Compliance at Box

Overview

As the leading Cloud Content Management (CCM) platform, Box enables advanced privacy and compliance in the digital age, no matter which industry or geography our customers are in. Box is committed to providing our customers a CCM solution that helps them meet and exceed their regulatory and compliance needs and obligations.

Box has achieved a number of certifications that demonstrate our capabilities and commitment to security. This knowledge paper is provided without NDA and highlights some of our key certifications to document our investments in compliance and security across our platform.

The specific certifications may be obtained under NDA with Box and the list below is not intended to be an exhaustive list of Box's security compliance posture.

Box Certifications and Third-Party Reports

- **SOC 1 (Service Organization Controls) / SSAE18 Type II**

  Box maintains a SOC 1 report issued by an independent third-party assessor based on the SSAE 18 standard. The SOC 1 allows companies that use Box to support their financial reporting requirements (e.g., Sarbanes-Oxley) and gives them assurance that Box has appropriate internal controls in place.

- **SOC 2 / SOC 3 (Service Organization Controls) / AT-C 205 Type II**

  Box maintains SOC 2 and SOC 3 reports for the Security, Availability, and Confidentiality Trust Service Principles, which are based on the American Institute of CPAs TSP Section 100 2017 Trust Services Criteria. The SOC 2 and SOC 3 reports are issued by an independent third-party assessor who validates the controls and processes Box has implemented to make Box secure and highly available while protecting the confidentiality of customer data.

  Box's SOC 3 Report can be viewed on Box's Trust Center (https://www.box.com/trust).

- **International Organization for Standardization (ISO) 27001:2013**

  Box has achieved ISO 27001 certification for its Information Security Management System, which covers the entire Box cloud collaboration platform and all supporting infrastructure. A globally recognized security standard, ISO 27001 provides a guideline for the information security policies and controls that an organization should have in place to secure their systems. Through ISO 27001 compliance, customers can be assured that Box has a formal information security program, based on a highly recognized international standard, which has been validated by an independent third-party auditor.
  Box's ISO 27001 certificate can be viewed on Box's Trust Center (https://www.box.com/trust).

- **International Organization for Standardization (ISO) 27017:2015**

  Box has achieved ISO 27017 certification which defines requirements and includes guidance for information security controls applicable to the provision and use of cloud services. It sets forth an additional set of controls that must be implemented alongside a company's existing ISO 27001 program and has been validated by an independent third-party auditor.
  Box's ISO 27017 certificate can be viewed on Box's Trust Center (https://www.box.com/trust).

- **International Organization for Standardization (ISO) 27018:2014**

  Box has achieved ISO 27018 certification which defines requirements and includes guidance on how to implement processes to protect personally identifiable information (PII). It sets forth an additional set of controls that must be implemented alongside a company's existing ISO 27001 program and has been validated by an independent third-party auditor.
  Box's ISO 27018 certificate can be viewed on Box's Trust Center (https://www.box.com/trust).

- **FINRA (Financial Industry Regulatory Authority) / SEC 17a-4**
  SEC 17a-4 is a regulation enforced by FINRA, for the retention and storage of electronic broker-dealer records. With Box Governance, Box enables institutions in highly regulated industries, like financial services, to comply with retention requirements such as SEC 17a-4 while using Box.

- **HIPAA (Health Insurance Portability and Accountability Act) / HITECH (Health Information Technology for Economic and Clinical Health) Act**
  In 2012, Box announced compliance with HIPAA and HITECH obligations, reinforcing Box's position as a secure cloud platform for collaboration, external sharing, and mobile productivity. Being able to configure Box in a HIPAA-compliant way allows covered healthcare entities—providers, insurers, life sciences innovators and data processors—to improve the efficiency of their daily operations and focus on improving real health outcomes for patients and Box will sign a Business Associate Agreement (BAA) with customers.

- **Payment Card Industry Data Security Standard (PCI DSS)**
  Box obtained PCI DSS Level 1 compliance as a service provider which allows customers to store payment card data in the Box platform. Achieving the highest level of compliance demonstrates that the security of the infrastructure meets these extensive and rigorous requirements and safely store information such as payment card data with assurance that they are meeting their compliance obligations.

- **FedRAMP/FISMA (Federal Risk and Authorization Management Program; Federal Information Security Management Act)**
  FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. FedRAMP is mandatory for Federal Agencies moving services to the cloud. FedRAMP, like FISMA, is based off the NIST 800-53 standard of controls and Box also is FISMA compliant. Box has been granted an Authority to Operate and is listed on FedRAMP.gov as a FedRAMP Authorized system.

- **Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Level 4 Authorization**
  The DoD Cloud SRG sets security requirements for the Department of Defense for Cloud Computing. Box has been accredited at Impact Level 4 which is for Controlled Unclassified Information (CUI) which includes Export Control, Privacy Information and Protected Health Information.

- **Information System Security Management and Assessment Program (ISMAP) – Japan**

  ISMAP is a Japanese government security assessment program to ensure that Cloud Providers meet an appropriate level of security for the Japanese government. Box has been evaluated and has been approved under the ISMAP program by the Japanese government and is registered on ismap.go.jp.

Summary

Box is designed with the security and privacy of customers in mind and strives to meet and exceed industry best practices. Box's controls are independently validated and demonstrates Box's commitment to security and compliance.