UNIT V

SECURITY ASSESSMENT

Information Security Compliance Monitoring

Cybersecurity compliance policies are critical documents that set the standard for security-based activities and behaviors, such as the encryption of emails, management of passwords, and rules surrounding the use of social media.

As the number of cybersecurity attacks increases, organizations tend to enforce cyber security by creating more stringent regulations. And, with the new industry requirements affecting all industries, cyber security compliance has become the driving force of underlying success.

Therefore to prepare for the changing organizational needs, companies need to create a security-first approach to stay safe and ahead of the evolving requirements.

What is Cyber Security Compliance? With Examples

Cyber security compliance is all about ensuring that the companies adhere to all the important regulatory requirements and follow the national and state-level cyber laws to protect sensitive information. In simple terms, cybersecurity compliance is the risk management method that is aligned with some pre-defined security measures and controls data confidentiality.

Organizations have to implement the systematic risk governance approach that combines with the respective authorities, industry-relevant units, and laws to meet the data management requirements.

An information security management system that adheres to the regulatory requirements to guide companies about the precautionary measures that should be followed to minimize the possibility of a breach.

Additionally, IT security compliance help in monitoring and accessing the process of devices, systems, and networks that adheres to the regulatory compliance requirements.

Why Do You Need Cybersecurity Compliance?

Cyber security and data leakages can have a huge impact on organizations; for this, the protection quality of cyber security defines the level of safety of businesses. Businesses should adhere to cyber security rules and requirements or teach their employees about the **best Ethical Hacking** certification.

This compliance not only helps businesses in sticking to regulations but also allows for security management services. Here are a few other reasons why you need cybersecurity compliance:

1. Regulatory penalties avoidance

The organizations could face serious fines and penalties for not complying with the security regulations. Establishing cyber security plans regarding regulations minimizes the possibility of having a breach.

2. Risk management system

Cyber security compliance is a risk management system that allows data protection, activity monitoring, the safety of network infrastructure, and security policies for authorization. These security regulations provide a set of requirements for collecting, storing, managing, and sharing sensitive data.

Types of Data Subject to Cybersecurity Compliance

Cyber security and data protection laws mainly focus on protecting sensitive data like protected health information (PHI), personally identifiable information (PII), and financial information.

1. Personally Identifiable Information

When used, personally identifiable information helps identify an individual's relevant data. It may include direct identifiers that help identify the person's unique identity, race, and other factors. Try **KnowledgeHut's cyber security training courses online** to learn about personally identifiable information.

Takeaways:

- PII used data to identify the individual's identity
- The PII includes full name, driver's license, financial information, and medical records.
- Non-sensitive personal information is easily accessible from public sources like gender, code, zip code, and date of birth.

2. Personal Health Information (PHI)

Personal health information includes the data that is used to identify someone's details regarding their treatment or health history:

- Record of information
- Medical record
- Information about medical appointments
- Prescription records
- Insurance records

3. Financial Data

Financial Data includes information about credit card numbers, payment methods, and other details that could steal someone's identity. Sensitive data includes:

- Social security numbers
- Credit card number
- Bank account number
- Credit history and credit ratings

Some other sensitive data are subject to state, industry regulations, and regional include:

- Email addresses, passwords, usernames
- IP Addresses
- Authenticators include biometrics like voice prints, facial recognition data, and fingerprints.
- Race
- Religion

Significance of Cybersecurity Compliance

It is important to know that cyber security compliance is not just a collection of mandatory requirements. Instead, it defines the consequences that define the overall success of your business.

This compliance is, however, important for small enterprises that are the prime victim of cyber criminals. Let's have a look at the **2020 Data Breach investigation report**:

- Around 45% of breaches were because of hacking
- 22% of breaches include Social engineering
- 28% include small businesses
- 70% were outsiders

Cybersecurity Compliance Framework

Let's have a look at the cybersecurity compliance framework:

1. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce 2014. Ideally designed for the private organizations of the United States, the NIST framework is one of the biggest cyber security frameworks applied to all organizations looking for a cyber security program. It works around five functions, called:

- Protect
- Detect
- Identify
- Respond
- Recover

2. COBIT

Control Objective for Information and Related Technologies is a cyber security framework created by the ISACA for IT management and governance. It's a highly processed-oriented framework, COBIT's create links between businesses and IT goals to distribute responsibilities to IT and businesses. COBIT follows the five processes

- Evaluate, Direct, and Monitor (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service, and Support (DSS)
- Monitor, Evaluate, and Assess (MEA)

COBIT is also designed to cater to three objectives, viz. increased agility, increased earning potential, and legal compliance

3. IASME Governance

Created by the Information Assurance of Small and Medium Enterprise (IASME) Consortium, this governance was made to become an affordable and accessible alternative to the ISO/IEC 27001 standard.

IASME is unique because it's a partnership between British academics and Small/Medium enterprises (SMEs) and is made to fulfill the needs of cyber security needs of small businesses.

