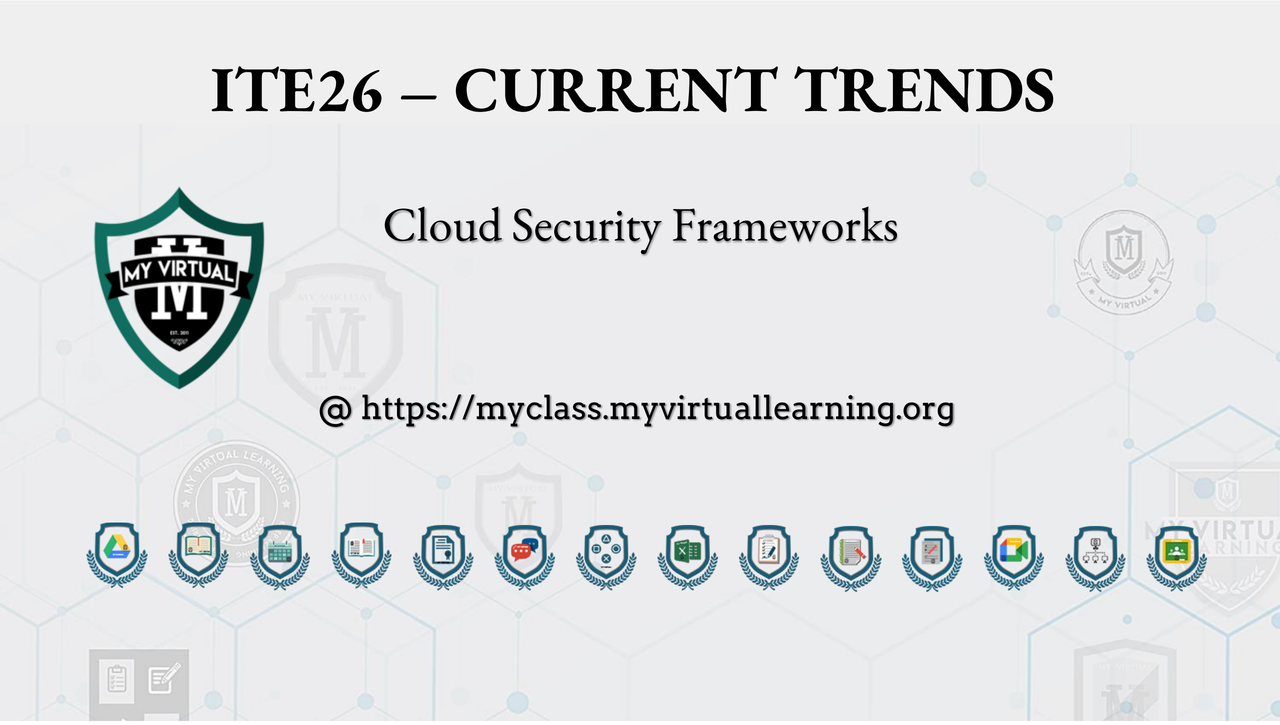


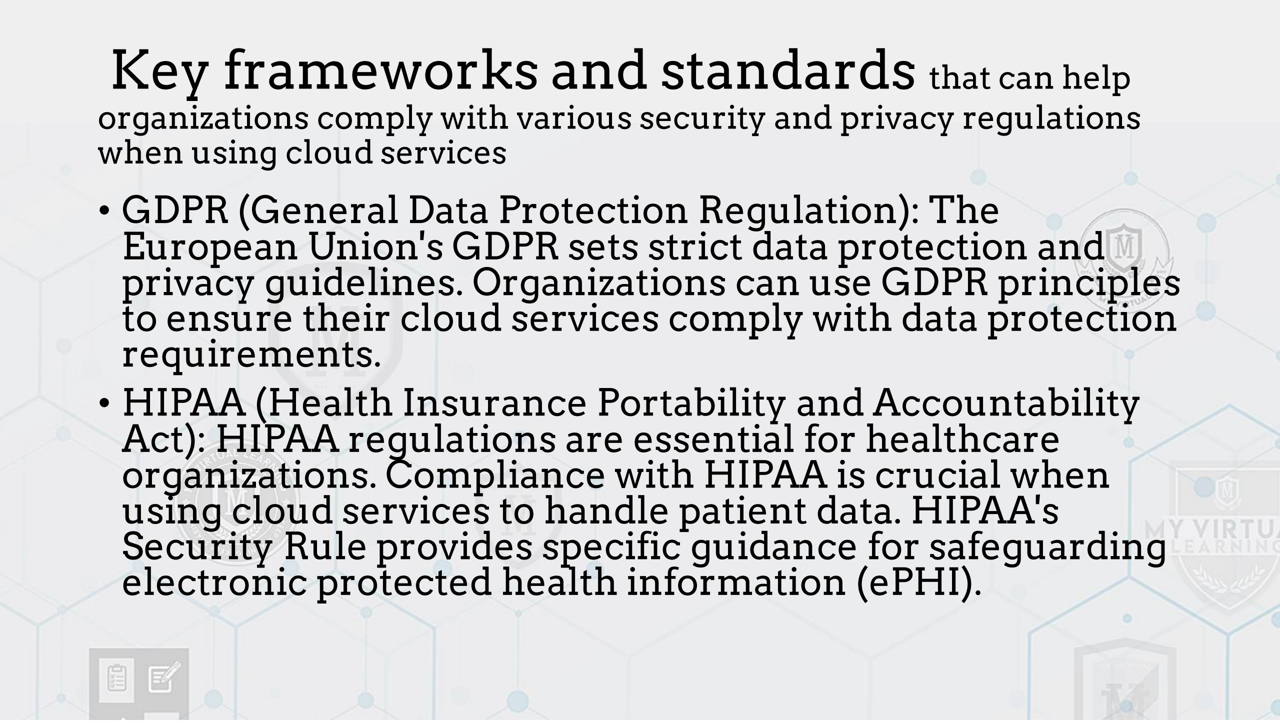
ITE26 – CURRENT TRENDS

Cloud Security Frameworks

@ https://myclass.myvirtuallearning.org

- The primary issues regarding security in the banking and financial services industry are predominantly rooted in elements such as business culture, governance, and compliance rather than solely technology-related.

- Cloud security frameworks provide guidance and tools to assist organizations in recognizing potential vulnerabilities and putting security measures in place to alleviate these vulnerabilities.



Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

- GDPR (General Data Protection Regulation): The European Union's GDPR sets strict data protection and privacy guidelines. Organizations can use GDPR principles to ensure their cloud services comply with data protection requirements.
- HIPAA (Health Insurance Portability and Accountability Act): HIPAA regulations are essential for healthcare organizations. Compliance with HIPAA is crucial when using cloud services to handle patient data. HIPAA's Security Rule provides specific guidance for safeguarding electronic protected health information (ePHI).

Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

- ISO 27001: ISO 27001 is an international standard for information security management systems. Organizations can use it to establish and maintain a robust cloud security framework, ensuring compliance with various security and privacy regulations.
- NIST SP 800-53: The National Institute of Standards and Technology (NIST) provides this comprehensive framework for federal agencies in the United States. It's often used as a foundation for cloud security compliance, especially for government and related organizations.

Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

- SOC 2 (Service Organization Control 2): SOC 2 reports are issued based on the Trust Services Criteria and are often used to assess the security, availability, processing integrity, confidentiality, and privacy of cloud service providers.
- FedRAMP (Federal Risk and Authorization Management Program): FedRAMP is a U.S. government program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services.

Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

- CCPA (California Consumer Privacy Act): For organizations operating in California or handling California residents' data, CCPA regulations must be adhered to. CCPA governs the privacy rights of consumers and includes requirements for data protection in the cloud.
- FISMA (Federal Information Security Management Act): FISMA applies to federal agencies and their use of cloud services. It defines requirements for information security and mandates compliance for cloud solutions used by government entities.

Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

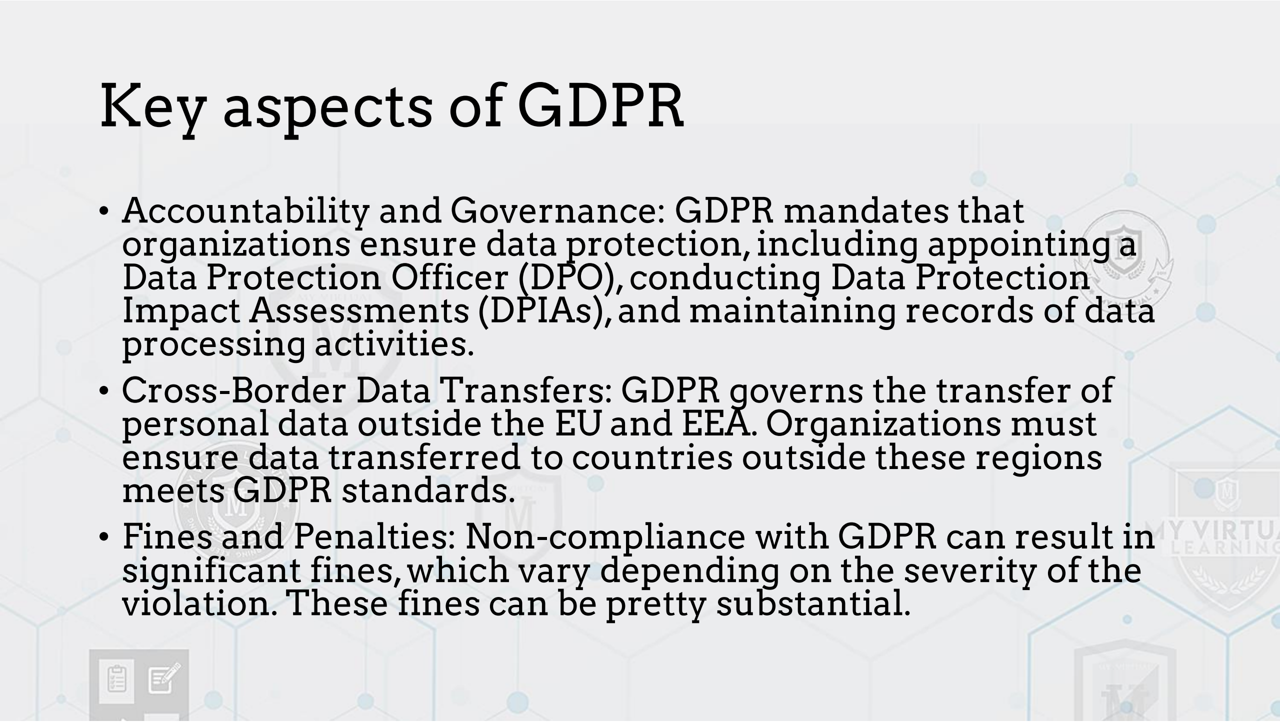
- CSA STAR (Cloud Security Alliance Security, Trust, and Assurance Registry): The CSA STAR program allows cloud providers to self-assess and publicly disclose their security practices, which can assist organizations in evaluating and choosing compliant cloud services.
- CIS Controls: The Center for Internet Security (CIS) provides a set of prioritized security best practices known as the CIS Controls. They can help organizations establish effective security measures in cloud environments.

