Discipline

Information on Standard Compliance

CS5002

Activity-10

Sheikh Muhammed Tadeeb (AU19B1014)

❖ Problem Statement:

Give information about Compliance standard like

1. HIPA
2. PCI-DSS
3. FIPS
4. SOC1,2,3

and its use industry or domain.

❖ Solution:

1. HIPA:

- **Brief:**

  HIPAA stands for 'Health Insurance Portability and Accountability Act'. It is focused on protection of privacy of individually identifiable health information and gives patients an array of rights with respect to that information. It is applicable on Covered Entities (CE) and Business Associates (BA) which are generating, accessing, processing and transmitting PHI. HIPAA is a legal requirement, governed by the US government.

- **Uses:**

  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:

  1. Disclosure to the individual (if the information is required for access or accounting of disclosures, the entity MUST disclose to the individual).

  2. Treatment, payment, and healthcare operations.

3. 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).

4. Incident to an otherwise permitted use and disclosure.

5. Public interest and benefit activities.

2. PCI-DSS:

- **Brief:**

Payment Card Industry Data Security Standard is one of the most granular and specific standards aiming towards securing credit and debit card related information. It applies to all entities involved in payment card processing including merchants' processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmits cardholder data (CHD) and/or sensitive authentication data (SAD). PCI DSS is Industry regulation enforced by payment brands and has set 6 goals, broken into 12 requirements and more than 300 sub-requirements to be implemented within the cardholder data environment.

- **Uses:**

1. Build and Maintain a Secure Network and Systems.
2. Protect Cardholder Data.
3. Maintain a Vulnerability Management Program.
4. Implement Strong Access Control Measures.
5. Regularly Monitor and Test Networks.
6. Maintain an Information Security Policy.

3. FIPS (Federal Information Processing Standard):

- **Brief:**

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information. It requires use of FIPS 140 2 validated cryptographic modules when accessing AWS US East/West, AWS GovCloud (US), or AWS Canada (Central) through use of the command line interface (CLI) or programmatically by using the APIs, the following sections provide the list of available FIPS endpoints by AWS Region. The Amazon Virtual Private Cloud VPN endpoints in AWS GovCloud (US) operate using FIPS 140-2 validated cryptographic modules. all AWS FIPS endpoints have been updated to only accept a minimum of Transport Layer Security (TLS) 1.2 connections.

- **Uses:**

1. FIPS are applied to the potential use case and align with the government data's perceived value. The complying, or regulated party, then, must adhere to standards used to handle government information. As the secrecy and sensitivity of government data rises from classified to (top) secret, the severity of the FIPS standard rises as it is applied to the persons, practices, and technologies in place to hold and transmit the data.

2. Among FIPS standards are ones that cover data encryption such as the Advanced Encryption Standard (AES), which is a FIPS standard.

4. SOC (System and Organization Controls):

- **Brief:**

AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance.

- *AWS SOC 1 (Formerly SSAE 16/ISAE 3402):*

The AWS SOC 1 report focuses on AWS's processes and controls relevant to our customers' financial reporting. Many AWS customers use the AWS SOC 1 as an integral part of their Sarbanes-Oxley efforts and other security and compliance initiatives where key controls operated by AWS are evaluated and validated.

- *AWS SOC 2 – Security & Availability:*

The AWS SOC 2 report focuses on the security and availability controls, as defined by the American Institute of Certified Public Accountants (AICPA) Security Trust Principles, operated by AWS. This report is leveraged by a wide range of AWS customers, including but not limited to customers in the technology, healthcare, banking, and financial services industries. This report is leveraged to meet a wide range of security control and compliance requirements based on the AICPA's mature industry control criteria.

- *AWS SOC 3 – Security & Availability:*

The SOC 3 report is a public report. It is a summarized version of the SOC 2 report and enables you to validate that AWS has completed a favourable independent audit against the AICPA's Security Trust Principles.

- **Uses:**

1. Security

   Firewalls, Intrusion detection, multi-factor authentication

2. Availability

   Performance monitoring, Disaster recovery, Incident handling

3. Confidentiality

   Encryption, Access controls, Firewalls

4. Processing Integrity

   Quality assurance, Process monitoring

5. Privacy

   Access Control, Multi-factor authentication, Encryption