, and hybrid cloud offerings — enabling agencies to seamlessly migrate and extend their data center workloads to the cloud while complying with federal security standards. By supplying cloud, colocation, and managed hosting services over its carrier-class network, CenturyLink provides government agencies with more than just security standards; it allows the agencies to take advantage of benefits of having existing people, process, tools, and automation in place. This combination also enables government organizations to focus on their mission rather than taking time and resources that may result from the need to re-architect legacy infrastructure.

Dedicated Cloud

Dedicated Cloud is a physically isolated, single tenant compute offering delivering increased performance. CenturyLink's Dedicated Cloud service combines a private cloud platform with best of breed technology implementations. This powerful combination equips businesses with the tools to rapidly build, control, and customize IT environments. CenturyLink Dedicated Cloud eliminates the capital burden of investing in expensive physical server deployments that often go underutilised. Every component of CenturyLink Dedicated Cloud supports the demands placed on IT infrastructure without the burden of long-term contracts or the lead time of traditional deployments. With Dedicated Cloud, clients are able to deploy compute resources quickly and easily when needed, and turn them off when no longer required. CenturyLink Dedicated Cloud offers enterprises a way to reshape their environments to meet the needs of hybrid IT without sacrificing security and performance. Clients utilising a dedicated VMware® vCenter server are able to seamlessly replicate workload from on-premise VMware clouds to a Dedicated Cloud Compute infrastructure, and manage failover automation using VMware vCenter™ Site Recovery Manager™. VMware vRealize Operations can be utilised with CenturyLink Dedicated Cloud providing capacity management and workload analysis tool with a vast variety of reports and dashboards.

Virtual Private Cloud

Virtual Private Cloud is a flexible multi-tenant service where compute, networking, and storage are logically isolated providing the necessary reliability to execute business-critical missions. CenturyLink provides the infrastructure—including space and power, compute resources, storage resources, virtualization operating system, networking resources—and use of the Control portal and API for provisioning and management.



Whether clients are looking to offload a few virtual machines, create new applications, or migrate legacy workloads, CenturyLink Cloud's infrastructure and management tools offer a more enterprise-ready path to the cloud.

CenturyLink also supports a portfolio of managed services available on-demand, with hourly billing.

FISMA vs. FedRAMP

The FISMA Framework

FISMA uses multiple documents and standards as part of the information security program, but most specifically Federal Information Processing Standards (FIPS) 199, FIPS 200, and NIST Special Publication 800-53 Rev. 4 as the primary security controls. Federal agencies, departments, and their contractors are required to implement this framework.

- **FIPS 199** - Organizations must first determine the security category of their information and information systems, which includes a Low, Moderate, or High impact ranking. Security categories are based on the potential impact of an event that creates a threat or vulnerability to information and information systems.
- **FIPS 200** - Represents the minimum-security controls requirements for information and information systems. Organizations are required to cover 17 security-related areas for information and information systems. All minimum-security controls must be implemented unless legitimately exempt.
- **NIST SP 800-53 Rev. 4** - Represents the tailored set of baseline security controls for information systems and organizations. Baseline controls are chosen from the FIPS 199 and FIPS 200, and the goal of SP 800-53 is to provide a comprehensive overview.

**FISMA requires that all federal departments and agencies report annually on their information security status*.

FedRAMP Framework

FedRAMP was created to build a cohesive risk management program that could be used throughout the entire federal government. For starters, it entails a four-step process for authorizing an organization to host a cloud environment. These initial steps include Initiating, Assessing, Authorizing, and Leveraging.

- **Initiating** - Agencies or cloud service providers (CSPs) are the initiators for the FedRAMP program by pursuing a security authorization. The FedRAMP requirements are based on NIST SP 800-53 controls (the same applies to FISMA).
- **Assessing** - Based on the NIST SP 800-53, CSPs must hire a third-party assessment organization (3PAO) to perform an independent assessment.
- **Authorizing** - Upon completion, the security assessment package will then be forwarded to the FedRAMP Joint Authorization Board (JAB) for review.
- **Leveraging** - The CSP will then continue to work with the executive departments and agencies for the Authority to Operate (ATO) permissions.