Key frameworks and standards that can help organizations comply with various security and privacy regulations when using cloud services

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge): While MITRE ATT&CK is not a compliance framework, it is a valuable resource for enhancing cloud security. It provides a knowledge base of known attacker tactics and techniques
- ISO/IEC 27017:2015: ISO/IEC 27017 is a specific standard focused on information security controls for cloud services. It provides guidelines and controls for cloud service providers and customers.

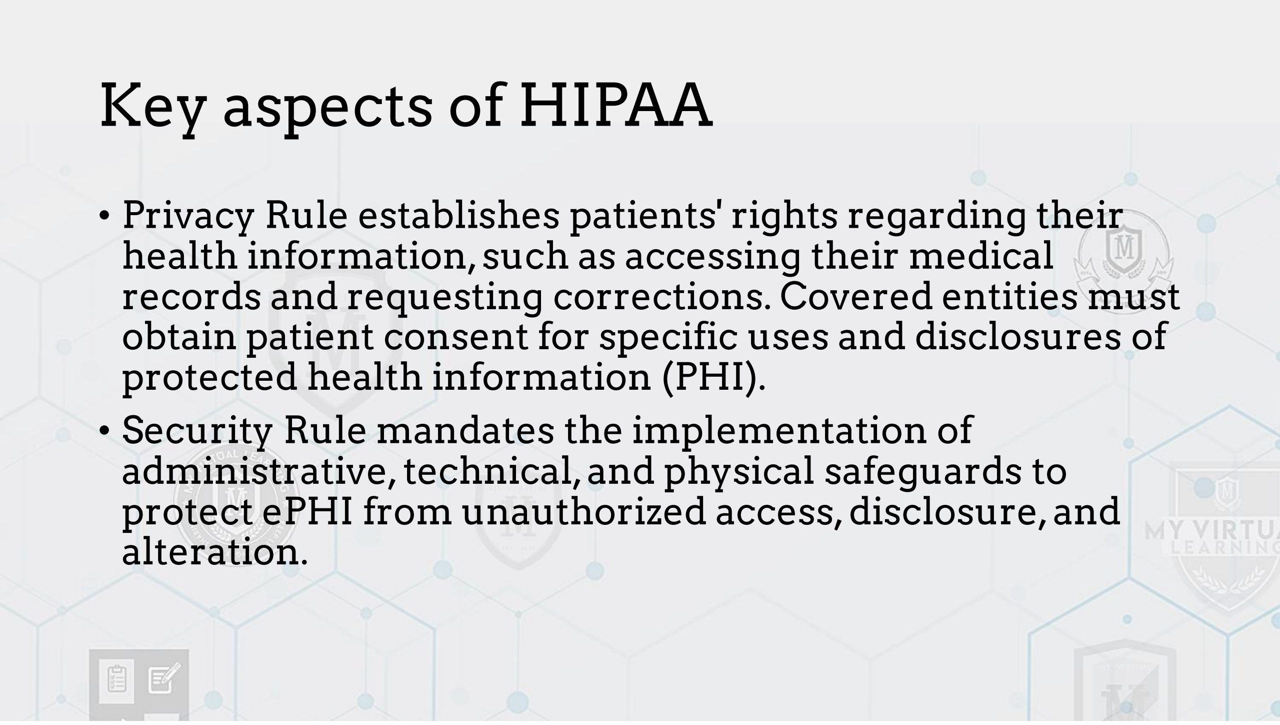
Key aspects of GDPR

- Data Protection Principles: It requires organizations to obtain explicit consent for data processing and to inform individuals about the purposes for which their data is being collected.
- Individual Rights: GDPR grants individuals several rights, including the right to access their own data, the right to rectify inaccuracies, the right to erasure (or "right to be forgotten"), and the right to data portability.
- Data Breach Notification: Organizations must report data breaches to the relevant data protection authority and affected individuals within a specific timeframe.



