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), 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 achieves 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

<table>
<thead>
<tr>
<th>PCI DSS Section</th>
<th>PCI DSS Requirement</th>
<th>Akamai’s Approach</th>
<th>Documentation (PDF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>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 Authenticator program, which uses individual SSH keys rather than passwords. Access Control Description</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Akamai does not store cardholder data.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>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.</td>
<td>PCI DSS Compliance Configuration Guide</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>The Secure Content Delivery Network is composed entirely of servers running Linux, an operating system that is seldom affected by malicious software, such as Trojanized shell scripts.</td>
<td></td>
</tr>
</tbody>
</table>
Akamai Compliance Management

- 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
- 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.

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 for 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
- 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.
Akamai Compliance Management

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

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
- 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
- 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.

**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:

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

<table>
<thead>
<tr>
<th>BITS MS Tab</th>
<th>Topic</th>
<th>Akamai’s Approach</th>
<th>Documentation (PDF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Risk Management</td>
<td>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.</td>
<td>Vulnerability Management Process</td>
</tr>
<tr>
<td>B</td>
<td>Security Policy</td>
<td>Akamai maintains a security policy which is available to all employees. The penalty for security violations can include termination.</td>
<td>Akamai Information Security Policy Safety and Security</td>
</tr>
<tr>
<td>C</td>
<td>Organizational Security</td>
<td>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 to review the current security posture of the company.</td>
<td>Akamai Information Security Policy NDA Template for 3rd Parties</td>
</tr>
</tbody>
</table>

**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.
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 address 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

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.

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