Introduction to regulatory compliance

02/11/2019 • 3 minutes to read • Contributors

In this article

HIPAA
PCI
PII
GDPR
Compliant foundation in Azure

This is an introductory article about regulatory compliance, therefore it's not intended for implementing a compliance strategy. It is for general awareness only. More detailed information about Azure compliance offerings is available at the Microsoft Trust Center. Moreover, all downloadable documentation is available to Azure customers under a nondisclosure agreement from the Microsoft Service Trust Portal.

Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws enforced by governing bodies in their geography or rules required by voluntarily adopted industry standards. For IT regulatory compliance, people and processes monitor corporate systems in an effort to detect and prevent violations of policies and procedures established by these governing laws, regulations, and standards. This in turn applies to a wide array of monitoring and enforcement processes. Depending on the industry and geography, these processes can become quite lengthy and complex.

For multinational organizations (particularly those in heavily regulated industries, such as healthcare and financial services), compliance can be challenging. Standards and regulations abound, and in certain cases can change frequently. This can make it difficult for businesses to keep abreast of evolving international electronic data handling laws.

As with security controls, organizations should understand the division of responsibilities regarding regulatory compliance in the cloud. Cloud providers strive to ensure that their platforms and services are compliant. But organizations also need to confirm that their applications, the infrastructure those applications depend on, and services supplied by third parties are also certified as compliant.

The following are descriptions of compliance regulations in various industries and geographies:

HIPAA

A healthcare application that processes protected health information (PHI) is subject to both the Privacy Rule and the Security Rule encompassed within the Health Information Portability and Accountability Act (HIPAA). At a minimum, HIPAA could likely require that a healthcare business receive written assurances from the cloud provider that it will safeguard any PHI received or created.

PCI

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes, including Visa, MasterCard, American Express, Discover, and JCB. The PCI standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit-card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm-specific Internal Security Assessor (ISA) who creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by a Self-Assessment Questionnaire (SAQ) for companies.

PII

Personally identifiable information (PII) is any datapoint that could be used to identify a consumer, employee, partner, or any other living or legal entity. Many emerging laws, particularly those dealing with privacy and individual PII, require that businesses themselves comply and report on compliance and any breaches that might occur.

GDPR

One of the most important developments in this area is the recent enactment by the European Commission of the General Data Protection Regulation (GDPR), designed to strengthen data protection for individuals within the European Union. GDPR requires that data about individuals (such as "a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address") be maintained on servers within the EU and not transferred out of it. It also requires that companies notify individuals of any data breaches, and mandates that companies have a data protection officer (DPO). Other countries have, or are developing, similar types of regulations.

Compliant foundation in Azure

To help customers meet their own compliance obligations across regulated industries and markets worldwide, Azure maintains the largest compliance portfolio in the industry—in breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). Azure compliance offerings are grouped into four segments: globally applicable, US Government, industry-specific, and region/country-specific.

Azure compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Each offering description in this document provides an up-to-date scope statement indicating which Azure customer-facing services are in scope for the assessment, as well as links to downloadable resources to assist customers with their own compliance obligations.

More detailed information about Azure compliance offerings is available from the Microsoft Trust Center. Moreover, all downloadable documentation is available to Azure customers under a nondisclosure agreement from the Service Trust Portal in the following sections:

- **Audit reports:** Includes sections for FedRAMP, GRC assessment, ISO, PCI DSS, and SOC reports.
- **Data protection resources:** Includes compliance guides, FAQ and white papers, and pen test and security assessment sections.