Key aspects of GDPR

- Accountability and Governance: GDPR mandates that organizations ensure data protection, including appointing a Data Protection Officer (DPO), conducting Data Protection Impact Assessments (DPIAs), and maintaining records of data processing activities.
- Cross-Border Data Transfers: GDPR governs the transfer of personal data outside the EU and EEA. Organizations must ensure data transferred to countries outside these regions meets GDPR standards.
- Fines and Penalties: Non-compliance with GDPR can result in significant fines, which vary depending on the severity of the violation. These fines can be pretty substantial.



Key aspects of HIPAA

- Privacy Rule establishes patients' rights regarding their health information, such as accessing their medical records and requesting corrections. Covered entities must obtain patient consent for specific uses and disclosures of protected health information (PHI).
- Security Rule mandates the implementation of administrative, technical, and physical safeguards to protect ePHI from unauthorized access, disclosure, and alteration.

Key aspects of HIPAA

- Breach Notification Rule requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services (HHS), and, in some cases, the media in case of a breach of unsecured PHI.
- Transactions and Code Sets establish standardized formats for electronic healthcare transactions and code sets to simplify health information exchange. This is particularly relevant for healthcare providers, health plans, and clearinghouses.

Key aspects of HIPAA

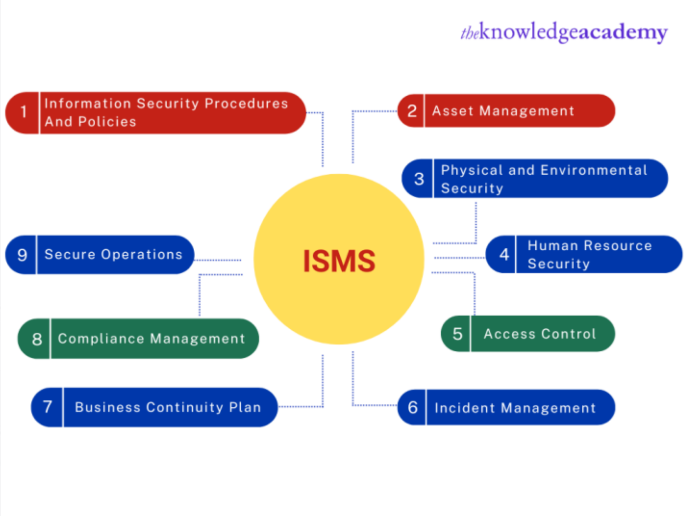
- National Provider Identifier (NPI): HIPAA mandates using a unique identifier, the National Provider Identifier.
- Enforcement: The Office for Civil Rights (OCR) within the HHS enforces HIPAA regulations. Non-compliance with HIPAA can lead to civil and criminal penalties.
- Business Associates: HIPAA extends its privacy and security requirements to business associates of covered entities, such as third-party service providers that handle PHI. Business associates must sign contracts with covered entities, known as Business Associate Agreements, which obligate them to protect PHI.

Key aspects of HIPAA

- HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of HIPAA, introduced provisions related to electronic health records (EHRs), breach notification, and increased penalties for HIPAA violations.

Key aspects of ISO 27001

- Information Security Management System (ISMS): ISO 27001 establishes the framework for creating an ISMS, a systematic approach to managing information security risks.



