Information Security Standard compliances

Compliance is a critical component of any security program. Compliance lives by the rule that states **We Trust but Verify**. The concept is that we must obtain evidence of compliance with stated policies, standards, laws, regulations, etc. in order to issue the proper attestations as required.

Compliance, which is only a point in time, is directly impacted by the ever changing and always evolving rules and regulations which makes it quite challenging for organizations to maintain a sound compliance posture. The continuous expansion and extension of our production environments also adds to the compliance challenges we all face today

Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so. Software, for example, may be developed in compliance with specifications created by a standards body, and then deployed by user organizations in compliance with a vendor's licensing agreement. The definition of *compliance* can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation.

What are the five key functions of a Compliance Department?

- To identify the risks that an organisation faces and advise on them (identification)
- To design and implement controls to protect an organisation from those risks (prevention)
- To monitor and report on the effectiveness of those controls in the management of an organisations exposure to risks (monitoring and detection)
- To resolve compliance difficulties as they occur (resolution)
- To advise the business on rules and controls (advisory)

IT compliance guidelines vary by country; HIPAA, SOX, GLBA ,FISMA for example, is a U.S. legislation.

Compliance is a prevalent business concern, partly because of an ever-increasing number of regulations that require companies to be vigilant about maintaining a full understanding of their regulatory compliance requirements. Some prominent regulations, standards and legislation with which organizations may need to be in compliance include:

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. Covered entities (anyone providing treatment, payment, and operations in healthcare) and business associates (anyone who has access to patient information and provides support in treatment, payment, or operations) must meet HIPAA Compliance. Other entities, such as subcontractors and any other related 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 health data created, received, maintained or transmitted electronically, also known as electronic protected health information (ePHI).

According to the U.S. Department of Health and Human Services (HHS), the HIPAA Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. Additionally, the Security Rule establishes a national set of security standards for protecting specific health information that is held or transferred in electronic form.

The Security Rule operationalizes the Privacy Rule's protections by addressing the technical and nontechnical safeguards that covered entities must put in place to secure individuals' electronic PHI (e-PHI). Within HHS, the Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

THE NEED FOR HIPAA COMPLIANCE

HHS points out that as health care providers and other entities dealing with PHI move to computerized operations, including computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems, HIPAA compliance is more important than ever. Similarly, health plans provide access to claims as well as care management and self-service

applications. While all of these electronic methods provide increased efficiency and mobility, they also drastically increase the security risks facing healthcare data.

The Security Rule is in place to protect the privacy of individuals' health information, while at the same time allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. The Security Rule, by design, is flexible enough to allow a covered entity to implement policies, procedures, and technologies that are suited to the entity's size, organizational structure, and risks to patients' and consumers' e-PHI.

PHYSICAL AND TECHNICAL SAFEGUARDS, POLICIES, AND HIPAA COMPLIANCE

The HHS requires physical and technical safeguards for organizations hosting sensitive patient data. These physical safeguards include…

Limited facility access and control with authorized access in place

Policies about use and access to workstations and electronic media

Restrictions for transferring, removing, disposing, and re-using electronic media and ePHI

Along the same lines, the technical safeguards of HIPAA require access control allowing only for authorized personnel to access ePHI. Access control includes…

Using unique user IDS, emergency access procedures, automatic log off, and encryption and decryption

Audit reports or tracking logs that record activity on hardware and software

Other technical policies for HIPAA compliance need to cover integrity controls, or measures put in place to confirm that ePHI is not altered or destroyed. IT disaster recovery and offsite backup are key components that ensure that electronic media errors and failures are quickly remedied so that patient health information is recovered accurately and intact. One final technical safeguard is network, or transmission security that ensures HIPAA compliant hosts protect against unauthorized access to ePHI. This safeguard addresses all methods of data transmission, including email, internet, or private networks, such as a private cloud.

To help ensure HIPAA compliance, the U.S. government passed a supplemental act, The Health Information Technology for Economic and Clinical Health (HITECH) Act, which raises penalties for health organizations that violate HIPAA Privacy and Security Rules. The HITECH Act was put into place due to the development of health technology and the increased use, storage, and transmission of electronic health information.