FISMA and FedRAMP Difference

Both FISMA and FedRAMP use the same NIST Baseline Controls, but are different because:

- FISMA is required for all federal agencies, departments, and their contractors regardless if they are a cloud service provider or not. FedRAMP is required for all agencies or cloud service providers that currently use, host, or want to host federal information in a cloud environment.
- It's important to remember that FedRAMP does not deploy any new controls; it adds additional controls from the NIST Baseline Controls, which are built from the NIST SP 800-53 Rev 4. In fact, the number of controls for a FedRAMP assessment will contain more than a FISMA assessment. The goal of the NIST SP 800-53 Rev. 3 was to address controls and improvements for the attributes of a cloud environment.

Assessments for FISMA and FedRAMP

The difference between a FISMA and FedRAMP assessment is that a FISMA assessments can be performed by any third-party that conducts security assessments. However, a 3PAO must be used for FedRAMP assessments. An initial list of FedRAMP accredited 3PAOs was announced in May 2012. The FedRAMP JAB continues to add accredited 3PAOs to the accreditation list on a rolling basis when 3PAOs successfully meet the requirements.

This list can be referenced on the GSA FedRAMP site at: https://www.fedramp.gov/marketplace/accredited-3paos/

There are three controls levels for FedRAMP assessments:

- For LOW impact levels, the current FISMA Baseline Controls are set at 124. For FedRAMP, there will be just one additional control to the assessment.
- For MODERATE impact levels, the current FISMA Baseline Controls are set at 261. For FedRAMP, there will an additional 65 controls.
- For HIGH impact levels, the current FISMA Baseline Controls are set at 343. For FedRAMP, there will an additional 78 controls.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), sets the standard for protecting sensitive patient data. Any company that deals with Protected Health Information (PHI) must ensure that all the required physical, network, and process security measures are in place and maintained.

This includes Covered Entities (CE), and anyone who provides treatment, payment and operations in healthcare and Business Associates (BA), anyone with access to patient information and provides support in treatment, payment or operations. Subcontractors or business associates of business associates must also be in compliance.

The HIPAA Privacy Rule addresses the saving, accessing and sharing of medical and personal information of any individual, while the HIPAA Security Rule more specifically outlines national security standards to protect heath data created, received, maintained or transmitted electronically, also known as Electronic Protected Health Information (ePHI).

CEs and their BAs can leverage CenturyLink to process, maintain, and store ePHI. With the required controls in place in the customer's environment (data encryption, access restrictions, etc.), CenturyLink will sign a Business Associate Agreement (BAA) that can be leveraged as part of a customer's overall compliance program. Additionally, CenturyLink can provide an Attest Engagement audit report in accordance with AT Section 101.

This report demonstrates an independent service auditor has examined CenturyLink's assertion that the description of its information security program for its network and hosting services provided in the report, is fairly presented and that the information security program governing the services adopts essential elements of the HIPAA Security Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Products and Services Available for HIPAA

Cloud Services
Hybrid-ready public cloud provides the agility, scalability and security expected from an enterprise-class cloud backed by an industry leading global network.

Managed Services
Managed Services secure and optimize network, applications, and infrastructure allowing enterprises to compete at the speed of business.

Managed Security
CenturyLink Managed Security Services provide a full complement of threat prevention, threat management, incident response and analysis services to support your hosted or on-premise enterprise security environments.

Managed Hosting
Maintain complex IT infrastructure and applications with our comprehensive portfolio of Managed Hosting services including fully managed networks, servers, storage, operating systems, and security.

Managed Storage and Backups
Gives a range of storage options including data replication and backup/archiving. CenturyLink solutions are secure, affordable, and can provide data resilience up to five nines.

CSA STAR

In demonstration of its commitment to cyber security and promoting cloud industry best practices, CenturyLink Cloud has submitted a Cloud Security Alliance CSA Consensus Assessments Initiative Questionnaire (CAIQ). This information is publicly available, promoting industry transparency and providing customer visibility into CenturyLink's security practices.

The Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of cloud security industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events, and products.

CSA STAR Program

CSA is the industry organization responsible for STAR — the Security, Trust and Assurance Registry, a cloud security provider certification program. STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings. It is a three-tiered provider assurance program integrating self- assessments, third-party audit, and continuous monitoring.

CSA STAR Self Assessment

CSA Self-Assessment is free and open to all cloud providers and allows them to submit self-assessment reports that document compliance to CSA-published best practices. Since the initial launch at the end of 2011, the CSA has seen tremendous growth in STAR Self Assessment. Cloud providers may submit two different types of reports to indicate their compliance with CSA best practices. Participation in the program is entirely voluntary, and not all cloud vendors rise to this level of scrutiny or security.