theknowledgeacademy

ISMS

1 Information Security Procedures And Policies

2 Asset Management

3 Physical and Environmental Security

4 Human Resource Security

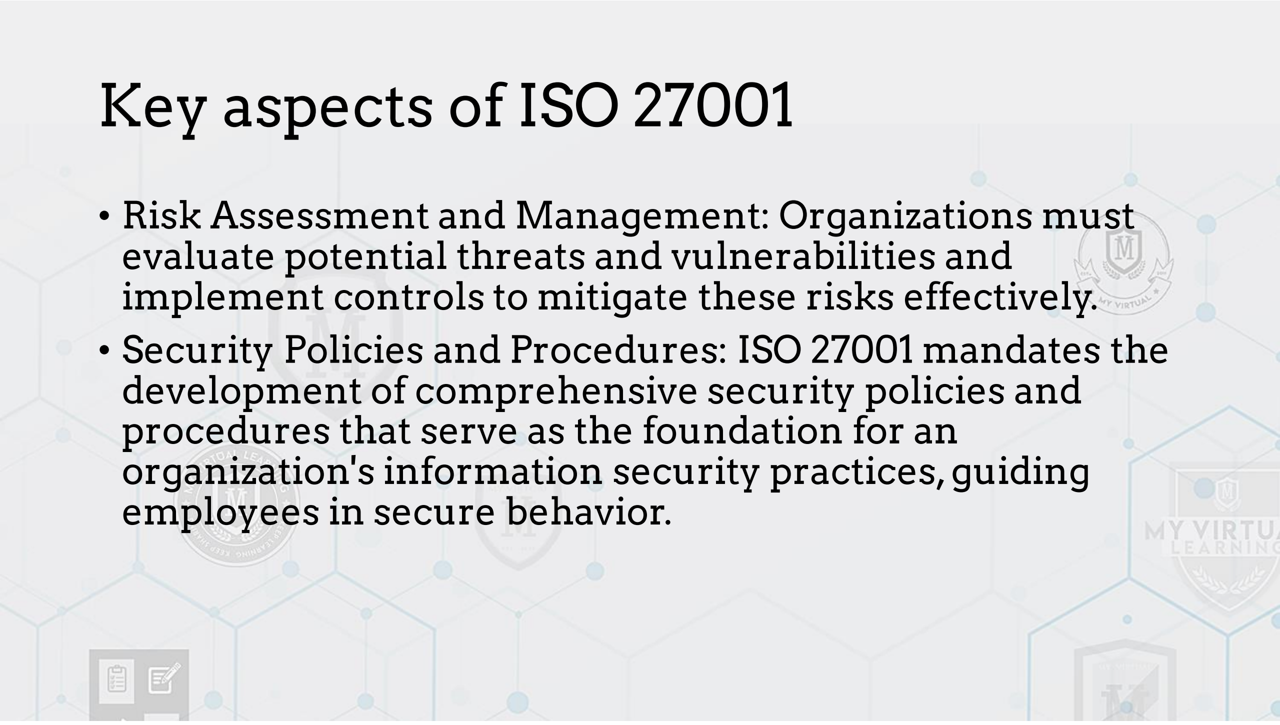
5 Access Control

6 Incident Management

7 Business Continuity Plan

8 Compliance Management

9 Secure Operations

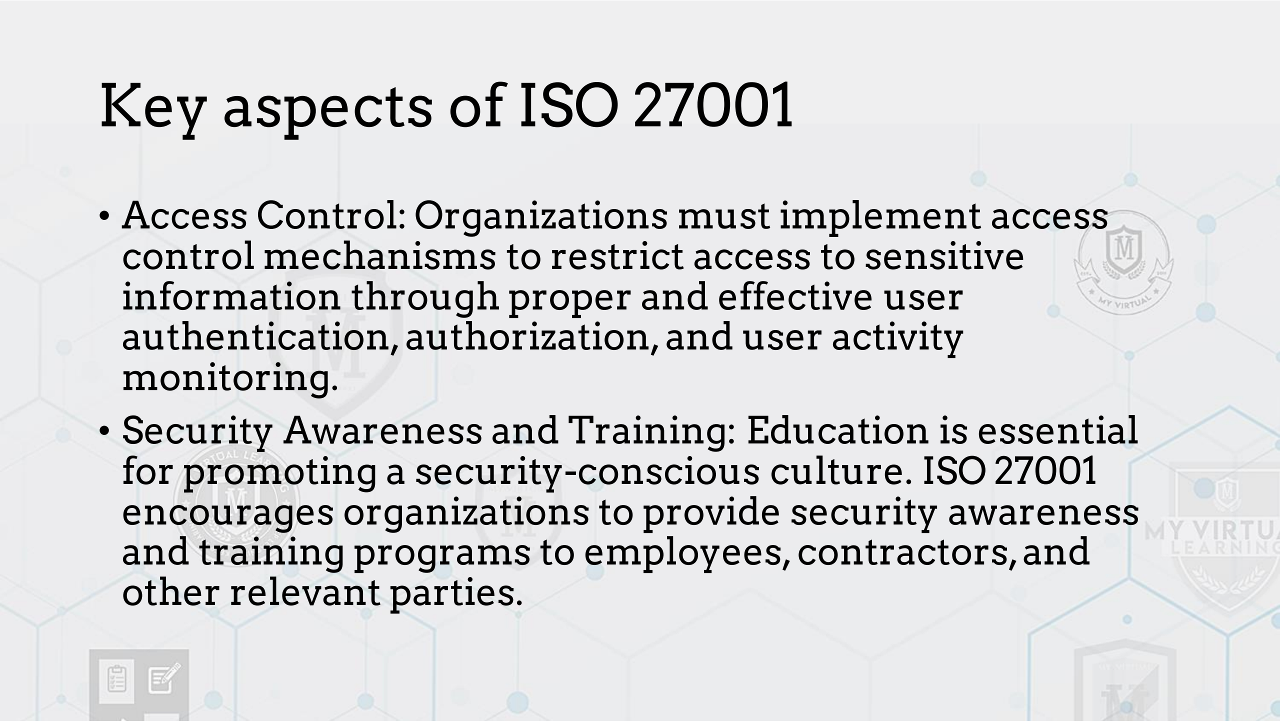


Key aspects of ISO 27001

- Risk Assessment and Management: Organizations must evaluate potential threats and vulnerabilities and implement controls to mitigate these risks effectively.
- Security Policies and Procedures: ISO 27001 mandates the development of comprehensive security policies and procedures that serve as the foundation for an organization's information security practices, guiding employees in secure behavior.

