Dr. D. Y. Patil Pratishthan’s

Institute for AdvancedComputing &Software Development

IACSD

Compliance Audit

INDEX

What Is a Compliance Audit?

A compliance audit is an independent evaluation to ensure that an organization is following external laws, rules, and regulations or internal guidelines, such as corporate bylaws, controls, and policies and procedures. Compliance audits may also determine if an organization is conforming to an agreement, such as when an entity accepts government or other funding Depending on the circumstances, the audit may be conducted by an employee, such as an internal auditor, a certified public accountant, a third-party auditor, or a government auditor. In many circumstances, auditors may seek the expert advice of outside specialists, such as lawyers.

Essentially, a compliance audit asks if you are doing what you said you would do.

What Cyber security Challenges do Organizations Face?

Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cybercrimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today’s technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

CYBER CRIME

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day-by-day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances.

Compliance Basics

Compliance is the 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.

Types of Security Audits:

There are many different types of security audits. Each audit has its own goal and objective. Some audits are even especially relevant for a certain business model and might not be needed for your company. However, there are some types of IT audits that are relevant for all businesses and companies. Here are the four main security audits that every business should be conducting on a regular basis:

1. Risk Assessment:

As indicated by the name, the purpose of risk assessment security auditing is to identify the different types of risk that a business might be prone to. It is an undeniable fact that no matter what your business is, it will always be prone to some risks. And you cannot be prepared to face the risks or avoid them if you are not even aware about them in the first place. Therefore, risk assessment audits are extremely important as they help businesses identify their weaknesses and vulnerabilities so that the businesses can come with effective strategies to tackle them.

2. Vulnerability Assessment:

Just like the risk assessment helps businesses identify possible risks, the purpose of the vulnerability assessment is to showcase the areas of the business's security that are vulnerable and can be exploited to do harm to the business. During the vulnerability audit, the security audit companies indicate the aspects of the business that are weak and thus can be used to cause significant harm to the business.

The business's vulnerability keeps changing as the business grows and flourishes. Therefore, vulnerability assessment is a type of security audit that should be repeated on a regular basis so that the business owners are truly in touch with the weak links of their businesses and can plan the proper strategies to cover up and conceal these weaknesses to prevent any sort of exploitation.

3. Penetration Testing:

One of the major cyber security issues that businesses always have to face include hacking attempts. This is where penetration testing comes in. Penetration testing is a form of data security audit in which one of the auditors acts as a hacker and attempts to bypass the company's security system. The hacker may use different hacking methodologies and attempt different techniques to highlight the areas of the business that require a security upgrade. This helps businesses gather data which can then be used to strengthen the business's security system and ensure that the business is strong and can withstand any unauthorized attacks.

Penetration testing can be further divided into internal penetration testing and external penetration testing. In case of internal penetration testing, the business's internal security fortress is put to the test whereas the external penetration testing checks the business's overall security protocols. There is no way to label one of these penetration tests as better than the other and businesses should always opt for a hybrid approach where the auditors perform both internal as well as external penetration testing so that a comprehensive analysis of the company's security infrastructure and its reliability can be drawn.

4. Compliance Audit:

Almost all businesses have to abide by a certain set of rules and regulations. This compliance is necessary for the business's legal status. The set of the compliance rules is quite extensive and it also keeps changing and updating depending on the overall circumstances of the economy and the business community.

Although it is necessary to abide by these regulations, it is nearly impossible for a business to figure out whether it meets all the rules or not. This is where IT security audit companies come in. The company will go through the rules and regulations and confirm whether your business follows them all or not. The company will also indicate any changes that the business has to acknowledge. This takes a lot of load off of the business's shoulder as the compliance audit can be extensive and tedious. But when the experts handle this matter, the results are reliable and the businesses can be assured and have a peace of mind that they are headed in the right direction.

Security Audit Phases

A cyber security audit consists of five steps:

1. Define the objectives.
2. Plan the audit.
3. Perform the auditing work.
4. Report the results.
5. Take necessary action.

1. Define the Objectives

Lay out the goals that the auditing team aims to achieve by conducting the IT security audit. Make sure to clarify the business value of each objective so that specific goals of the audit align with the larger goals of your company.

Use this list of questions as a starting point for brainstorming and refining your own list of objectives for the audit.

- Which systems and services do you want to test and evaluate?
- Do you want to audit your digital IT infrastructure, your physical equipment and facilities, or both?
- Is disaster recovery on your list of concerns? What specific risks are involved?
- Does the audit need to be geared towards proving compliance with a particular regulation?

