Introduction

What are the cyber standards?

A cyber security standard is a set of best practices or guidelines that an organization or organizations can use to improve their cyber security posture.

To help individuals identify and implement appropriate measures to protect their data and systems from cyber threats ,organizations tend to use cyber security standards which guide them on how to retrieve data and recover from cyber security incidents.

Cyber standards provide a comprehensive framework for organizations looking to protect their data through best practices and robust policies.

Cyber security requires careful coordination of people, processes, systems ,networks and technology.

What are the proposed cyber Standards?

ISO/IEC 22301

This is an international standard that provides guidelines two organizations to ensure business continuity and to counter all cyber security incidents. ISO 22301 is the right standard for an organization to show their stakeholders how rapidly and organization can overcome in security to enable continuity of their operations.

To ensure an organization delivers what the clients needs, the rigor of a certified management system has spared up the process to ensure delivery of an interrupted services.

According to the ISO survey, ISO 22301 has experienced an 82.9 percentage increase in the worldwide certificates, showing the growth and importance of UKAS accredited certification in the recent times.

What is a business continuity Management system?

This is a recognized framework for ensuring an organization can continue business operations and respond effectively to disruptive events.

What is the purpose of BCMS?

The purpose of BCMS is to ensure that critical business processes keep running in the event of damage or emergencies and continuously develops and improves them.

What are the major components of BCMS?

Management support

Business impact analysis

Risk assessment

Having in place a business continuity plan

NIST CSF (Cyber Security Framework)

The NISD CSF (National Institute of Standards and Technology Security Framework) is an international standard that provides a set of guidelines, best practices and standards for countering cyber security incidents as a voluntary framework.

The framework gives organizations and ability to assess, identify and manage their cybersecurity incidents in a structured manner

The NIST CSF is increasingly being adopted by organizations as a voluntary framework to better their cyber security status although the framework is not mandatory.

What are the elements of the NIST cyber security framework?

Recover- Implement and develop strategies to restore systems and data due to a cyber security

 incident

Detect- Develop and implement detection processes to identify as cyber-security event.

Respond -implement response plans for the known cyber security incidents.

Identify -Develop an organization's baseline security posture and identify risks

Protect -Implement security controls to protect against known risks.

What are the benefits of NIST cyber security framework?

Provides a common language and a set of tools and organization can use to counter cyber security risks.

It can be used to identify and manage cyber security incidents in an organization.

The framework helps organizations to communicate about cyber security risks.

What are the implementations of the NIST cyber security framework?

There are general steps that organizations should take when implementing the framework. This include;

Access your organizations current cyber security capabilities and practices.

Identify important aspects of the framework to organization.

Implement a strategy for the framework

Develop the NIST CSF

Change your implementation of the framework overtime

HIPAA PRIVACY RULE

The health insurance portability and accountability is a united states act of Congress that refers to the creation of national standards to prevent sensitive patient health information from looking without the patient's knowledge.

The HIPAA privacy rule standard is an international standard that uses covered entitles to protect and avoid disclosure of individual's health information subjected to the privacy rule

The privacy rule has standards that allow individuals to understand the management of the information.

The people who seek healing and care are protected by the privacy rule which allows for important usage of information.

What is the key to hipa compliance plan?

HIPAA compliance plan includes:

HIPAA policies to protect patients information

 Risk analysis and management policies all year around

What are the steps towards HIPAA compliance?

Designate a HIPAA privacy and security office

Develop an implement HIPAA policies and procedures

Provide HIPAA training to all staff members

Complete gap and security risk analysis (SRA) to determine the current state of HIPAA compliance.

What are the transcriptions and the code set rule?

The security rule

The HIPAA security Rule support the privacy rule and works only with health information protected by electronics.

The security rule states that covered in titles must:

Comply with the workforce

Identify and prevent reasonable threats to security and integrity of the information.

And should I integrity and confidentiality in EPHI they create, receive and transmit.

The Enforcement rule

The enforcement rule is supplemented by HITECH ACT of 2001. The rule implements procedures for compliance and sets for penalties for violation of the hIPAA rules.

The Unique Identifiers Rule

The unique identifiers rule Monday it's the use of standardized unique codes to identify healthcare organizations, employees and patients.

Regulated identification system enhances efficiency and security in healthcare operations.

HITECH ACT

The Health Information Technology for Economics and Clinical Health act was enacted by the American reinvestment act of 2009.

The HITECH ACT requires business associates to comply with the HIPAA security rule and to report PHI breaches.

ISO/IEC 27001

ISO/IEC 27001 is an international standard that ensures an organization's facets of its ISMS are working effectively. The standard also provides a framework for managing sensitive company information.

What is ISO 27001 certification?

The certification of ISO 27001 states that to protect an organization's data and organization has to invest in people processes and technology.

Through acredited certification body, certification is achieved and it proves to an organization's consumers that the organization is controlling information security according to international best practices.

How does an ISO 27001 audit works?

An ISO 27001 audit involve a competent and objective audition reviewing;

The ISMS on elements of each and testing that it meets the standards requirements

The organization's on information requirements

That the policies, processes and other controls are practical and efficient

What are the five stages of an audit?