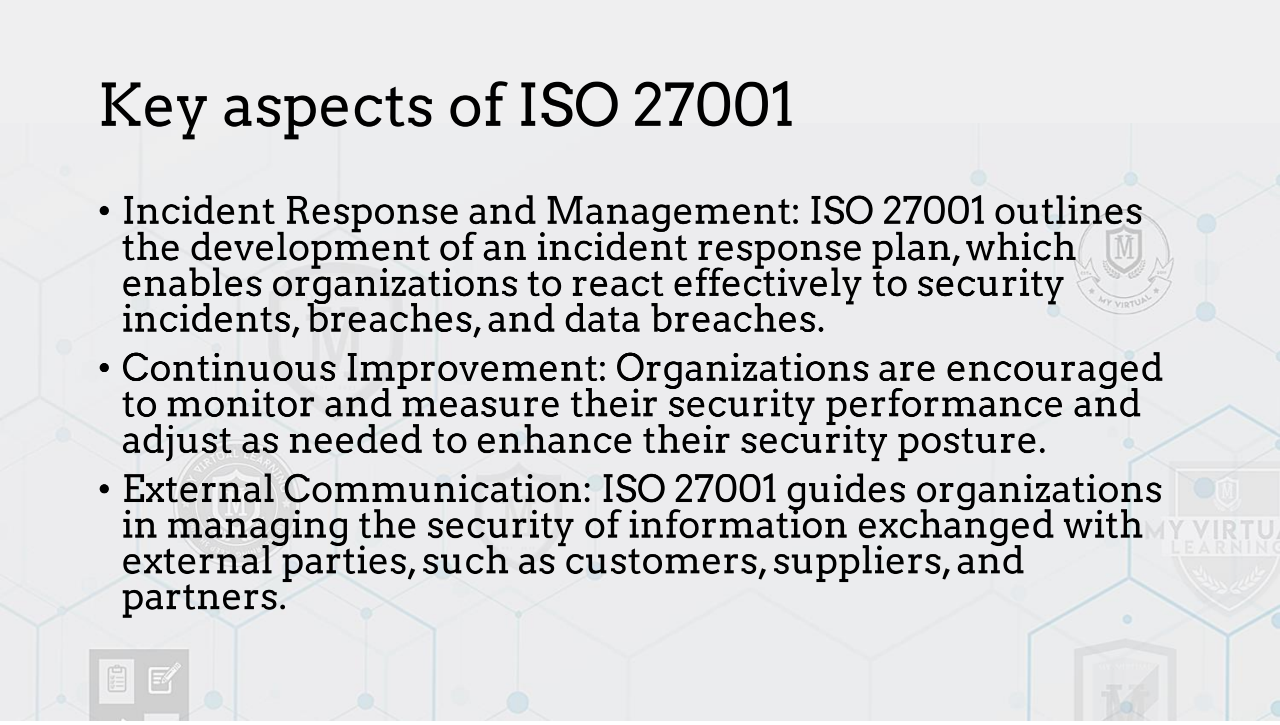
Key aspects of ISO 27001

- Legal and Regulatory Compliance: ISO 27001 helps organizations understand and address legal and regulatory requirements that impact their information security practices to ensure compliance with relevant laws and regulations related to information security.
- Asset Management: ISO 27001 emphasizes identifying and classifying information assets by understanding the value of data and ensuring that appropriate security controls are in place to protect these assets.