2. Plan the Audit

A thoughtful and well-organized plan is crucial to success in an IT security audit.

You’ll want to define the roles and responsibilities of the management team and the IT system administrators assigned to perform the auditing tasks, as well as the schedule and methodology for the process. Identify any monitoring, reporting and data classification tools that the team will use and any logistical issues they may face, like taking equipment offline for evaluation.

Once you’ve decided on all the details, document and circulate the plan to ensure that all staff members have a common understanding of the process before the audit begins.

3. Perform the Auditing Work

The auditing team should conduct the audit according to the plan and methodologies agreed upon during the planning phase. This will typically include running scans on IT resources like file-sharing services, database servers and SaaS applications like Office 365 to assess network security, data access levels, user access rights and other system configurations. It’s also a good idea to physically inspect the data centre for resilience to fires, floods and power surges as part of a disaster recovery evaluation.

During this process, interview employees outside the IT team to assess their knowledge of security concerns and adherence to company security policy, so any holes in your company’s security procedures can be addressed moving forward. Be sure to document all findings uncovered during the audit.

4. Report the Results

Compile all your audit-related documentation into a formal report that can be given to management stakeholders or the regulatory agency. The report should include a list of any security risks and vulnerabilities detected in your systems, as well as actions that IT staff recommend taking to mitigate them.

5. Take Necessary Action

Finally, follow through with the recommendations outlined in your audit report. Examples of security-enhancement actions can include:

- Performing remediation procedures to fix a specific security flaw or weak spot.
- Training employees in data security compliance and security awareness.
- Adopting additional best practices for handling sensitive data and recognizing signs of malware and phishing attacks.
- Acquiring new technologies to harden existing systems and regularly monitor your infrastructure for security risk

Principal of Audit

The basic principles of auditing are confidentiality, integrity, objectivity, and independence, skills and competence, work performed by others, documentation, planning, audit evidence, accounting system and internal control, and audit reporting.

Auditor personal abilities

- They show integrity
- They are effective communicators
- They are good with technology
- They are good at building collaborative relationships
- They are always learning
- They leverage data analytics
- They are innovative
- They are team orientated

Security evaluation

The examination of a system to determine its degree of compliance with a stated security model, security standard, or specification. The evaluation may be conducted

(a) by analysing the detailed design, especially of the software, often using verification and validation

(b) by observing the functional behaviour of the system, or

(c) by attempting to penetrate the system using techniques available to an “attacker”.

Security Evaluation phases

The three phases necessary for a security evaluation plan are preparation, security evaluation, and conclusion.

National Institute of Standards and Technology (NIST) Overview

The National Institute of Standards and Technology promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST carries out its mission through the following programs:

- the NIST Laboratories, conducting world-class research, often in close collaboration with industry, that advances the nation's technology infrastructure and helps U.S. companies continually improve products and services;

- the Hollings Manufacturing Extension Partnership, a nationwide network of local centres offering technical and business assistance to smaller manufacturers to help them create and retain jobs, increase profits, and save time and money; and
- the Baldrige Performance Excellence Program, which promotes performance excellence among U.S. manufacturers, service companies, educational institutions, health care providers, and non-profit organizations; conducts outreach programs; and manages the annual Malcolm Baldrige National Quality Award, which recognizes performance excellence and quality achievement.

Components of framework

NIST Cybersecurity Framework consists of 3 parts. These parts must work jointly to assist organizations to build a comprehensive cybersecurity strategy.

1. Framework core

The first framework component of the NIST Cybersecurity Framework is framework core. The framework core mostly contains guidance information and cybersecurity activities. In other words, it presents industry standards in a way that helps organizations tackle cyber risks.

2. Implementation tiers

The implementation tier framework component serves as a way for the organization to evaluate its current cybersecurity posture. Simply put, NIST cybersecurity framework implementation tiers help organizations assess what level of standards are best for their cybersecurity program.

3. Profiles

Finally, the framework profile component enables your organization to develop a blueprint for minimizing the cyber risks that are aligned with organizational goals. Organizations may focus on more than one profile to detect weak spots as well as opportunities for improving cybersecurity posture.

General Data Protection Regulation (GDPR) Overview

GDPR can be considered as the world's strongest set of data protection rules, which enhance how people can access information about them and places limits on what organisations can do with personal data. The full text of GDPR is an unwieldy beast, which contains 99 individual articles.

