



Akamai Compliance Management

Reduce Risk with SSL Delivery and Acceleration Services
Help support PCI, ISO, FISMA, BITS and HIPAA Compliance Initiatives

Maintaining regulatory compliance for your business takes a lot of work. Akamai Compliance Management provides tools and documentation to assist with compliance initiatives for delivering business applications and websites. It increases confidence in meeting regulatory standards required for credit card transactions (PCI), federal information security management (FISMA), the ISO Code of Practice for Information Security Management (ISO 27001/27002), and financial services regulations (BITS) and the Health Insurance Portability and Accountability Act (HIPAA).^{1*}

Akamai Compliance Management can help streamline your compliance initiatives. Akamai helps assure that the delivery of your data does not negatively impact compliance with a variety of standards required for your business. Continuing to adapt to new frameworks, Akamai Compliance Management offers modules to help customers in their efforts to maintain compliance with PCI, FISMA, ISO, BITS, and HIPAA standards and regulations.

PCI Module

Any business accepting credit card transactions has a responsibility to protect customer transaction data. The PCI Security Standards Council defined the PCI Data Security Standard (PCI DSS), a global standard for safeguarding credit card data, covering the end-to-end-card transaction infrastructure, including all systems that process, store, or transmit credit card data. Steep financial penalties apply to merchants and banks that are out of compliance.

Whether a global commerce company or an emerging online business is looking to leverage the web as an efficient business channel, the risk of non-compliance is a significant issue.

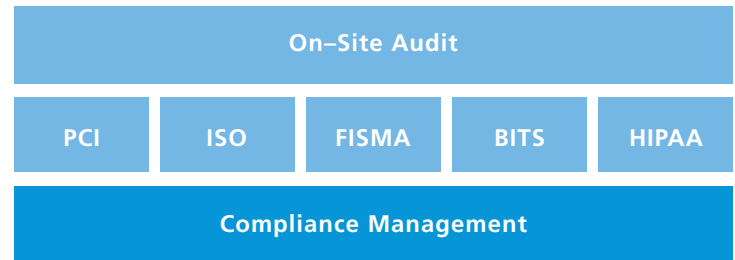
Achieving PCI compliance can be an involved and costly process, often requiring independent audits and multi-step certification processes of the end-to-end card transaction infrastructure. As the leading commerce accelerator for the majority of the world's largest e-commerce firms, Akamai proactively achieved and maintains PCI Compliance of Akamai's SSL network. This translates into pre-certification of this portion of the overall infrastructure, reducing validation requirements for compliance.

The PCI Module packages services, support, reporting, documentation, and service terms to help support PCI compliance validation for customers leveraging the network.

What's Included in the PCI Module:

Akamai's network, management infrastructure, and associated processes and procedures, are consistent with the "best practice" security requirements of PCI. The pre-established Akamai certification will accelerate the overall PCI compliance process. The PCI Module includes:

- Akamai PCI Certificate of Compliance
- Standard terms and conditions for PCI
- Executive summary of Akamai's quarterly SSL network scanning reports
- Configuration validation tool available via the portal
- Service integration tools and guidelines to ensure client metadata is configured per PCI DSS
- PCI Incident notification and response procedures
- Includes a summary of Akamai's stance addressing the sections of the PCI standard as they apply to Akamai, with links to more detailed supporting documentation.



PCI DSS Section	PCI DSS Requirement	Akamai's Approach	Documentation (PDF)
1	Install and maintain a firewall configuration to protect cardholder data.	Akamai's Secure Content Delivery Network is a set of publicly accessible servers that do not store cardholder data. The proprietary TRIP software router reduces inappropriate connections while functioning as a load balancer.	Secure Content Delivery Network
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	All software on the Secure Content Delivery Network is either custom-written for Akamai or modified and secured. Access to the network is controlled by the specialized Authgate program, which uses individual SSH keys rather than passwords.	Access Control Description
3	Protect stored cardholder data.	Akamai does not store cardholder data.	
4	Encrypt transmission of cardholder data across open, public networks.	The Secure Content Delivery Network encrypts traffic sent over the public internet. Customers can set their own security parameters, within the guidelines of PCI compliance.	PCI DSS Compliance Configuration Guide
5	Use and regularly update anti-virus software or programs.	The Secure Content Delivery Network is composed entirely of servers running Linux, an operating system that is seldom affected by malicious software and traditionally does not require the use of anti-virus programs.	