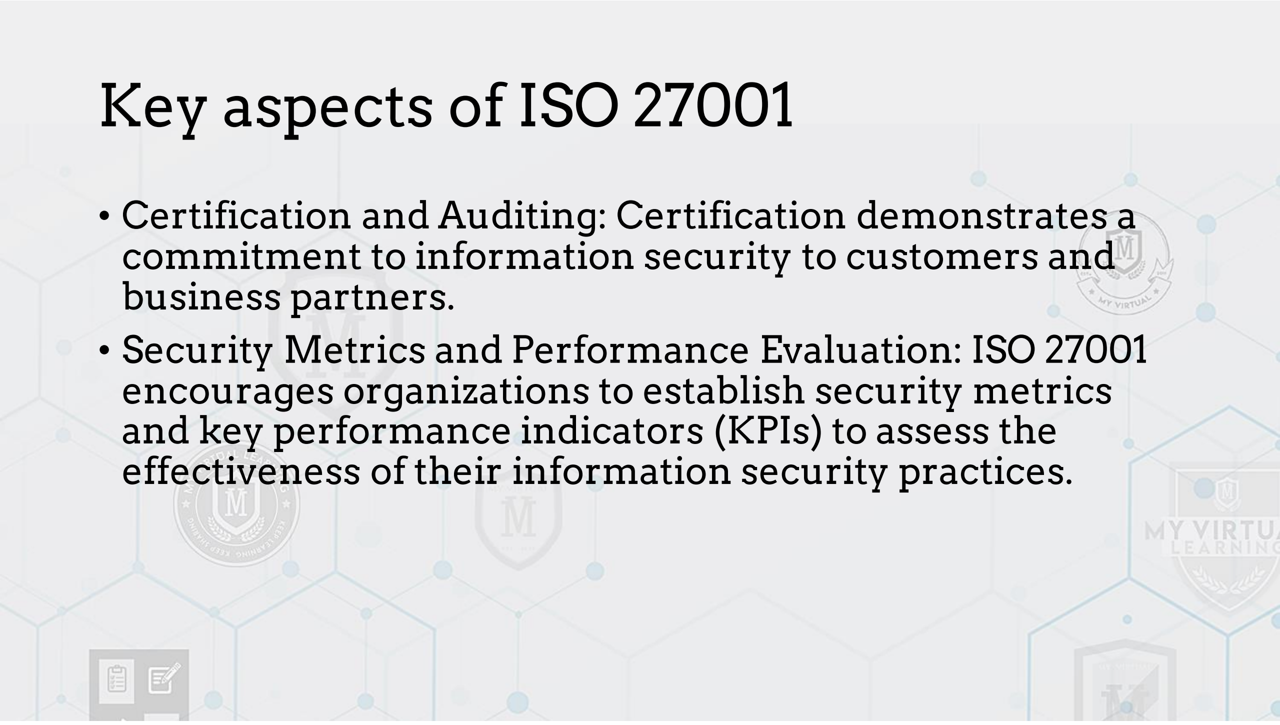
Key aspects of ISO 27001

- Access Control: Organizations must implement access control mechanisms to restrict access to sensitive information through proper and effective user authentication, authorization, and user activity monitoring.
- Security Awareness and Training: Education is essential for promoting a security-conscious culture. ISO 27001 encourages organizations to provide security awareness and training programs to employees, contractors, and other relevant parties.



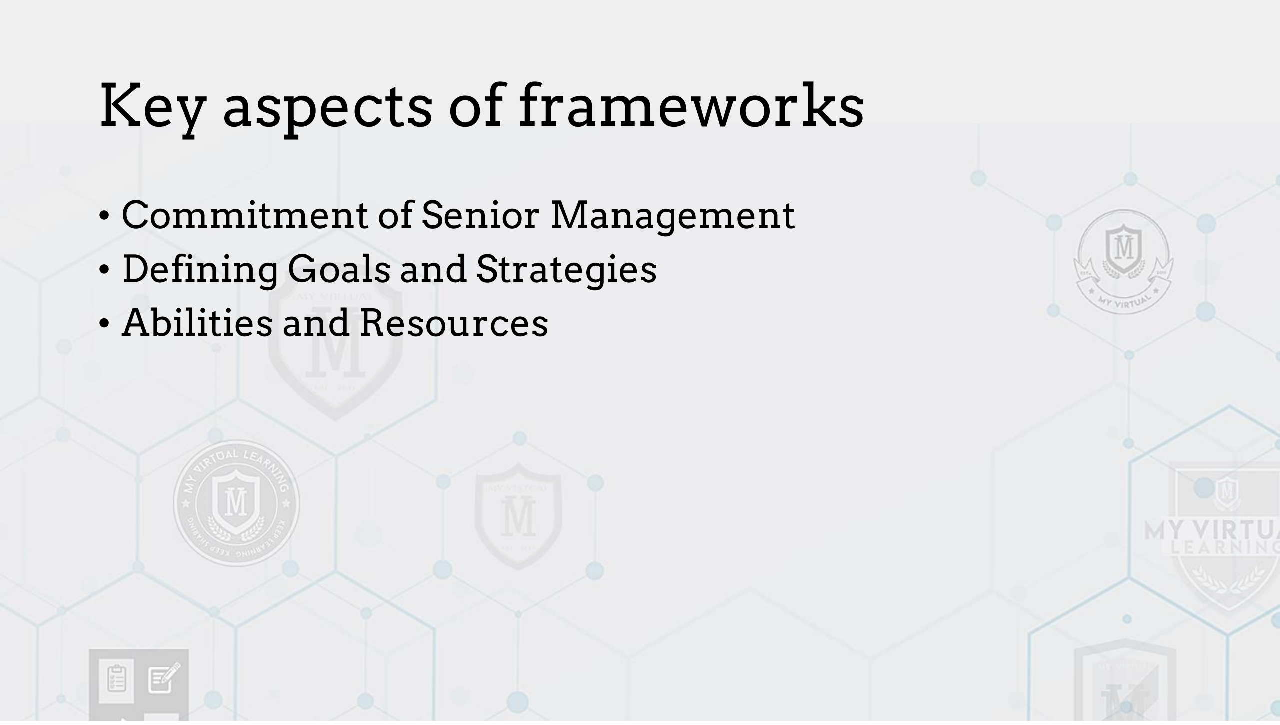
Key aspects of ISO 27001

- Incident Response and Management: ISO 27001 outlines the development of an incident response plan, which enables organizations to react effectively to security incidents, breaches, and data breaches.
- Continuous Improvement: Organizations are encouraged to monitor and measure their security performance and adjust as needed to enhance their security posture.
- External Communication: ISO 27001 guides organizations in managing the security of information exchanged with external parties, such as customers, suppliers, and partners.