The regulation exists as a framework for laws across the continent and replaced the previous 1995 data protection directive. The GDPR's final form came about after more than four years of discussion and negotiations – it was adopted by both the European Parliament and European Council in April 2016. The underpinning regulation and directive were published at the end of that month.

GDPR came into force on May 25, 2018. Countries within Europe were given the ability to make their own small changes to suit their own needs. Within the UK this flexibility led to the creation of the Data Protection Act (2018), which superseded the previous 1998 Data Protection Act.

The strength of GDPR has seen it lauded as a progressive approach to how people's personal data should be handled and comparisons have been made with the subsequent California Consumer Privacy Act.

Key Steps to Ensure GDPR Compliance

Indian companies that handle 'personal data' of EU residents are required to comply with GDPR. The companies dealing with data of EU residents are needed to restructure their privacy policies and contractual arrangements with EU companies and those organizations that provide data of EU residents. Here are certain key GDPR provisions which must be fulfilled by companies which are dealing with said data:

Lawful and Legitimate Purpose: Processing of personal information is to be undertaken in compliance with the following principles:

a. Processing should be done lawfully and with full transparency. For lawful processing, at least one of the requirements under GDPR must be met, such as where the Data Subject has given consent to data processing; or processing is necessary for the execution of a contract to which the Data Subject is a party; or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority etc.

b. Personal Data should be collected for specified legitimate and explicit purposes and not further processed if incompatible with those purposes (except where specifically permitted under GDPR), and it should be adequate, accurate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Consent must be obtained: Where processing is based on consent, obtaining of consent should be specific, informed and unambiguous. This compliance can be done by providing checkbox when visiting an internet website such as obtaining consent for cookies, but silence, pre-ticked checkboxes or any inactivity would not constitute consent. If the processing has multiple purposes, then the consent should be given for all of them. If the consent is given in the context of a written declaration concerning other matters, the consent request should be provided separately from other content, in an intelligible and easily accessible form, using clear and plain language.

Data Minimalization: GDPR supports the data minimalization principle, requiring companies to only use and keep the personal data that is needed at any time for the required purpose. If it’s not needed for that intended purpose and duration, it should be removed from the database of the company. The people who have consented to data can withdraw their consent any time and can ask to the company to delete their data. Companies must then remove all data related to that person from its database, as well as any other database such as archives or anywhere downstream where the data may have been shared and stored.

Special Categories of Personal Data: There are extra requirements that are to be complied with while processing of special categories of personal data. Personal data is subject to much more care as any breach of such data would make the privacy of such people vulnerable. Processing of personal data relating to criminal convictions and offenses and processing which does not require identification.

Information to be provided to Data Subject: The controller at the time of obtaining the personal data has to provide the Data Subject with all the required information such as contact details and identity and contact details of the data protection officer (only required in some cases), purposes and legal basis of processing, existence of the data subject's rights such as right to access, recipients or categories of recipients of the personal data, period of storage of personal data, rectification or erasure of personal data, right to withdraw consent, the right to lodge a complaint with a supervisory authority, right to data portability etc. Information on similar lines is also to be provided to the data subject (where personal data has not been obtained from the data subject) under Article 14 of GDPR, except in certain prescribed circumstances which enumerate following rights of data subjects:

The right of access: Right to obtain from the controller confirmation regarding the processing of their personal data, and also access to their personal data and information.

Right to rectification: Right to obtain from the controller rectification of inaccurate personal data, also they have a right to have incomplete personal data completed.

Right to get their data removed: Right to obtain from the controller erasure of personal data and the controller is required to remove personal data where one of the grounds applies such as: (a) the personal data is no longer necessary in relation to the purposes for which it was collected (b) the Data Subject withdraws their consent on which the processing was based (c) the Data Subject objects to the processing and there are no legitimate grounds for the processing, etc.

Right to restriction of processing: Right to obtain from the controller restriction of processing in circumstances(prescribed) such as where the accuracy of the personal data is contested by the data subject; the processing is unlawful etc.

Right to data portability: Right to receive the personal data provided to a controller, in a structured, commonly used and computer/laptop/mobile phone readable format and the right to transmit that data to another controller. This right does not apply to a task carried out in the public interest or in the exercise of official authority by the controller.

International Organization for Standardization (ISO) 2700x

When it comes to keeping information assets secure, organizations can rely on the ISO/IEC 27000 family.

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

How does ISO 27001 work?