The Consensus Assessments Initiative Questionnaire (CAIQ) The CAIQ provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. The questionnaire provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. This is the report that CenturyLink Cloud offers to document compliance and commitment to world-class cybersecurity standards.

The Cloud Controls Matrix (CCM)

The CCM provides a control framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to Information Security (IS) tailored to the cloud industry.

EU DATA Directive

EU Data Protection Directive (Directive 95/46/EC) is a directive adopted by the European Union designed to protect all personal data collected, processed or exchanged for or about citizens of the EU.

Directive 95/46/EC encompasses all key elements from Article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data." These recommendations are founded on seven principles, since enshrined in EU Directive 94/46/EC:

- ***Notice***—data subjects should be given notice when their data is being collected;
- ***Purpose***—data should only be used for the purpose stated and not for any other purposes;
- ***Consent***—data should not be disclosed without the data subject's consent;
- ***Security***—collected data should be kept secure from any potential abuses;
- ***Disclosure***—data subjects should be informed as to who is collecting their data;
- ***Access***—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- ***Accountability***—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Data Directive's Article 29 Working Party

Article 29 of the EU Directive establishes a "Working Party on the Protection of Individuals with regard to the processing of Personal Data". It is generally known as the "Article 29 Working Party". It is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EU Commission acting in an independent and advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics. It also advises the EU Commission on the adequacy of data protection standards in non-EU countries.

The Working Party negotiated with U.S. representatives about the protection of personal data, and the Safe Harbor Principles were the result. According to critics the Safe Harbor Principles do not provide for an adequate level of protection because they contain fewer obligations for the controller and allow the contractual waiver of certain rights.

In October 2015, the European Court of Justice ruled that the Safe Harbor regime was invalid as a result of an action brought by an Austrian privacy campaigner in relation to the export of subscribers' data by Facebook's European business to Facebook in the USA. The US and European Authorities have been working on a replacement version of the Safe Harbor for 2 years, but no agreement has yet been reached. Until a new Safe Harbor is agreed model contract clauses or binding corporate rules may be used as an alternative method of ensuring that data transferred from the EEA to the USA is protected.

The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

EU “Model Contract”

The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26 (4) of directive 95/46/EC that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2). That is, they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

A 'model contract' is a general type of contract that includes specific provisions dealing with data protection, and that has been approved either by the EU Commission or by the Data Protection Commissioner. The EU-approved model contracts are in the form of blank templates, which can be filled in with the appropriate details (names of the organizations, types of personal data, etc.).

The EU's model contracts are available from the EU Commission website.

There are two types of model contracts:

- A contract to facilitate a transfer of personal data between a data controller in the EEA, and a data controller outside the EEA; and
- A contract to facilitate transfer of personal data between a data controller in the EEA, and an agent or subcontractor – referred to as a 'data processor' – located outside the EEA.

The data controller located in the EEA is referred to in the contracts as a *data exporter*; the other party, located outside the EEA, is termed a *data importer*.

German Federal Data Protection

The Bundesdatenschutzgesetz, or BDSG, is Germany’s Federal Data Protection Act. Enacted in 1970 and later amended in 1990 and 2009 as the use of information technology grew, the regulatory framework was created and expanded to protect and safeguard the use of personal data. In addition to the incremental BSDG compliant standards, the act requires all parties to assure that Safe Harbor requirements are also met.

CenturyLink maintains a standard operating MSA and Annex clearly identifying scope, responsibilities, and obligations, enabling CenturyLink Cloud customers to remain in BDSG compliance. CenturyLink ensures the required technical and organizational measures are adhered to for protection of personal data against misuse and loss in accordance with the requirements of the BDSG.

OSPAR

Outsourcing continues to be prevalent in today's business landscape. In outsourcing, Financial Institutions (FIs) rely on the Outsourced Service Providers (OSPs) to handle certain business functions. Outsourcing has proven to be effective; however FIs should ensure that their service providers maintain the same level of governance, rigor, and consistency as themselves.

Loss of sensitive customer data or loss of service capability may result in reputation risk or regulatory breaches. Outsourcing risks must be managed, to not adversely affect the FIs' operations and customers. The service can be outsourced, but the risk cannot.

To address this, the Association of Banks in Singapore (ABS) has established this industry set of standards and controls for the FIs' Outsourced Service Providers (OSPs) operating in Singapore. These Guidelines form the minimum baseline controls that OSPs, which wish to service the FIs, should have in place. However, FIs with specific needs would continue to liaise with their OSPs on a bilateral basis to impose any additional specific requirements. Establishing a banking industry standard baseline will assure FIs of the appropriate design of their OSP's internal controls and the effectiveness of those controls. OSPAR is specific to Singapore at this time for CenturyLink.