ISO Module

The ISO 27001/27002 standards for information security outline hundreds of potential controls, control mechanisms, and best practices. The standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization. The framework covers structure, risk assessment and treatment, security policy, organization of information security, asset management, human resources security, physical security, communications and operations management, access control, information security incident management, business continuity, and compliance.

The ISO Module packages services, documentation, and service terms facilitating fast compliance validation for ISO 27001/27002 to customers leveraging the Akamai EdgePlatform.

What's Included in the ISO Module:

Akamai's network, management infrastructure, and associated processes and procedures, are consistent with the security requirements of ISO.

The ISO module of Akamai Compliance Management will accelerate the overall ISO 27001/27002 compliance process. The ISO Module includes:

- Standard terms and conditions for ISO 27001/27002
- Executive summary of Akamai's annual ISO 27001/27002 assessment
- Incident response procedures
- Includes a summary of Akamai's stance addressing the sections of the ISO 27001/27002 standard as they apply to Akamai, with links to more detailed supporting documentation.

FISMA Module

The Federal Information Security Management Act (FISMA) is a United States Federal law that requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. In August 2009, Akamai was issued an Authorization to Operate (ATO) from the Department of Homeland Security under NIST Special Publication 800-53.

FISMA requires periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. It requires policies, procedures, testing, corrective action planning, and training, based on risk assessments, to ensure information security is addressed throughout the life cycle of each organizational information system.

The FISMA Module packages services, documentation, and service terms facilitating fast compliance validation of standards established by the Federal Information Security Management Act by customers leveraging the Akamai EdgePlatform.

ISO COMPLIANCE DOCUMENTATION

Akamai Compliance Management ISO provides information on Akamai's compliance with ISO Standards.

This page includes the ISO information you are most likely to need:

- Table showing summary for each ISO section, with links to details.
- Compliance Management ISO Terms and Conditions.

For additional information:

- Open the ISO Quick Facts document for short answers on basics of the service.
- Search the Compliance Management knowledgebase.

ISO Compliance by Section Number

This table summarizes how Akamai complies with ISO, arranged by ISO section number. Links in the Documentation column open PDF files describing compliance for the specific ISO Section number. Or you can download a zip file of all the documentation in the table.

ISO Section	ISO Requirement	Akamai's Approach	Documentation (PDF)
5	Security Policy	Akamai maintains a security policy which is available to all employees. The penalty for security violations can include termination.	Safety and Security Akamai Information Security Policy
6	Organization of information security	Akamai has a dedicated Information Security team, headed by the Senior Director of Information Security. Akamai's Deputy General Counsel is the Chief Privacy Officer.	PII InfoSec_Duties Akamai Information Security Policy
7	Asset Management	Physical assets belonging to Akamai are tracked in databases. Rules and limits are in place for the use of Akamai's assets.	Electronic_Communications_Policy PDAs
8	Human Resources Security	Employees of Akamai are granted the access necessary to perform their jobs, and receive annual training on security and ethics. Akamai performs background checks on new hires and immediately revokes access for employees leaving the company.	Akamai_Background_Check_Policy Guiding_Principles Security_Awareness_Policy
9	Physical and Environmental Security	By design, Akamai's deployed networks are accessible via the public internet. Corporate systems have additional protections in place to protect against malware. Akamai offices are locked and only employees have regular access to them.	Akamai_Anti-Virus_Policy

FISMA COMPLIANCE DOCUMENTATION

Akamai Compliance Management FISMA provides information on Akamai's compliance with the FISMA Security Standards.

This page includes the FISMA information you are most likely to need:

- Table showing summary for each FISMA section, with links to details.
- Compliance Management FISMA Terms and Conditions.

For additional information:

- Open the NIST Quick Facts document for short answers on basics of the service.
- Search the Compliance Management knowledgebase.

FISMA Compliance by NIST 800-53 Section Number

This table summarizes how Akamai complies with FISMA, arranged by NIST 800-53 section number. Links in the Documentation column open PDF files describing compliance for the specific NIST 800-53 Section number. Or you can download a zip file of all the FISMA documentation in the table.