ISO 27001 works on a top-down, technology-neutral, risk-based approach. The specification defines six planning processes, which include Defining a security policy, Defining the scope of ISMS, conducting risk assessment, managing assessed risks, picking control objectives that are to be implemented and preparing the statement of applicability. ISO 27001 draws coordination between all sections of an organization and enhances management responsibility, ensures continual improvement, conducts internal audits and undertakes corrective and preventive actions.

History of ISO/IEC 27001

The ***ISO 27001*** standard was published in October 2005, essentially replacing the old BS 7799-2 standard (see Figure 1). 1S0- 27001 is the specification for an Information Security Management System. BS 7799 itself was a standing standard, first published in the 1990s as a code of practice. As it matured, a second part emerged to cover management systems, on the basis, of which certification is granted, that is, it is an auditable standard. Today, more than 1,000 BS 7799 certificates are in place, across the world. ISO 27001 enhanced the content of BS 7799-2 (i.e., Part II of the BS 7799) and harmonized it with the other standards.

A scheme has been introduced by various certification bodies for conversion from BS 7799 certification to ISO 27001 certification.

ISO/IEC 27001:2005 domains

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives;
- use within organizations as a way to ensure that security risks are cost effectively managed;
- use within organizations to ensure compliance with laws and regulations;
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;
- use by the management of organizations to determine the status of information security management activities;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners

and other organizations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organizations to provide relevant information about information security to customers.

SOx Reports

The Sarbanes-Oxley Act of 2002, often simply called SOX or Sarbox, is U.S. law meant to protect investors from fraudulent accounting activities by corporations. Sarbanes-Oxley was enacted after several major accounting scandals in the early 2000's perpetrated by companies such as Enron, Tyco, and WorldCom. So what is SOX? The law mandates strict reforms to improve financial disclosures from corporations and prevent accounting fraud. It also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

The law is named for the two congressmen who drafted it, Paul Sarbanes and Michael Oxley. The U.S. Securities and Exchange Commission (SEC) administers the act.

Though Sarbanes-Oxley does not call out any specific IT requirements, the law does have a great impact on information systems – and in particular the security of those systems – owed to the fact that the financial information covered under the law is processed and stored by IT systems. Section 404 in particular has had very costly implications for publicly-traded companies as it is expensive to establish, maintain, and validate the required internal controls.

SOC Reports - Auditor Process Overview

In a nutshell, a SOC report is issued after a third-party auditor conducts a thorough examination of an organization to verify that they have an effective system of controls related to security, availability, processing integrity, confidentiality, and/or privacy. The report, which is issued by a Certified Public Accountant (CPA), provides reasonable assurance over the design and operating effectiveness of controls and clearly outlines any potential risks for customers or partners that are considering working with the organization.

To understand SOC lingo, there are a few key terms you will want to be familiar with:

- **Service Organization** – the organization that is being tested.
- **User Entity** – the organization that outsources a function to a service organization.
- **Control** – the auditable process or mechanism designed to prevent or detect risk.

Transparency is crucial when it comes to gaining the trust of another organization and its stakeholders, such as vendor compliance, internal audit, IT management, and legal departments. The success or failure of specific controls has a significant impact on the reputation, financial statements, and stability of the service organization.

SOX COMPLIANCE AND SECURITY CONTROLS

What is SOX compliance? While the details of the Sarbanes-Oxley Act are complex, "SOX compliance" refers to the annual audit in which a public company is obligated to provide proof of accurate, data-secured financial reporting.

Basics of SOX Compliance
*****
Keep data secure and free of tampering
Track attempted security breaches and resolutions
Keep event logs available for independent auditing
Prove compliance for past 90 days

To this end, while SOX measures seek to govern the financial operations and disclosures of corporate entities and any of their contracted financial service providers, the regulations pertain to a breadth of departments, and a few to IT.

SOX reporting specifically involves IT departments because adequate SOX internal controls require complete file safety and full visibility into financial record history—conditions which require each IT employee to understand his or her role in demonstrating SOX compliance.

COBIT framework

COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for information technology (IT) management and IT governance.

The COBIT business orientation includes linking business goals with its IT infrastructure by providing various maturity models and metrics that measure the achievement while identifying associated business responsibilities of IT processes. The main focus of COBIT 4.1 was illustrated with a process-based model subdivided into four specific domains, including:

- Planning & Organization
- Delivering and Support
- Acquiring & Implementation
- Monitoring & Evaluating

All of this is further understood under 34 processes as per the specific line of responsibilities. COBIT has a high position in business frameworks and has been recognized under various international standards, including ITIL, CMMI, COSO, PRINCE2, TOGAF, PMBOK, TOGAF, and ISO 27000. COBIT acts as a guideline integrator—merging all solutions under one umbrella.