Regulation vs. Framework

Regulatory compliance refers to the adherence to laws, regulations, guidelines, and specifications relevant to an organization's business. Subsequently compliance risk — or more accurately the risk of noncompliance — is associated with civil punishment through regulatory penalties as the result of negligence due to a general failure to comply with applicable requirements. Typical compliance requirements include legislation such as the Dodd-Frank Act, and regulations such as HIPAA and PCI. And in some cases, there may be a risk of criminal punishment, as with Sarbanes-Oxley (SOX).[2]

A security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are basically an outline for building an information security program to manage risk and reduce vulnerabilities and are used to define and prioritize the tasks required to build security into an organization. By contrast, a regulatory compliance is an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business needs.[3]

Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use. There are frameworks that are developed for specific industries as well as different regulatory compliance goals. They also come in varying degrees of complexity and scale. However, you will find that there is a large amount of overlap in general security concepts as each one evolves.[3]

The beauty of any of these frameworks is that there is overlap between them; the Cloud Security Alliance (CSA) developed the Cloud Controls Matrix (CCM), which gives a detailed understanding of security concepts, and principles that are aligned to the CSA guidance in 13 domains. As a framework the CCM provides the needed structure, detail and clarity relating to information security tailored to the cloud industry. CenturyLink has taken the next step to provide a publically available

Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document the security controls existing in IaaS, PaaS and SaaS offerings.

The CAIQ provides a set of over 140 questions a cloud consumer and a cloud auditor may wish to ask of a cloud provider.[4] For example, ISO 27002 defines information security policy in Section 5; COBIT defines it in the section "Plan and Organize"; Sarbanes Oxley defines it as "Internal Environment"; HIPAA defines it as "Assigned Security Responsibility"; and PCI DSS defines it as "Maintain an Information Security Policy." By using a common framework like ISO 27000, a company can then use the CAIQ as a "crosswalk" to show compliance with multiple regulations such as PCI DSS, HIPAA, FISMA, and the Sarbanes-Oxley Act (SOX).

Considering there are many regulatory requirements, simply determining what is required can be a daunting task. Frameworks provide the necessary guidance for both the service provider as well as the auditor seeking evidence of compliance. With these frameworks as guidance merely achieving and maintaining compliance isn't an easy task. On the flip side, the consequences of non-compliance can be detrimental.