NIST 800-53 Section	FISMA Requirement	Akamai's Approach	Documentation (PDF)
AC	Access Control	Access to Akamai's deployed networks is tightly controlled and formally approved; access is limited to Akamai employees who need to access it as part of their job duties. All access is done via an encrypted connection. Developers may not access the production networks.	Deployed Network Access
AT	Awareness and Training	Akamai trains all new hires on security practices and runs an annual security awareness campaign.	Security Awareness Policy
AU	Audit and Accountability	The Alert Management System oversees Akamai's deployed networks in real time, sending alerts to Akamai's NOCC (Network Operations Control Center), which runs continuously. Logs are stored for forensic purposes, and are accessible via the Query reporting tool.	Alert Management Software
CA	Security Assessment and Authorization	Customers following NIST 800-53 work with Akamai to maintain their compliance.	
CM	Configuration Management	Changes to the Akamai deployed networks proceed through a series of regular steps. Development follows best-practice guidelines to create a single, atomic release (rather than a release followed by patches), resulting in a hand-off to the System Quality	QA_SOGs Software Development Process

What's Included in the FISMA Module:

Akamai's network, management infrastructure, and associated processes and procedures, are consistent with the security requirements specified by the Federal Information Systems Management Act and the NIST Special Publication 800-53. The FISMA module of Akamai Compliance Management will accelerate the overall FISMA compliance process. The FISMA Module includes:

- Standard terms and conditions for the Federal Information Systems Management Act
- Incident response procedures
- Includes a summary of Akamai's stance addressing the sections of the NIST 800-53 standard as they apply to Akamai, with links to more detailed supporting documentation.

BITS Module

BITS (www.bits.org) is a division of The Financial Services Roundtable and a not-for-profit industry consortium whose members are 100 of the largest financial institutions in the United States.

BITS requires periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. It requires policies, procedures, testing, corrective action planning, and training, based on risk assessments, to ensure information security is addressed throughout the life cycle of each organizational information system.

The BITS Module packages documentation and service terms facilitating fast compliance validation of standards established by the BITS self-assessment effort for customers leveraging the Akamai EdgePlatform.

What's Included in the BITS Module:

Akamai's network, management infrastructure, and associated processes and procedures, are consistent with the security requirements specified by the BITS standard. The BITS module of Akamai Compliance Management will accelerate the overall BITS compliance process. The BITS Module includes:

- Standard terms and conditions for BITS
- Incident response procedures
- Includes a summary of Akamai's stance addressing the sections of the BITS standard as they apply to Akamai, with links to more detailed supporting documentation.

BENEFITS TO YOUR BUSINESS

- **Reduced Risk:** *Pre-authorized compliance terms for the Akamai SSL network and, 'best-practice' guidance lead to reduced risk of being out of compliance.*
- **Extend your network:** *Akamai Compliance Management makes it easier to use Akamai as an extension of your network, relative to your compliance efforts.*
- **Faster Compliance:** *Easy-to-use validation tools and documentation combined with pre-certification of the Akamai SSL network accelerates and streamlines the overall compliance process.*
- **Compliance-related Cost Savings:** *Complete compliance documentation reduces the customer's burden in accomplishing compliance review on end-to-end network infrastructure.*

BITS COMPLIANCE DOCUMENTATION

Akamai Compliance Management BITS provides information on Akamai's compliance with the BITS Security Standards.

This page includes the BITS information you are most likely to need:

- Table showing summary for each BITS section, with links to details.
- Compliance Management BITS Terms and Conditions.

For additional information:

- Open the [BITS Quick Facts](#) document for short answers on basics of the service.
- Search the Compliance Management [knowledgebase](#).

BITS Compliance

This table summarizes how Akamai complies with BITS, arranged by BITS SIG Tab number. Links in the Documentation column open PDF files describing compliance for the specific BITS SIG Tab number. Or you can download a zip file of all the BITS documentation in the table.

BITS SIG Tab	Topic	Akamai's Approach	Documentation (PDF)
A	Risk Management	Akamai performs regular internal reviews and risk assessments for corporate, information, and network security. As Akamai continues to roll out new services on its network, security is incorporated into product design and review. Akamai's security professionals meet regularly with a cross-functional executive team to review corporate and network security issues.	Vulnerability Management Process
B	Security Policy	Akamai maintains a security policy which is available to all employees. The penalty for security violations can include termination.	Akamai Information Security Policy Safety and Security
C	Organizational Security	The Sr. Director of Information Security is the senior executive responsible for overseeing all of Akamai's security efforts. The Sr. Director reports to the Sr.VP of Operations and meets with the Akamai Executive Committee monthly to review the current security posture of the company.	Akamai Information Security Policy NDA Template for 3rd Parties

HIPAA Module

Many healthcare and pharmaceutical organizations and their business associates are required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related regulations such as HITECH. HIPAA, the health information “Privacy Rule” and “Security Rule”, and HITECH provide federal protections for personal health information held by covered entities and give patients an array of rights with respect to that information.