The latest COBIT version 5 came out in April 2012 and consolidated the principles of COBIT 4.1, Risk IT Frameworks, and Val IT 2.0. This version draws reference from IT Assurance Framework (ITAF) from ISACA and the revered BMIS (Business Model for Information Security).

The Various COBIT Components

Framework

IT helps in organizing the objectives of IT governance and bringing in the best practices in IT processes and domains while linking business requirements.

Process Descriptions

It is a reference model and also acts as a common language for every individual in the organization. The process descriptions include planning, building, running, and monitoring of all IT processes.

Control Objectives

This provides a complete list of requirements that have been considered by the management for effective IT business control.

Maturity Models

Accesses the maturity and the capability of every process while addressing the gaps.

Management Guidelines

Helps in better-assigning responsibilities, measuring performances, agreeing on common objectives, and illustrating better interrelationships with every other process.

Difference between COBIT and ITIL

	COBIT	ITIL
Definition	A set of guidelines for any organization to develop, implement, monitor, and improve technology governance.	A framework for best practices, planning, and selection, geared to improving IT services to better meet the company's needs.
Scope	Focuses on ITSM, but has a broader scope than ITIL, since it studies the entire organization.	Focuses on ITSM, and not on the whole company. It remains within the domain of IT.
Approach	A top-down approach, focusing more on IT service governance.	A bottom-up approach, focusing more on IT service management.
Goals and Objectives	1. Effectively manage the IT department to the company's advantage and set it in the right direction. 2. Align IT goals and business goals. 3. Bring IT values to the business. 4. Manage resources, risks, and IT efficiency.	1. Organize all the IT services within the company and make them run smoothly. 2. Create opportunities for constant operational perfection. 3. Reduce the company's IT costs without sacrificing effectiveness. 4. Improve the decision-making within the company.
The Big Question	"How do I best leverage my IT department's resources for the benefit of the company?"	"How do I organize my IT teams and their workload in the most efficient way?"

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.

Covered Entities

The following types of individuals and organizations are subject to the Privacy Rule and considered covered entities:

- **Healthcare providers**: Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule.
- **Health plans*:*** Entities that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers; health

maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans.

Exception: A group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.

- **Healthcare clearinghouses*:*** Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.
- **Business associates*:*** A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing.

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- Disclosure to the individual (if the information is required for access or accounting of disclosures, the entity MUST disclose to the individual)
- Treatment, payment, and healthcare operations
- Opportunity to agree or object to the disclosure of PHI (Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object)
- Incident to an otherwise permitted use and disclosure

- Public interest and benefit activities—The Privacy Rule permits use and disclosure of protected health information, without an individual’s authorization or permission, for 12 national priority purposes external icon:

1. When required by law
2. Public health activities
3. Victims of abuse or neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement
7. Functions (such as identification) concerning deceased persons
8. Cadaveric organ, eye, or tissue donation
9. Research, under certain conditions
10. To prevent or lessen a serious threat to health or safety
11. Essential government functions
12. Workers’ compensation

HIPAA Security Rule

While the HIPAA Privacy Rule safeguards protected health information (PHI), the Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

To comply with the HIPAA Security Rule, all covered entities must do the following:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures
- Certify compliance by their workforce

Covered entities should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures. The HHS Office for Civil Rights enforces HIPAA rules, and all complaints should be reported to that office. HIPAA violations may result in civil monetary or criminal penalties.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

History of PCI-DSS

Five different programs have been started by card companies:

- Visa's Cardholder Information Security Program
- MasterCard's Site Data Protection
- American Express's Data Security Operating Policy
- Discover's Information Security and Compliance
- the JCB's Data Security Program

The intentions of each were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. To cater out the interoperability problems among the existing standards, the combined effort made by the principal credit card organizations resulted in the release of version 1.0 of PCI DSS in December 2004. PCI DSS has been implemented and followed across the globe.