CenturyLink Compliance

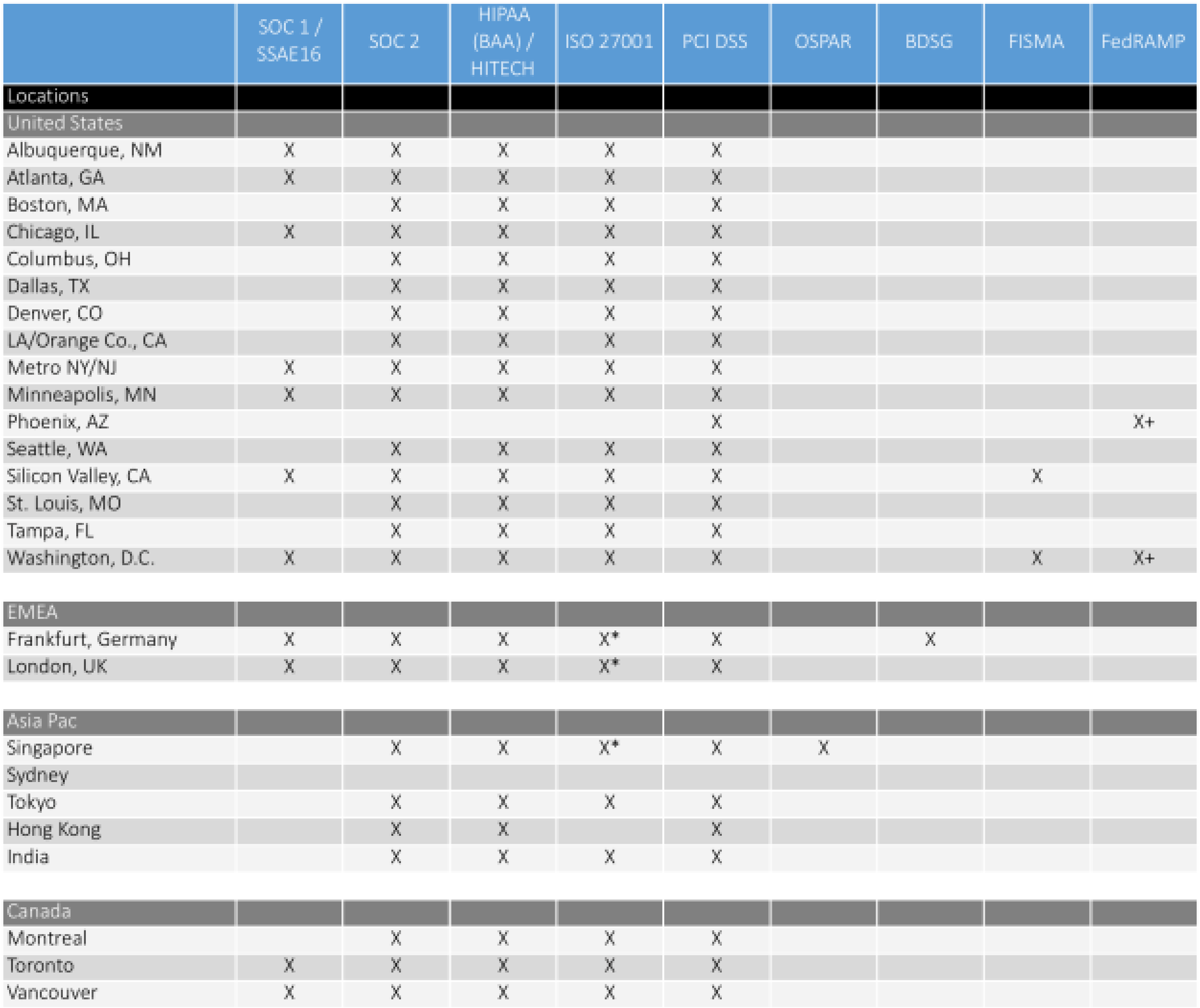
CenturyLink builds solutions tailored to the compliance and security requirements of the customer. The solutions are engineered and managed to help enable customers to meet compliance standards. This includes role-based administration, the use of hardware with no removable media, support for data encryption in transit and at rest, destruction of data on failed drives and hardware housed in secured physical cages. An accredited third-party audits every data center regularly. 56 of CenturyLink's globally located data centers are SSAE 16 audited.

Compliance engages external audit firms to perform multiple assessments designed to address CenturyLink customers' diverse compliance requirements. Schellman (formerly Brightline CPAs & Associates, Inc.) is one of these firms and is the first and only company in the world accredited to perform a suite of services that includes SSAE16/ISAE3402 SOC1 examinations, SOC 2/3 examinations, PCI/DSS compliance validation and ISO 27001:2013 certification. Coalfire performs assessments associated with PCI/ROCs.

CenturyLink protects its customers' most sensitive information through the strictest of policies and procedures. Data replication is a critical part of CenturyLink's working disaster recovery strategy, and only ship data backups to data centers within the same region in support of customers with data sovereignty requirements. Role-based system access of the CenturyLink Cloud Platform is aligned with specific roles that govern what can be done in the system. More granular permissions can be added to individual server groups.

All activities against cloud servers are automatically logged and stored up to a specific time period to meet the customer's compliance requirements. This ensures quick identity of who has performed what actions in the cloud environment. What is more, humans cannot edit these logs. CenturyLink data centers enforce strict controls and secure access to the physical hardware. This includes fully secured server cages and 24/7 monitoring.

Availability Matrix



	SOC 1 / SSAE16	SOC 2	HIPAA (BAA) / HITECH	ISO 27001	PCI DSS	OSPAR	BDSG	FISMA	FedRAMP
Locations									
United States									
Albuquerque, NM	X	X	X	X	X				
Atlanta, GA	X	X	X	X	X				
Boston, MA		X	X	X	X				
Chicago, IL	X	X	X	X	X				
Columbus, OH		X	X	X	X				
Dallas, TX		X	X	X	X				
Denver, CO		X	X	X	X				
LA/Orange Co., CA		X	X	X	X				
Metro NY/NJ	X	X	X	X	X				
Minneapolis, MN	X	X	X	X	X				
Phoenix, AZ					X				X+
Seattle, WA		X	X	X	X				
Silicon Valley, CA	X	X	X	X	X			X	
St. Louis, MO		X	X	X	X				
Tampa, FL		X	X	X	X				
Washington, D.C.	X	X	X	X	X			X	X+
EMEA									
Frankfurt, Germany	X	X	X	X*	X		X		
London, UK	X	X	X	X*	X				
Asia Pac									
Singapore		X	X	X*	X	X			
Sydney									
Tokyo		X	X	X	X				
Hong Kong		X	X		X				
India		X	X	X	X				
Canada									
Montreal		X	X	X	X				
Toronto	X	X	X	X	X				
Vancouver	X	X	X	X	X				