DATA PROTECTION FOR HEALTHCARE ORGANIZATIONS AND MEETING HIPAA COMPLIANCE

The need for data security has grown with the increase in the use and sharing of electronic patient data. Today, high-quality care requires healthcare organizations to meet this accelerated demand for data while complying with HIPAA regulations and protecting PHI. Having a data protection strategy in place allows healthcare organizations to:

Ensure the security and availability of PHI to maintain the trust of practitioners and patients

Meet HIPAA and HITECH regulations for access, audit, integrity controls, data transmission, and device security

Maintain greater visibility and control of sensitive data throughout the organization

The best data protection solutions recognize and protect patient data in all forms, including structured and unstructured data, emails, documents, and scans, while allowing healthcare providers to share data securely to ensure the best possible patient care. Patients entrust their data to healthcare organizations, and it is the duty of these organizations to take care of their protected health information.

SOX

A DEFINITION OF SOX COMPLIANCE

In 2002, the United States Congress passed the **Sarbanes-Oxley Act** (SOX) to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of corporate disclosures. The act sets deadlines for compliance and publishes rules on requirements. Congressmen Paul Sarbanes and Michael Oxley drafted the act with the goal of improving corporate governance and accountability, in light of the financial scandals that occurred at Enron, WorldCom, and Tyco, among others.

All public companies now must comply with SOX, both on the financial side and on the IT side. The way in which IT departments store corporate electronic records changed as a result of SOX. While the act does not specify how a business should store records or establish a set of business practices, it does define which records should be stored and the length of time for the storage. To comply with SOX, corporations must save all business records, including electronic records and electronic messages, for "not less than five years." Consequences for noncompliance include fines or imprisonment, or both.

THREE MANAGEMENT OF ELECTRONIC RECORDS RULES

As a result of SOX, IT departments are responsible for creating and maintaining an archive of corporate records. They seek ways in which to do this that are both cost effective and that are in complete compliance with the requirements of the legislation. Three rules in Section 802 of SOX affect the management of electronic records.

- First rule: This rule concerns the destruction, alteration, or falsification of records and the resulting penalties.
- Second rule: A rule that defines the retention period for records storage; best practices suggest corporations securely store all business records using the same guidelines as public accountants.

- Third rule: This rule outlines the type of business records that need to be stored, including all business records, communications, and electronic communications.

SOX COMPLIANCE AND SECURITY CONTROLS

The best plan of action for SOX compliance is to have the correct security controls in place to ensure that financial data is accurate and protected against loss. Developing best practices and relying on the appropriate tools helps businesses automate SOX compliance and reduce SOX management costs.

Data classification tools are commonly used to aid in addressing compliance challenges by automatically spotting and classifying data as soon as it is created and applying persistent classification tags to the data. Solutions that are context aware have the ability to classify and tag electronic health records, cardholder and other financial data, confidential design documents, social security numbers, PHI, PII, and other structured and unstructured data that is regulated.

SECTION 906 OF THE SOX ACT

Section 906 of the SOX Act requires a written statement to be submitted by the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO). This statement is to be submitted with a periodic report, also required by the Act. The content of the written statement, according to section 906 "shall certify that the periodic report containing the financial statements fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer."

It's paragraph "(c)" in section 906 where penalties for violations are recorded. These penalties are for either;

1. Knowingly certifying a report that does not "comport" with the requirement of section 906
2. Willfully certifying a report that does not "comport" with the requirement of section 906

The fine for a knowing violation will be "not more" than $1,000,000 or imprisoned "not more" than 10 years in prison, or both. A willful violation is significantly more costly at "not more" than $5,000,000 or 20 years in prison, or both.

DATA PROTECTION AND COMPLIANCE

Data classification enables security teams to more easily monitor and enforce corporate policies for data handling. Depending on the sensitivity of data and its applicable regulations, it may need to be encrypted, compressed, or saved to a different file format. With the correct policies in place, corporations can prevent unauthorized users, even those with administrative rights to the system, from viewing regulated data. The best solutions also **prevent data egress** through copying to removable storage devices. Another feature of security solutions that are worth the investment is its ability to safeguard shared data. These so-called “masking” features give users access to necessary information while ensuring compliance with regulations.

COMPLIANCE AND AUDITS

Being in SOX compliance and complying with other regulatory standards is nearly impossible without the correct security solutions in place. Providing evidence of compliance is even worse because evidence must prove written controls are in place, communicated, and enforced while supporting non repudiation. The correct security software solution provides the supportable evidence so that all of your compliance efforts are worthwhile.