Key aspects of ISO 27001

- Certification and Auditing: Certification demonstrates a commitment to information security to customers and business partners.
- Security Metrics and Performance Evaluation: ISO 27001 encourages organizations to establish security metrics and key performance indicators (KPIs) to assess the effectiveness of their information security practices.



Key aspects of frameworks

- Commitment of Senior Management
- Defining Goals and Strategies
- Abilities and Resources

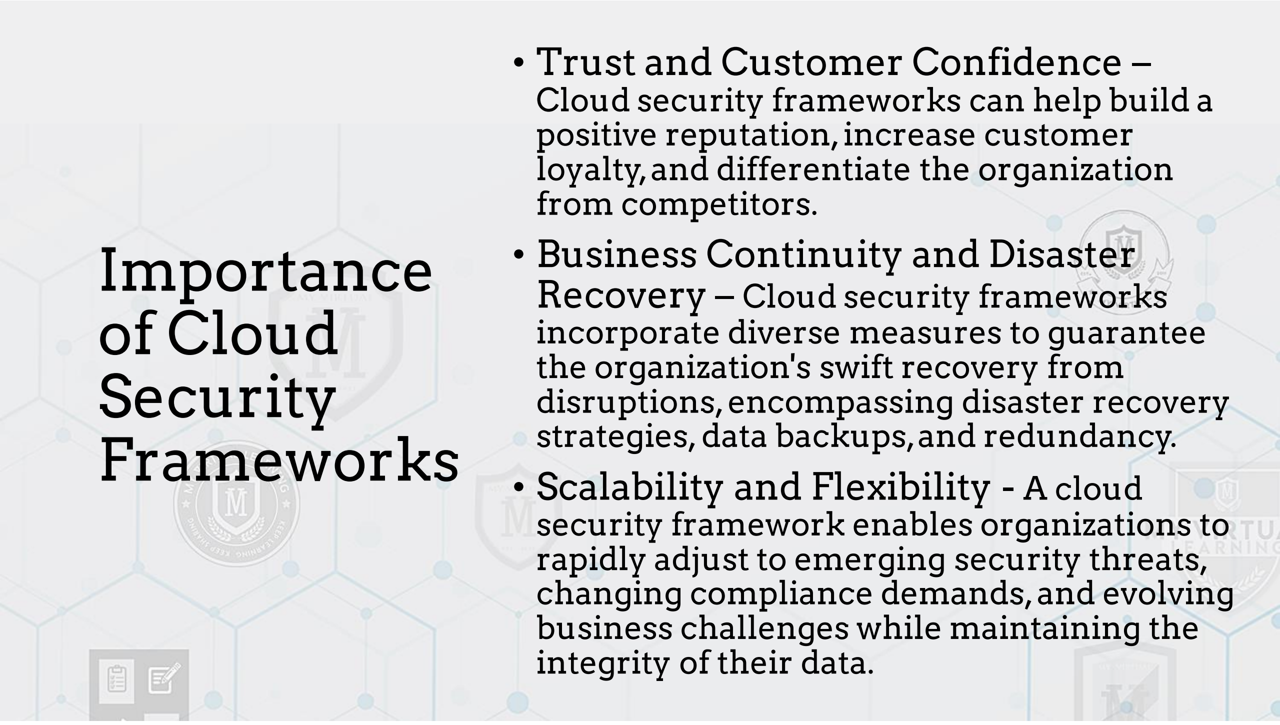
Best practices

It is vital to establish the necessary controls to satisfy regulatory mandates when choosing a cloud security framework that matches the requirements of your business.

- Develop a risk assessment plan that aids in recognizing potential risks and weaknesses, prioritizing response actions, and setting up suitable security measures to safeguard against these risks.
- Implement policies and protocols to reduce risks and ensure adherence to regulatory mandates.
- Put in place monitoring mechanisms to enable early detection, prompt response to threats, and reduce the potential impact by preventing attacks from escalating.

Importance of Cloud Security Frameworks

- Protection of Data - The cloud security framework ensures that the data is encrypted, access is authorized, and data loss or leakage is prevented.
- Mitigation of Security Risks - The cloud security framework helps identify and mitigate various security risks associated with the cloud, like data breaches, account hijacking, insecure interfaces, and shared technology vulnerabilities.
- Compliance with Regulations - Cloud security compliance management helps organizations adhere to their cloud systems' internal rules, standards, and regulatory requirements and avoid fines and penalties.



Importance of Cloud Security Frameworks

- Trust and Customer Confidence – Cloud security frameworks can help build a positive reputation, increase customer loyalty, and differentiate the organization from competitors.
- Business Continuity and Disaster Recovery – Cloud security frameworks incorporate diverse measures to guarantee the organization's swift recovery from disruptions, encompassing disaster recovery strategies, data backups, and redundancy.
- Scalability and Flexibility - A cloud security framework enables organizations to rapidly adjust to emerging security threats, changing compliance demands, and evolving business challenges while maintaining the integrity of their data.