The IASME also covers risk management, malware protection, vulnerability scanning, incident management, risk management, firewalls, business continuity, and more.

4. TC Cyber

The technical Committee cyber division is one of the many technical groups that operate under the European Telecommunications Standards Institute (ETSI). This activity focuses on cyber security and compliance strategy security that has led the organization to work on different aspects with different sets of standards. The ETSI is split into nine areas:

- Protection of personal data and communications
- Cybersecurity tools
- EU legislative support
- Forensic
- Quantum-safe cryptography
- Enterprise cybersecurity

5. COSO

COSO means Committee of Sponsoring Organizations of the Treadway Commission. It's another cybersecurity framework that is more holistic and targeted toward removing corporate fraud. As COSO is all about auditing and accounting bodies, the COSO framework is built on the process of 'internal control' that relates to risk management.

COSO contains five interrelated components:

- Risk assessment
- Control activities
- Information and communication
- Monitoring
- Control environment

6. CISQ

Consortium for IT Software Quality (CISQ) is a joint endeavor between the Object Management Group (OMG) and Carnegie Mellon University's Software Engineering Institute (SEI). The CISQ's international standards help automate software quality measurement, and the division of reliable, secure, and trustworthy software is built around these areas:

- Structure Quality
- Technical Debt
- Software Size

7. TC Cyber

The technical Committee cyber division is one of the technical groups that operate under the European Telecommunications Standards Institute. This activity is used to support the development and testing of standards for ICT-enable systems.

ETSI TC Cyber has led to companies working on different security aspects with different

standards. The TC Cyber security work is divided into these areas:

- Enterprise/individual cybersecurity
- Cybersecurity tools
- EU legislative support
- Forensics
- Quantum-safe Cryptography
- Protection of personal data and communication

8. FedRAMP

Federal Risk and Authorization Management Program (FedRAMP) is a set of standardized approaches that helps in security assessment, monitoring, and authorization for cloud products and services. Introduced by the U.S. government, it is used by all departments and agencies.

Additionally, FedRAMP uses the NIST SP-800 and Cloud service providers (CSPs) to ensure that companies must undertake the Federal Information Security Management Act (FISMA).

How to Create Cybersecurity Compliance Program

Here are the steps that you must keep in mind to ensure you are given a handsome security compliance analyst salary for their work:

Step 1: Create a compliance Team

A compliance team is important for all types of businesses, and it doesn't exist in a vacuum. As organizations are moving toward critical operations to the cloud, they need to create an independent workflow and communicate across business and IT departments.

- Set Controls:
- Depending on the risk tolerance, you need to know how to transfer the risk. The set controls include:
- Encryption
- Firewall
- Password Policies
- Vendor Risk Management Program
- Insurance
- Employee Training

Step 2: Establish a Risk Analysis Process

As more standards and regulations focus on taking a risk-based approach to comply with organizations of all sizes to get into the risk analysis process. Here's the process that comes along:

1. Identifying the risk: Identifying all information assets and information systems, networks, and data they access.

2. Assess Risk: Review each level of data type and identify how risk information is stored, collected, and transmitted.
3. Analyze risk: After accessing risk, you need to analyze the risk. For this, the companies need the following formula:
4. Risk = (Likelihood of Breach x Impact)/Cost
5. Set Risk Tolerance: After analyzing the risk, you should determine whether to refuse, accept, transfer or mitigate the risk.
6. Set Up Policies: Policies help document compliance activities and controls. These policies are the foundation of necessary internal and external audits.

Step 3: Monitor and Respond

Most of the compliance requirements depend on how the threats are involved. Cybercriminals continuously work to identify ways to get into the breach. They identify vulnerabilities called Zero-Day Attacks and modify their strategies to work accordingly. Continuous monitoring of the policies and procedures helps identify threats before they lead to data breaches.

Major Cyber Security Compliance Requirements

Various information security regulation requirements establish cybersecurity compliance standards. While there are different methods, their target content combines with each other to deliver a similar goal. So, create rules that are easy and simple to follow and adapt as per the company's technological environment.

Some of the major cybersecurity compliance solutions and requirements are:

1. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a U.s Federal statute that was signed in 1996. It includes health-related information that complies with HIPAA privacy standards to process claims, share information and receive payments.

This cybersecurity compliance management ensures that Health Care Plan's and health care clearinghouses and other businesses associated with this won't disclose any private and confidential data without someone's consent.

The act is based on three fundamental parts Security rules, Breach notification, and Privacy Rules for reporting an accident. This law isn't applied to companies that are not present in the U.S.

2. FISMA

The Federal Information Security Management Act controls the federal U.S. system to protect

economic interest information, assets, and operations from the risk of breach. The FISMA displays minimum requirements for security maintenance and threat prevention in the national-level agency system. This act stick with the active laws and cyber security directives to address the compliance and procedures within the information security programs.

Additionally, it covers the information system security plan and controls, conducts risk assessment, and ensures continuous monitoring.