A software solution for meeting compliance requirements should be able to monitor data, enforce policies, and log every user action. With evidentiary-quality trails, all of the data needed for compliance is in place. Protect your data and your business with a software solution that ensures SOX compliance and rest a little easier during your next audit.

GLBA

A DEFINTION OF GLBA COMPLIANCE

The Gramm-Leach-Bliley Act (GLB Act or GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

The primary data protection implications of the GLBA are outlined its Safeguards Rule, with additional privacy and security requirements issued by the FTC's Privacy of Consumer Financial Information Rule (Privacy Rule), created under the GLBA to drive implementation of GLBA requirements. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

BENEFITS OF GLBA COMPLIANCE

Complying with the GLBA puts financial institutions at lower risk of penalties or reputational damage caused by unauthorized sharing or loss of private customer data. There are also several privacy and security benefits required by the GLBA Safeguards Rule for customers, some of which include:

Private information must be secured against unauthorized access.

Customers must be notified of private information sharing between financial institutions and third parties and have the ability to opt out of private information sharing.

User activity must be tracked, including any attempts to access protected records.

Compliance with the GLBA protects consumer and customer records and will therefore help to build and strengthen consumer reliability and trust. Customers gain assurance that their information will be

kept secure by the institution; safety and security cultivate customer loyalty, resulting in a boost in reputation, repeat business, and other benefits for financial institutions.

HOW GLBA COMPLIANCE WORKS

The GLBA requires that financial institutions act to ensure the confidentiality and security of customers' "nonpublic personal information," or NPI. Nonpublic personal information includes Social Security numbers, credit and income histories, credit and bank card account numbers, phone numbers, addresses, names, and any other personal customer information received by a financial institution that is not public. The Safeguards Rule states that financial institutions must create a written information security plan describing the program to protect their customers' information. The information security plan must be tailored specifically to the institution's size, operations, and complexity, as well as the sensitivity of the customers' information. According to the Safeguards Rule, covered financial institutions must:

Designate one or more employees to coordinate its information security program;

Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;

Design and implement a safeguards program, and regularly monitor and test it;

Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and

Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

In order to achieve GLBA compliance, the Safeguards Rule requires that financial institutions pay special attention to employee management and training, information systems, and security management in their information security plans and implementation.

POTENTIAL GLBA PENALTIES

Once a GLBA non-compliance allegation is proven, the punishment can have business-altering, and even life-altering, ramifications.

Some non-compliance penalties include:

● Financial institutions found in violation face fines of $100,000 for each violation.

● Individuals in charge found in violation face fines of $10,000 for each violation.

● Individuals found in violation can be put in prison for up to 5 years.

EXAMPLES OF NON-COMPLIANCE ALLEGATIONS

Since the Act has went into effect, there have been several allegations, including:

Paypal (operating as Venmo) allegedly violated both the Federal Trade Act and the GLBA. According to one source, “The FTC also asserts that the privacy practices it alleges violate the GLBA and its Privacy Rule, and that the security failures it alleges violate the GLBA and the Safeguarding Rule.”

Early in the Act’s existence, the FTC invoked the GLBA against several mortgage companies for a number of violations.

BEST PRACTICES FOR GLBA COMPLIANCE

The main focus of the GLBA is to expand and tighten consumer data privacy safeguards and restrictions. The primary concern, related to the GLBA, of IT professionals and financial institutions is to secure and ensure the confidentiality of customers’ private and financial information. Maintaining GLBA compliance is critical for any financial institution, as violations can be both costly and detrimental to continued operations. However, by taking steps to safeguard NPI and comply with the GLBA, organizations will not only benefit from improved security and the avoidance of penalties, but also from increased customer trust and loyalty.

What is ISO compliance?

While ISO certification provides independent validation of a company's conformity to a set of standards created by the International Organization for Standardization (ISO), the certification process can be long. Thus, many organizations prefer to focus on being ISO compliant rather than ISO certified.

ISO compliance means adhering to the requirements of ISO standards without the formalized certification and recertification process. For example, organizations may choose to follow guidelines for establishing a quality management system as outlined in ISO 9001. Unlike ISO 9001 certification which requires a series of audits, ISO compliance focuses on using the standards as a way to make decisions regarding policies, procedures, and processes so that they align with the specifications.