ISO 27001 – X* = Global Network Services and Managed Hosting Services – X = Colocation Only FedRAMP – X+ = Moderate controls, defined by FedRAMP for the physical and environmental controls

Glossary

AIPCA
The association that develops and scores the Uniform Certified Public Accountants examination. The organization serves as an advocate before legislative bodies, public interest groups and other professional organizations, provides educational guidance materials to its members and monitors and enforces member compliance with certified public accountants' technical and ethical standards.

AOC
Attestation of Compliance is a form for merchants and service providers to attest to the results of an assessment as documented in the Report on Compliance (ROC)

ATO
Authorization to Operate

BA - A Business Associate is a person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

BAA - Business Associates Agreement

CAIQ - A spreadsheet providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency.

CCM - A matrix specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

CE - Under HIPAA, a Covered Entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

CSA - An organization that promotes research into best practices for securing cloud computing and the ability of cloud technologies to secure other forms of computing.

ePHI - Electronic protected health information refers to any protected health information (PHI) that is covered under HIPAA security regulations and is produced, saved, transferred or received in an electronic form.

FISMA - FISMA represents a compliance framework and stands for the Federal Information Security Management Act. It was enacted in 2002 and requires all federal agencies, departments, and their contractors to adequately safeguard their information systems and assets.

FedRAMP - Stands for the Federal Risk and Authorization Management Program. It was enacted in December, 2011 and requires all federal organizations that use, or plan to transition to, a cloud environment to implement the FedRAMP program for cloud security controls.

HIPAA - A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.

ISO - ISO is an international organization composed of national standards bodies from over 75 countries.

ISO 27001 - ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

JAB - Joint Authorization Board, The primary governance and decision-making body for FedRAMP are the Chief Information Officers (CIOs) from the Department of Homeland Security (DHS), General Services Administration (GSA), and Department of Defense (DOD).

OSPAR - To establish an industry standard baseline and controls for Outsourced Service Providers (OSPs) operating in Singapore to assure Financial Institutions (FIs) of the appropriate design of their OSP's internal controls and the effectiveness of those controls.

P-ATO - Provisional Authorization to Operate

PCI DSS - A standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customer's credit card data.

PCI ROC - Report on Compliance is a report containing the details of an entity's compliance status and documents the specific parts in scope of the assessment.

PHI - Individually identifiable health information collected from an individual that is created or received by a healthcare provider, employer, or plan. Any information related to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This may include, but is not limited to:

- Patient's Name
- Patient's Social Security Number
- Phone Number or Address
- Medical History
- Current Medical Condition
- Test results and images

SOC 1 - Service Organization Controls Report - Examination engagements undertaken by a service auditor to report on controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.

SOC 2 - Service Organization Controls Report - Reports on various organizational controls related to security, availability, processing integrity, confidentiality or privacy. The standard for regulating these five issues was formed under the AICPA Trust Services Principles and Criteria.

Appendix

Reference 1

HIPAA Privacy, Security, and Breach Notification Audit Program

Reference 2

Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection

Lessons Learned from OCR Privacy and Security Audits - IAPP Global Privacy Summit 2013

Reference 3

IT security frameworks and standards: Choosing the Right One

Reference 4

STAR Self Assessment

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

Global Headquarters	United Kingdom	Singapore	Toronto, ON
Monroe, LA (800) 784-2105	+44 (0)118 322 6000	+65 6768 8098	1-877-387-3764
EMEA Headquarters	**Asia Pacific Headquarters**	**Canada Headquarters**	

This document is to serve as an informational resource guide only. Customers are responsible for their assessment and implementation of any resources within this guide. This document does not create any guarantees, warranties, or contractual commitments, and does not alter any current contracts or agreements with CenturyLink customers. This document represents CenturyLink's products and offerings as of the date of issue. Services not available everywhere. Business customers only. CenturyLink may change or cancel services or substitute similar services at its sole discretion without notice.

740102315 - compliance-resource-guide-CM150983