The Payment Card Industry Security Standards Council (PCI SSC) was then formed, and these companies aligned their individual policies to create the PCI DSS.[3] MasterCard, American Express, Visa, JCB International and Discover Financial Services established the PCI SSC in September 2006 as an administration/governing entity which mandates the evolution and development of PCI DSS. Independent/private organizations can participate in PCI development after proper registration. Each participating organization joins a particular SIG (Special Interest Group) and contributes to the activities which are mandated by the SIG. The following versions of the PCI DSS have been made available:

Different Levels of PCI

All companies who are subject to PCI DSS standards must be PCI compliant. However, how they prove and report their compliance is based on how many transactions they process per year and how they process those transactions. The acquirer or payment brands may also choose to manually place an organization into a reporting level at their discretion.[6]

At a high level, the merchant levels are as follows:

- Level 1 – Over 6 million transactions annually
- Level 2 – Between 1 and 6 million transactions annually
- Level 3 – Between 20,000 and 1 million transactions annually (or any e-commerce merchant)
- Level 4 – Less than 20,000 transactions annually

Each card issuer maintains their own table of compliance levels as well as a separate table for service providers.

Centre for Internet Security (CIS) Critical Security Controls

The Centre for Internet Security Critical Security Controls for Effective Cyber Defense is a publication of best practice guidelines for computer security. The project was initiated early in 2008 in response to extreme data losses experienced by organizations in the US defense industrial base.[1] The publication was initially developed by the SANS Institute. Ownership was then transferred to the Council on Cyber Security (CCS) in 2013, and then transferred to Centre for Internet Security (CIS) in 2015. It was originally known as the Consensus Audit Guidelines and it is also known as the CIS CSC, CIS 20, CCS CSC, SANS Top 20 or CAG 20.

CIS Compliance

The Centre for Internet Security (CIS) benchmarks are a set of best-practice cybersecurity standards for a range of IT systems and products. CIS Benchmarks provide the baseline configurations to ensure compliance with industry-agreed cybersecurity standards. The benchmarks are developed by CIS alongside communities of cybersecurity experts within industry and research institutes.

CIS Benchmarks can be seen as frameworks to configure IT services and products. Organizations can use the guidelines to improve cybersecurity and help protect against cyber threats. CIS Benchmarks cover a huge range of products and systems including server software, operating systems and network devices. These systems are widespread in all modern organizations and offices, making CIS Benchmarks a vital tool when it comes to closing vulnerabilities in an IT network.

CIS Benchmarks are free to use and are easily downloaded. They're useful to any stakeholders dealing with an organization's IT governance, cybersecurity policies and systems. The Center for Internet Security also offers a membership option which enhances cybersecurity compliance monitoring and resources. CIS Benchmarks are also important to IT system vendors, who can gain certification to show the product reaches CIS compliance.

CIS Benchmarks

CIS Benchmarks are frameworks for calibrating a range of IT services and products to ensure the highest standards of cybersecurity. They're developed through a collaborative process with input from experts within the cybersecurity community. There are more than 100 different benchmarks covering a range of well-known vendors and systems. CIS Benchmarks provide guidance for all areas of an IT network, including operating systems, server systems, office software and network devices.

CIS Benchmarks are free to download and use. The documents cover everything from initial set up to configuration of all parts of the IT system. The guidance is regularly updated and renewed to reflect new iterations of the IT service or product. CIS Benchmarks represent the baseline settings to ensure an IT system or product is secure. The aim is to enhance international cybersecurity standards in all types of organizations. CIS Benchmarks are used by organizations, governments and institutes across the world.

CIS Benchmarks are compatible with existing IT risk management policies and procedure. They can slot into well-known frameworks for IT governance such as the NIST Cybersecurity Framework.

SSE-CMM Project

An alternative approach to evaluating assurance is built on the capability maturity model (CMM) paradigm, which is a five-level model of increasingly mature processes and continuous improvement. The CMM originated in the Carnegie Mellon Software Engineering Institute (SEI) under the auspices of the U.S. Department of Defense (DoD).

The Systems Security Engineering Capability Maturity Model (SSE-CMM; copyright 1999 by the Systems Security Engineering Capability Maturity Model [SSE-CMM] Project) is based on the premise that if you can guarantee the quality of the processes that are used by an organization, then you can guarantee the quality of the products and services generated by those processes. It was developed by a consortium of government and industry experts and is now under the auspices of the International Systems Security Engineering Association (ISSEA) at www.issea.org. The SSE-CMM (www.sse-cmm.org/) makes the following salient points:

- Describes those characteristics of security engineering processes essential to ensure good security engineering
- Captures industry's best practices
- Accepted way of defining practices and improving capability
- Provides measures of growth in capability of applying processes

The SSE-CMM addresses the following areas of security:

- Operations security
- Information security

- Network security
- Physical security
- Personnel security
- Administrative security
- Communications security
- Emanation’s security ...