A company can obtain a certificate of compliance that provides customers and business partners with assurance but lacks the time-consuming and costliness of the certification audit. For example, organizations can meet the requirements of the ISO 9000 management standard and obtain the certificate of compliance. This certificate can be used to prove that the appropriate organizational structures exist to promote improvement.

ISO Compliance, Certification and Accreditation explained

The International Organisation for Standardisation (ISO) produces thousands of standards every year covering multiple topics and disciplines. A certain group of those standards known as management system standards are designed to support organisations in delivering products and services which are higher in quality, safer, more secure, more resilient, and environmentally friendly.

These standards are well known such as ISO 9001 (Quality Management), ISO 27001 (Information Security), ISO 14001 (Environmental), ISO 22301 (Business Continuity) and the soon to be launched ISO 45001 (Health and Safety).

Some organisations are required to implement these standards and some other to demonstrate their compliance to them. Within the industry there is a lot of "noise" about compliance, certification and accreditation, and the difference between these terms. So what do they actually indicate in reality?

Compliance

Any organisation can choose to implement a management system standard and use the standard to drive improvement and manage risk. They can choose to meet the requirements and perform internal audits as part of their overall management system. When an organisation implements such standards there are no mandatory requirements (demanded by the standards themselves) to undergo an external audit. Essentially any organisation can implement the standard and claim to be compliant.

Customers of such organisations may ask that their suppliers meet certain standards and in some cases suppliers may simply state that they are compliant however some customers may go one step further and ask for evidence or choose to audit their supplier. For organisations with multiple customers, this could certainly be a large burden having to handle multiple customer audits through the year. This costs time, resources, and often coinage to produce the same evidence time after time.

FISMA

DEFINITION OF FISMA COMPLIANCE

The Federal Information Security Management Act (FISMA) is a United States federal law passed in 2002 that made it a requirement for federal agencies to develop, document, and implement an information security and protection program. FISMA is part of the larger E-Government Act of 2002 introduced to improve the management of electronic government services and processes.

FISMA is one of the most important regulations for federal data security standards and guidelines. It was introduced to reduce the security risk to federal information and data while managing federal spending on information security. To achieve these aims, FISMA established a set of guidelines and security standards that federal agencies have to meet. The scope of FISMA has since increased to include state agencies administering federal programs like Medicare. FISMA requirements also apply to any private businesses that are involved in a contractual relationship with the government.

In April 2010 the Office of Management and Budget (OMB) released guidelines which require agencies to provide real time system information to FISMA auditors, enabling continuous monitoring of FISMA-regulated information systems.

FISMA COMPLIANCE REQUIREMENTS

The National Institute of Standards and Technology (NIST) plays an important role in the FISMA Implementation Project launched in January 2003, which produced the key security standards and guidelines required by FISMA. These publications include FIPS 199, FIPS 200, and the NIST 800 series.

The top FISMA requirements include:

Information System Inventory: Every federal agency or contractor working with the government must keep an inventory of all the information systems utilized within the organization. In addition, the organization must identify the integrations between these information systems and other systems within their network.

Risk Categorization: Organizations must categorize their information and information systems in order of risk to ensure that sensitive information and the systems that use it are given the highest level of security. FIPS 199 “Standards for Security Categorization of Federal Information and Information Systems” defines a range of risk levels within which organizations can place their various information systems.

System Security Plan: FISMA requires agencies to create a security plan which is regularly maintained and kept up to date. The plan should cover things like the security controls implemented within the organization, security policies, and a timetable for the introduction of further controls.

Security Controls: NIST SP 800-53 outlines an extensive catalog of suggested security controls for FISMA compliance. FISMA does not require an agency to implement every single control; instead, they are instructed to implement the controls that are relevant to their organization and systems. Once the appropriate controls are selected and the security requirements have been satisfied, the organizations must document the selected controls in their system security plan.

Risk Assessments: Risk assessments are a key element of FISMA's information security requirements. NIST SP 800-30 offers some guidance on how agencies should conduct risk assessments. According to the NIST guidelines, risk assessments should be three-tiered to identify security risks at the organizational level, the business process level, and the information system level.