Internal audio to conducts assurance audit through a five- phase process which includes:

Selection

Planning

Reporting

What are the ISO 27001 risk management

The ISO 27001 risk management gives a systematic way to evaluate an organization's risk and to understand how it may impact its information, security and implement an action plan against risk incidents.

ISO 27001 create awareness methodology and provides training and resources to help prevent human error that can lead to cyber security threats.

DFARS (Defense Federal Acquisition Regulation Supplement)

The DFARS is a set of cyber security regulations that the department of defense in process on external contractors and suppliers. The regulations include:

Implementing audit and accountability measures to ensure the security of DoD systems and data.

To protect all DoD systems and data from an authorized access

Implement a system of risk assessment and when it meant to identify risks threatening DoD systems and data

Establishing a strategy to respond to cyber attack that could threaten DoD systems or data

Ensure proper training of the contractors with access to DoD systems

What are the DFARS compliance requirements?

Deploy a federal team to inspect the contractor's security plan

Media protection

Incident response

Audit and accountability

Awareness on training

Access control

ISO/IEC 27032

ISO/IEC 27032 is a widely recognized standard that provides guidance on cyber security for organizations and it is designed to help them to protect themselves against cyber threats or risks.

The standard provides guidance for a long-term process preservation and allows organizations to establish a policy framework. It also allows organizations to take measures to protect their customers and other stakeholders.

It brings out different aspects in improving cyber security and its dependencies such as:

Information security

Network security

Internet security

Critical information infrastructure protection

ISO/IEC 27032 is an international standard that cover security practices for stakeholders in the cyberspace. This thunder to provides:

A framework to enable stakeholders to work together and resolving cyber security incidents.

And overview of cyber security.

Guidance for countering common cyber security threats

A description of stakeholders' roles in cybersecurity

ISO/IEC 27031

ISO/IEC27031 is a cyber standard that provides guidance on the concepts on principles behind the role of information and communication technology in ensuring business continuity

Achieving compliance with ISO 27031 gives organizations and understanding of the threats to ICT services ensuring safety in the event of an unplanned incident

What are the benefits of ISO 27031?

ISO 27031 helps an organization to understand the threats to ICT services which helps it to fight against such vulnerabilities to ensure safety in an unplanned incident.

It helps organizations ensure that their business continuity plans are able to deal with any type of disaster.

The standard also help organizations to implement their crisis recovery plans consistently

This standard safeguards assets, turnovers and profits hence during a disaster it minimizes the impact of the income, asset and reduces the risk of further losses.

ISO/IEC 27000 SERIES

This is an information security framework developed by international organization for standardization that can be used by all organizations whichever their size or strengt

Through audit andbcertification processes ISO 27000 is established. The standard consists of an overview and it defines lSMS requirement programs.

The ISO 27000 has a standard that cover a wide area of information security incidents.

What are the benefits of the ISO IEC 27000?

Reduce human error

Follow risk-based approach

Mitigate security threats and cyber attacks

Meet additional regulatory requirements

Delete the human factor in data breeches

The ISO IEC 27000 has information management security which combines to provide a globally recognized framework for best practices in information security management

ISO/IEC 27701

ISO/IEC 27701 outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy.Based on the requirements of ISO IEC 27701, the standard specifies the requirements of PIMS (privacy information management system)

The ISO 27701 ensures all your facets of your ISMS are working effectively. ISO defines the ISO 27701 as a standard that provides organizations with guidance for implementing, establishing,maintaining and improving the information security management system.

 ISO/IEC 27701 is a data privacy extension to ISO 27001. It assists organizations to establish systems to support compliance with the European Union General Data Protection Regulation (GDPR) and other data privacy requirements but as a global standard it is not GDPR specific.maintaining and improving the information security management system.

What are the benefits of ISO 27701?

ISO 27001 can benefit an organization by preventing a serious data breaching

This standard evolves as a better security evolved hence an organization can easily adapt to whatever the changes are.

What are the requirements of the implementation of ISO 27701?

The standard requires an existing management system to attach to. Only a few closes at applicable. The requirements of the standard are as below:

An organization should design, build and implement a personal information system

Follow the ISO 27701 guidelines when designing and implementing the PIMS.

Conclusion

 Practical measures are taken to ensure the protection of people, corporations, and societies against threats and adversaries is guaranteed and I also gives individual and organizations to help themselves during cyber security attacks or risks.

Organizations must have strong cybersecurity measures to protect their data and customersCyber security policies refer to the policies companies put in place to protect their digital systems. This is in the form of a statement that employees accept upon joining the company.

More companies use online systems, such as eCommerce stores and mailing lists that communicate offers to their customers..Cybersecurity is critical because it helps to protect organizations and individuals from cyber attacks. Cybersecurity can help to prevent data breaches, identity theft, and other types of cybercrime.

Cybersecurity is essential for protecting our digital assets, including sensitive personal and financial information, intellectual property, and critical infrastructure. Cyberattacks can have serious consequences, including financial loss, reputational damage, and even physical harm.

References

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.itgovernanceusa.com/cybersecurity-standards&ved=2ahUKEwjY38rf9bOBAxWthP0HHZJFDwcQFnoECBEQAQ&usg=AOvVaw1uSms\_0v0RN6qkzcOZLBP-