3. PCI-DSS

The payment card industry data security standard is a non-federal information security requirement that implements credit card data protection and security controls. The main goal of PCI-DSS is to protect the cardholder from any breach.

The PCI-DSS standard is applied to merchants that handle payment information irrespective of handling the transactions that happen per month. Non-compliant entities often risk losing their merchant license and may become a potential threat to cyber attacks.

4. GDPR

The General Data Protection Regulation (GDPR) is a data protection and privacy law that was published in 2016 and covers the European Economic Area and European Union Countries. It built a legal framework that guides EU-based employees' personal data protection and collection.

GDPR allows companies to show clear policies and conditions regarding their customer data collection policies and allow individuals to manage their data without restrictions.

5. ISO/IEC 27001

ISO/IEC 27001 is an international standard for implementing and managing the information security management system that belongs to the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) 27000 family of standards.

Businesses signify the adherence to compliance at all technological levels, including processes, tools, employees, and systems, to ensure integrity and protection.

6. Avoid Regulatory Fines

Conducting sufficient practices that stick to the regulatory requirements helps to prevent the regulatory penalties that happen during the breach. Also, in case of misconduct, regulatory compliance cyber security companies investigate it, resulting in huge fines.

However, it sometimes sends a message to other companies that they need to protect their data under all circumstances.

7. Risk Assessment Instrument

Important compliance obligations combine the collection of rules and regulations that helps review the most important system and procedure required for securing and managing sensitive data.

Establishing clear guidelines from cybersecurity compliance regulations or knowing about the rules from **cyber security training courses online** helps in risk assessment and targeting the vulnerabilities to focus on the important things required in the cybersecurity framework.

8. Industry Standard

Aligning security policies among other businesses helps IT professionals set a cyber security check standard, avoid misinterpretations, and overlay complicated operations among other companies.

The aligned procedure and the related framework for cybersecurity compliance certification can be treated as a risk prevention measure for customers that don't have to research the company's security standards. Also, unified policies are more secure and allow simplified and optimized b2b and b2c transactions.

How to Implement Cybersecurity Compliance?

To simplify cybersecurity compliance, we have deconstructed everything into simple steps. So, let's see how you can build a cybersecurity compliance plan with these easy steps:

1. Get a compliance team

Whether you are a big company or a small one, you must have a dedicated person with skills and knowledge in accessing cyber security compliance. The ownership and responsibility help in maintaining and updating the cyber security environment and creating a tough plan toward threats and challenges.

2. Establish a Risk analysis process

Establish and review an analysis process to see where the organization is going and what needs to be done. Break the process into:

- Identification: Helps distinguish assets, information systems, and networks they use to access.
- Analysis: Helps determine the risk impact; you can use this formula:
- Risk= Likelihood of breach x impact/ cost

Setting the risk tolerance: Categorizing and prioritizing the risk by transferring, accepting, and refusing or eliminating the risk.

3. Set security control

You must work on the security measures that your organization will handle the risk. Some of the controls contain:

- Network firewall
- Password Policies
- Data encryption
- Network access control
- Employee training
- Incident response plan
- Insurance

4. Policies and procedures

Documenting the security-oriented operations will help to have clear instructions about cyber security regulatory compliance programs. It helps align things systematically and revise and audit the network security compliance of the company.

5. Monitor and respond

Actively monitoring the security methods, improvements, and other measures helps identify new risks and respond by updating the required changes.

Cyber Security Compliance Best Practices

Compliance and security are interconnected, but compliance aims to keep up with government policies, industry regulations, security frameworks, and clients' contractual terms. Here are some of the best practices you must follow to keep with security compliance:

- Know your industry IT security regulatory complaint
- Develop a risk assessment plan
- Identify risks and vulnerabilities to establish the security controls
- Keep reviewing your compliance practices

Benefits of Cyber Security Compliance

A) Avoid penalties and fines

Not fulfilling the latest rules and regulations governing their business can be expensive for businesses that are not in compliance. Therefore as a cybersecurity compliance company, you should be aware of the latest trends and legislations to avoid fines and penalties.

B) Build customer trust and brand reputation

Business threats are not just limited to business interruptions and financial losses but are also damaging to the brand reputation and customer trust. Therefore, at the time of a data breach, an instant response is important to protect brand reputation and customer loyalty.

C) Improved data management

Companies must keep track of the sensitive information they have about their customers and where the data is stored. How do they handle, modify and access that information in a secure and streamlined manner?

D) Enhanced security

The compliance regulations allow businesses to build a cyber-security program, create organization-level cyber-security policies, and designate chief information security officers.

This will also minimize the risk, and you will be able to address the data breach.

E) Improved access control and accountability

Businesses should develop accountability for creating strategic management of security and cyber risk that comply with the cyber security regulations. Organizations should use a suitable risk management framework to regulate and monitor the security system and the client's sensitive information.

ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY
PALKULAM, KANYAKUMARI
OBSERVE OPTIMIZE OUTSPREAD