Certification and Accreditation: FISMA requires program officials and agency heads to conduct annual security reviews to ensure risks are kept to a minimum level. Agencies can achieve FISMA Certification and Accreditation (C&A) through a four-phased process which includes initiation and planning, certification, accreditation, and continuous monitoring.

THE BENEFITS OF FISMA COMPLIANCE

FISMA compliance has increased the security of sensitive federal information. Continuous monitoring for FISMA compliance provides agencies with the information they need to maintain a high level of security and eliminate vulnerabilities in a timely and cost-effective manner.

Companies operating in the private sector – particularly those who do business with federal agencies – can also benefit by maintaining FISMA compliance. This can give private companies an advantage when trying to add new business from federal agencies, and by meeting FISMA compliance requirements companies can ensure that they're covering many of the security best practices outlined in FISMA's requirements.

PENALTIES FOR FISMA NON-COMPLIANCE

For those government agencies or associated private companies that fail to comply with FISMA there are a range of potential penalties including censure by congress, a reduction in federal funding, and reputational damage.

FISMA COMPLIANCE BEST PRACTICES

Obtaining FISMA compliance doesn't need to be a difficult process. The following are some best practices to help your organization meet all applicable FISMA requirements. While this list is not exhaustive, it will certainly get you on the way to achieving FISMA compliance.

Classify information as it is created: Classifying data based on its sensitivity upon creation helps you prioritize security controls and policies to apply the highest level of protection to your most sensitive information.

Automatically encrypt sensitive data: This should be a given for sensitive information. Ideally, you should arm your team with a tool that can encrypt sensitive data based on its classification level or when it is put at risk.

Maintain written evidence of FISMA compliance: Stay on top of FISMA audits by maintaining detailed records of the steps you've taken to achieve FISMA compliance.

PCI

What is PCI Compliance

Payment card industry (PCI) compliance refers to the technical and operational standards that businesses must follow to ensure that credit card data provided by cardholders is protected. PCI compliance is enforced by the PCI Standards Council, and all businesses that store, process or transmit credit card data electronically are required to follow the compliance guidelines.

The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment, and store, process and transmit cardholder data, you need to host your data securely with a PCI compliant hosting provider.

BREAKING DOWN PCI Compliance

Payment card industry (PCI) compliance standards require merchants and other businesses to handle credit card information in a secure manner that helps reduce the likelihood that cardholders would have sensitive financial data stolen. If merchants do not handle credit card information properly, the card information could be hacked and used to make fraudulent purchases. Additionally, sensitive information about the cardholder could be used in identity fraud.

Being PCI compliant means consistently adhering to a set of guidelines set forth by companies that issue credit cards. The guidelines outline a series of steps that credit card processors must continually follow. Companies are first asked to assess their information technology infrastructure, business processes and credit card handling procedures to help identify potential threats that may compromise credit card data. Companies are then asked to address any gaps in security, and to avoid storing sensitive cardholder information, such as social security and driver's-license numbers, whenever possible. Companies are required to provide compliance reports to the card brands that they work with, such as American Express and VISA.

All companies that process credit card information are required to maintain PCI compliance, regardless of their size or the number of credit card transactions they process. All companies are broken into merchant levels based upon the number of transactions that are processed during a specified period.

PCI compliance is governed by the Payment Card Industry Security Standards Council, an organization formed in 2006 for the purpose of managing the security of credit cards. The requirements, known as the Payment Card Industry Data Security Standards (PCI DSS), are managed by the major credit card companies, including VISA, American Express, Discover and MasterCard, among others.

Read below for an excerpt about what is PCI compliance:

- **Goal: Building and maintaining a secure network**

Install and maintain a firewall configuration to protect cardholder data. Companies must create their own firewall configuration policy and develop a configuration test procedure designed to protect cardholder data. Your hosting provider should have firewalls in place to protect and create a secure, private network.

Do not use vendor-supplied defaults for system passwords and other security parameters. This means creating, maintaining and updating your system passwords with unique and secure passwords created by your company, not ones that a software vendor might already have in place when purchased.

- **Goal: Protect Cardholder Data**

Protect stored data. This requirement only applies to companies that store cardholder data. Specifically, companies that do not automatically store cardholder data are already avoiding a possible data security breach often targeted by identity theft. A PCI compliant hosting provider should provide multiple layers of defense and a secure data protection model that combines physical and virtual security methods. Virtual security includes authorization, authentication, passwords, etc. Physical includes restricted access and server, storage and networking cabinet locks, according to Computerworld.com.