HIPAA and related regulations specify a series of administrative, physical, and technical safeguards to use to assure the confidentiality, integrity, and availability of electronic protected health information. The Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”), in particular, addresses the technical and non-technical safeguards that organizations must put in place to secure protected health information (PHI).

The HIPAA Module packages documentation and service terms facilitating fast compliance validation of regulations enforced by the U.S. Department of Health and Human Services (HHS) for customers leveraging the Akamai EdgePlatform.

What’s Included in the HIPAA Module:

Akamai’s network, management infrastructure, and associated processes and procedures, are consistent with the security requirements specified by HIPAA and related regulations. The HIPAA module of Akamai Compliance Management will accelerate the overall HIPAA compliance process. The HIPAA Module includes:

- Standard terms and conditions for HIPAA
- Incident response procedures
- Documentation addressing the sections of the HIPAA “Security Rule” and “Privacy Rule” as they apply to Akamai
- A summary of Akamai’s stance, section by section

HIPAA COMPLIANCE DOCUMENTATION	
Akamai Compliance Management HIPAA describes Akamai’s compliance with the HIPAA Security Standards. The table below provides a listing of the Akamai documentation for each HIPAA section. For each section it provides the following:	
<ul style="list-style-type: none"> • Implementation specifications • Akamai’s approach • Links to additional documentation 	
You may also download a zip file of the HIPAA documentation.	
Health Insurance Reform: Security Standards; Final Rule	
Department of Health and Human Services, 68 Federal Register 8334, 45 CFR Parts 160, 162, and 164, February 20, 2003	
The document itself explains that “This final rule adopts standards as required under title II, subtitle F, sections 261 through 264 of the Health Insurance Portability and accountability Act of 1996 (HIPAA).” More casually, this document is sometimes called the “Security Rule”, and it covers how electronic data including protected health information (PHI) must be handled.	
For details see Akamai HIPAA Compliance (PDF). You may also download a zip file of the HIPAA documentation.	
Section	Documentation (PDF)
164.308(a)(1)(i) Standard: Security management process.	Vulnerability Management Process ISO 27001 Report Summary Akamai Technical Crisis and Incident Management Procedure Safety and Security Alert Management Software Removal of Operational Data From Test Network
164.308(a)(2) Standard: Assigned security responsibility	Akamai Information Security Policy
164.308(a)(3)(i) Standard: Workforce security	Deployed Network Access Access Control Description Akamai Background Check Policy Sensitive Termination Process for Automated Systems
164.308(a)(4)(i) Standard: Information access management	Deployed Network Access Access Control Description Protecting Confidential, Proprietary, and Personal Information

On-Site Audit Module

Akamai offers On Site Audit Modules for PCI, ISO, FISMA, BITS, and HIPAA. Any customers needing support from Akamai in order to verify compliance to a given standard will be supported by members of Akamai’s Information Security (InfoSec) team. The audit is structured as a fixed price engagement delivered at Akamai’s corporate offices in Cambridge, MA over 5 consecutive business days. Akamai’s Infosec team will work with customers to determine the most effective way to demonstrate the key facets of our services and will design and host a customized engagement for each customer. Additional needs for time or support may be arranged through a separate customer engagement agreement.

†This service does not guarantee compliance against a standard, but helps customers support their compliance programs.

The Akamai Difference

Akamai® makes the Internet work for some of the best-known companies in the world with its solutions for cloud computing, eCommerce, Web sites, HD video and software-as-a-service. Delivering unmatched performance, scale and security, Akamai’s solutions are built on the Akamai Intelligent Internet Platform™, unique in the industry due to its rich functionality and intelligence and because it is globally distributed across 650 cities, in 72 countries and integrated into about 1,000 of the Internet’s most important networks. To learn more visit www.akamai.com or follow us on Twitter @akamai.

Akamai Technologies, Inc.

U.S. Headquarters

8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
(877.425.2624)

www.akamai.com

International Offices

Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore



©2011 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice.