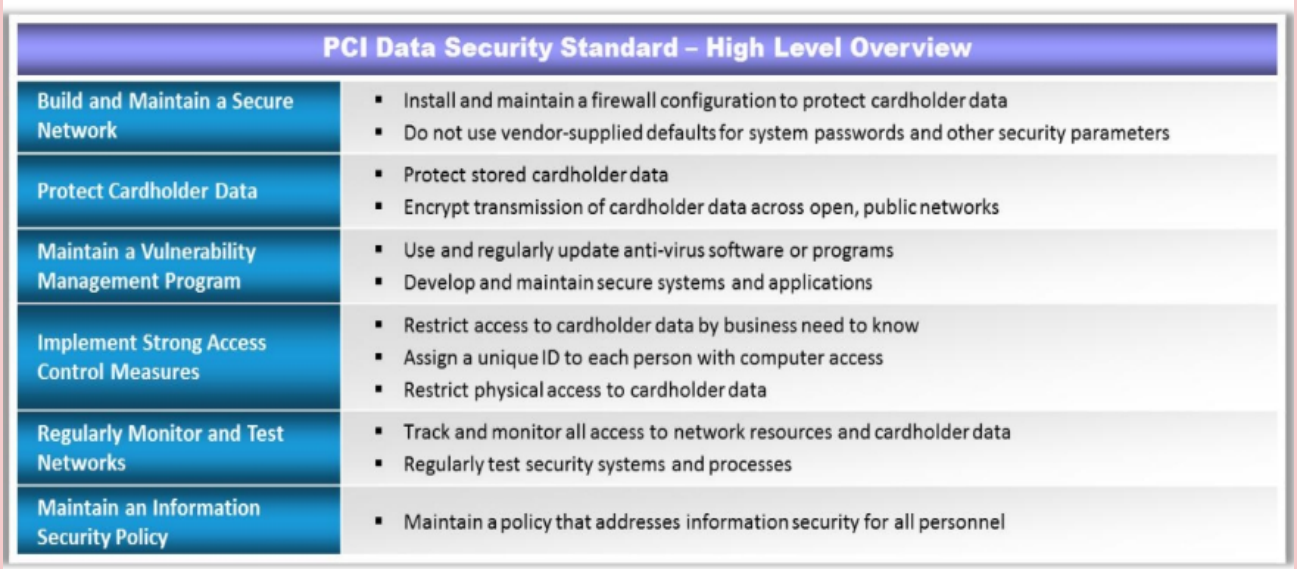
Information Security Laws and Standards-

1. Payment Card Industry Data Security Standard (PCI DSS)-

PCI DSS is a set of security standards that organizations must follow to protect cardholder data from unauthorized access, use, disclosure, disposal, modification, or destruction. It is mandatory for all organizations that handle cardholder information, and failure to comply can result in fines, penalties, and other sanctions.
Here are the key points:

- *PCI DSS is a global standard.*
- *PCI DSS is a living document and is updated regularly.*
- *There are different levels of PCI DSS compliance.*
- *There are resources available to help organizations comply with PCI DSS.*



PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

2. ISO/IEC 27001:2013-

ISO/IEC 27001, also known as Information Security Management Systems (ISMS), is an international standard that provides a framework for establishing, implementing, operating, monitoring,

reviewing, maintaining, and improving an organization's information security management system (ISMS).

- *Improved security posture: The standard helps organizations identify and address security risks, which can help to prevent security breaches.*
- *Increased compliance: The standard can help organizations comply with other security regulations, such as PCI DSS and HIPAA.*
- *Enhanced reputation: Demonstrating compliance with ISO/IEC 27001 can help to improve an organization's reputation and attract new customers.*
- *Reduced costs: Implementing the standard can help to reduce the costs of security breaches and downtime.*

3. Health Insurance Portability and Accountability Act (HIPAA)-

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that sets standards for the protection of health information. The law applies to healthcare providers, health plans, and other entities that transmit, store, or handle health information.

- *Portability: To ensure that individuals can keep their health insurance when they change jobs or lose their coverage.*
- *Accountability: To hold healthcare providers and health plans accountable for protecting health information.*
- *Privacy: To give individuals control over their health information.*

The rule requires healthcare providers and health plans to obtain written consent from individuals before using their health information for most purposes.

4. Sarbanes Oxley Act (SOX)-

The Sarbanes-Oxley Act of 2002 (SOX) is a federal law that was enacted in the United States in response to a number of corporate

accounting scandals, including the Enron and WorldCom scandals. The law is designed to protect investors by improving the accuracy and reliability of corporate financial reporting.

Title I of the Sarbanes-Oxley Act (SOX) establishes the Public Company Accounting Oversight Board (PCAOB), which oversees auditing firms that audit public companies. It sets up a central board to register audit services, define audit procedures, inspect and regulate audit quality, and enforce SOX requirements.

Title II of the Sarbanes-Oxley Act aims to keep external auditors unbiased. It sets rules for their independence, including how they're approved, when they rotate partners, and what they report. It also stops auditing firms from doing other, non-audit work for the companies they audit.

Title III of the Sarbanes-Oxley Act focuses on corporate responsibility. It requires top executives to personally ensure that financial reports are accurate and complete. It also outlines how external auditors should work with corporate audit committees. The title sets clear rules for corporate officers, outlines penalties for non-compliance, and specifies the consequences for violating these rules.

Title IV of the Sarbanes-Oxley Act focuses on enhancing financial disclosures. It includes measures to provide more detailed and transparent financial information by companies. This helps stakeholders better understand a company's financial performance, risks, and position.

Title V of the Sarbanes-Oxley Act is about addressing conflicts of interest among securities analysts. It sets a code of conduct for these analysts and mandates that they must disclose any conflicts of interest they are aware of. The goal is to rebuild trust in the reports and recommendations made by securities analysts to protect the interests of investors.

Title VI of the Sarbanes-Oxley Act has four sections. It aims to boost investor trust in securities analysts. It outlines the SEC's authority to

punish or disqualify securities professionals and sets conditions for disqualifying someone from working as a broker, advisor, or dealer. This title helps maintain the integrity of financial markets and protect investors.

Title VII of the Sarbanes-Oxley Act mandates studies and reports by the Comptroller General and the SEC. They investigate issues like accounting firm mergers, credit rating agencies' role, securities violations, enforcement actions, and whether investment banks helped companies manipulate earnings. This helps maintain transparency and accountability in financial markets.

Title VIII - "Corporate and Criminal Fraud Accountability Act of 2002": It outlines penalties for manipulating, destroying, or altering financial records and for obstructing investigations. It also protects whistle-blowers.

Title IX - "White Collar Crime Penalty Enhancement Act of 2002": This title increases penalties for white-collar crimes, enhances sentencing guidelines, and makes failing to certify corporate financial reports a criminal offense.

Title X - "Corporate Tax Returns": It requires the CEO to sign the company's tax return.

Title XI - "Corporate Fraud Accountability Act of 2002": This title makes corporate fraud and records tampering criminal offenses with specific penalties. It revises sentencing guidelines and allows the SEC to temporarily freeze large or unusual transactions.

5. The Digital Millennium Copyright Act (DCMA)-

The DMCA is a US law that enforces international copyright treaties. It makes it illegal to bypass copyright protection technologies or remove copyright information from works, protecting the rights of copyright owners.

Title I: Implements international copyright treaties by creating rules against the circumvention of technological measures protecting copyrighted works and tampering with copyright information.

Title II: Addresses copyright infringement liability online, offering protection for online service providers in cases of transitory communications, system caching, user-directed storage, and information location tools. It also includes special rules for nonprofit educational institutions.

Title III: Allows owners or lessees of computer programs to make copies when needed for computer maintenance or repair.

Title IV: Contains various provisions, including clarifying the Copyright Office's authority, granting exemptions for ephemeral recordings, promoting distance education, exempting nonprofit libraries and archives, addressing webcasting amendments, and ensuring residual payments for writers, directors, and screen actors when producers can't make the payments.

Title V of the DMCA is known as the Vessel Hull Design Protection Act (VHDPA). It introduces a system for safeguarding the unique designs of specific practical items that enhance their visual appeal or distinctiveness. In this context, "useful articles" refer to the hulls (including decks) of vessels that are no more than 200 feet in length.

6. The Federal Information Security Management Act:

The Federal Information Security Management Act of 2002 (FISMA) is a law that sets out important security standards and guidelines required by Congress. FISMA establishes a comprehensive framework to ensure the effectiveness of security controls over information resources supporting federal operations and assets. It mandates federal agencies to create a security program covering all information and information systems that play a role in agency operations and assets, even if managed by other agencies or external parties. The FISMA framework includes standards for categorizing information and systems based on their mission impact, minimum security

requirements, guidance for choosing security controls, guidance for evaluating their effectiveness, and guidance for authorizing system security.

7. General Data Protection Regulation:

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Here are some of the key provisions of the GDPR:

- *Right to be informed: Individuals have the right to be informed about how their personal data is being collected and used.*
- *Right of access: Individuals have the right to access their personal data.*
- *Right to rectification: Individuals have the right to have their personal data rectified if it is inaccurate.*
- *Right to erasure: Individuals have the right to have their personal data erased in certain circumstances.*
- *Right to restrict processing: Individuals have the right to restrict the processing of their personal data in certain circumstances.*
- *Right to data portability: Individuals have the right to receive their personal data in a structured, commonly used and machine-readable format, and to have it transmitted to another controller.*
- *Right to object: Individuals have the right to object to the processing of their personal data in certain circumstances.*
- *Automated decision-making: Individuals have the right not to be subject to a decision based solely on automated processing, unless certain conditions are met.*

The GDPR places a number of obligations on organizations that collect and use personal data. These obligations include:

- *Lawfulness of processing: Organizations must have a lawful basis for processing personal data.*
- *Data minimization: Organizations should only collect and use personal data that is necessary for the purpose for which it is being collected.*
- *Storage limitation: Personal data should not be stored for longer than is necessary.*
- *Integrity and confidentiality: Personal data must be kept secure and confidential.*
- *Accountability: Organizations must be able to demonstrate that they comply with the GDPR.*

8. Data Protection Act 2018 (DPA)-

Data Processing Agreements (DPAs) are legal contracts between organizations that outline how personal data will be handled when it is shared between them. DPAs are essential for ensuring that personal data is protected in accordance with data privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union (EU).

- *Enhanced Data Protection: DPAs ensure that personal data is handled in a compliant and secure manner, reducing the risk of data breaches and regulatory fines.*
- *Clearer Roles and Responsibilities: DPAs clearly define the roles and responsibilities of the data controller and data processor, minimizing confusion and potential conflicts.*
- *Increased Transparency: DPAs provide transparency regarding how personal data is being processed, which helps build trust with individuals whose data is being collected and used.*
- *Streamlined Compliance: DPAs help organizations demonstrate compliance with data privacy laws, facilitating audits and regulatory reviews.*