Encrypt transmission of cardholder data across open, public networks. Encrypted data is unreadable and unusable to a system intruder without the property cryptographic keys, according the PCI Security Standards Council. Cryptographic keys refers to the process in which plaintext, like the words seen here, are transformed into ciphertext. Ciphertext contains information unreadable to those without the cipher, or the specific algorithm that can decode the text.As an added security measure, sensitive

authentication data, including card validation codes or PIN numbers, must never be stored after authorization – even if this data is encrypted.

- **Goal: Maintain a Vulnerability Management Program.**

Use and regularly update anti-virus software. An anti-virus software service needs to be frequently updated to protect against the most recently developed malware. If your data is being hosted on outsourced servers, a managed server provider is responsible for maintaining a safe environment, including generating audit logs.

Develop and maintain secure systems and applications. This includes discovering newly identified security vulnerabilities via alert systems. Your PCI compliant hosting provider should be monitoring and updating their systems to accommodate any security vulnerabilities.

- **Goal: Implement Strong Access Control Measures**

Restrict access to cardholder data by business need-to-know. Limiting the number of personnel that have access to cardholder data will lessen the chances of a security breach.

Assign a unique ID to each person with computer access. User accounts with access should follow best practices, including password encryption, authorization, authentication, password updates every 30 days, log-in time limits, etc.

Restrict physical access to cardholder data. If your data is hosted in an off-site data center, your data center provider should have limited personnel with access to the sensitive information. PCI compliant data centers should have full monitoring, including surveillance cameras and entry authentication to ensure a secure and PCI compliant hosting environment.

- **Goal: Implement Strong Access Control Measures**

Track and monitor all access to network resources and cardholder data. Logging systems that track user activity and stored archives can help your hosting provider pinpoint the cause in the event of a security breach or other issue.

Regularly test security systems and processes. With regular monitoring and testing processes in place, your data hosting provider should be able to assure you that your customers' cardholder data is safe at all times.

- **Goal: Maintain an Information Security Policy**

Maintain a policy that addresses information security. This policy should include all acceptable uses of technology, reviews and annual processes for risk analysis, operational security procedures, and other general administrative tasks.

If you are choosing a data hosting provider, ask for documentation of the processes that ensure the 12 PCI compliance requirements can be met.

Looking for a PCI compliant provider? Otava can help. Our cloud solutions meet every requirement of PCI compliance and independent annual audits find our data centers are 100 percent compliant against PCI compliance. Get started with your disaster recovery, cloud or colocation solution today.

NERC

The NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

The NERC CIP plan consists of 9 standards and 45 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

CIP-002-1: Critical Cyber Asset Identification

CIP-003-1: Security Management Controls

CIP-004-1: Personnel and Training

CIP-005-1: Electronic Security Perimeters

CIP-006-1: Physical Security of Critical Cyber Assets

CIP-007-1: Systems Security Management

CIP-008-1: Incident Reporting and Response Planning

CIP-009-1: Recovery Plans for Critical Cyber Assets

The CIP program coordinates all of NERC's efforts to improve the North American power system's security. These efforts include standards development, compliance enforcement, assessments of risk and preparedness, the dissemination of critical information and raised awareness regarding key security issues. NERC's standards for governing critical infrastructure apply to entities that "materially impact" the reliability of the bulk power system. These entities include owners, operators and users of any portion of the system.

Under NERC CIP, covered entities are required to identify critical assets and to regularly perform a risk analysis of those assets. Policies for monitoring and changing the configuration of critical assets need to be defined, as do policies governing access to those assets. In addition, NERC CIP requires the use of firewalls to block vulnerable ports and the implementation of cyber attack monitoring tools. Organizations are also required to enforce IT controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyber attacks, natural disasters and other unplanned events.

Penalties for non-compliance with NERC CIP can include fines, sanctions or other actions against covered entities. Because NERC is a trans-national organization, the exact penalties vary from country to country.

The Legal and Regulatory department provides support to several of NERC’s key program areas: Compliance Operations, Investigations, and Standards. In addition, this department provides a wide range of legal support to the NERC management team regarding antitrust, corporate, commercial, insurance, contract, employment, real estate, copyright, tax, legislation, and other legal matters.