Tata Kelola TI (IT Governance)

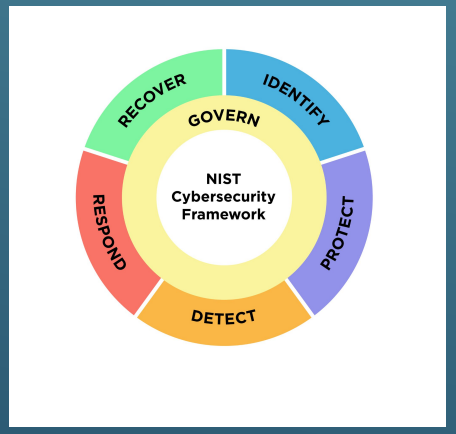
IT Risk Management

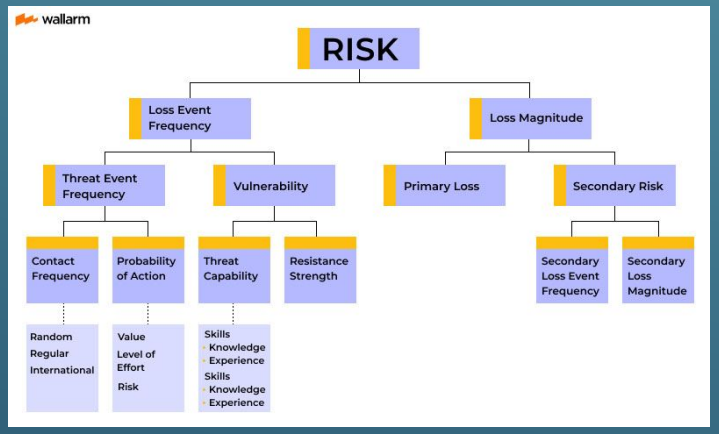
IT RISK MANAGEMENT FRAMEWORK

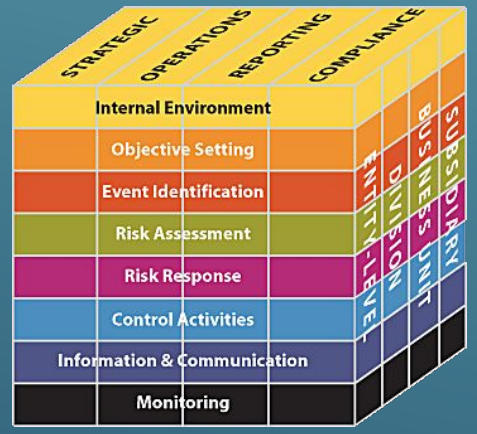
- An IT (Information Technology) risk management framework is a structured approach to identifying, assessing, mitigating, and managing risks related to the use of technology within an organization.
- It provides a systematic way to understand potential threats to information systems, data, and IT processes, and to implement measures to address these risks effectively.

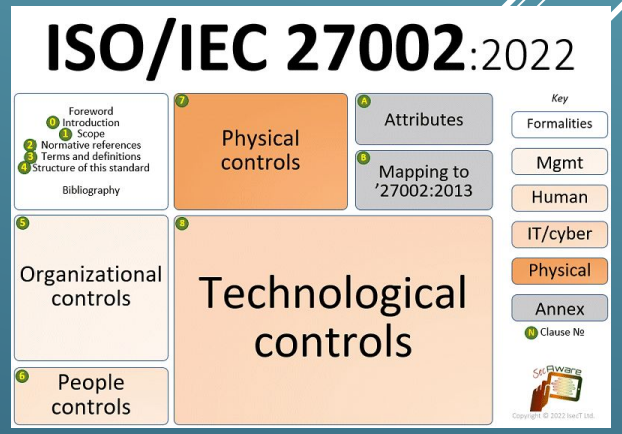
IT RISK MANAGEMENT FRAMEWORK

- **Frameworks :**
  - **ISO 27001/27002**
  - **NIST Cybersecurity Framework**
  - **FAIR (Factor Analysis of Information Risk)**
  - **COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management)**









IT RISK MANAGEMENT FRAMEWORK

- **Frameworks :**
  - **ISO 27001/27002**
    - **Risk Assessment: Conduct a thorough risk assessment based on ISO 27001/27002 guidelines to identify and prioritize information security risks.**
    - **Controls Implementation: Implement controls outlined in ISO 27002 to address identified risks, covering areas such as access control, cryptography, physical and environmental security, and incident management.**
    - **Continuous Improvement: Follow the PDCA (Plan-Do-Check-Act) cycle outlined in ISO 27001 to continuously monitor, review, and improve the effectiveness of information security controls.**

IT RISK MANAGEMENT FRAMEWORK

- **Frameworks :**
  - **NIST Cybersecurity Framework**
    - **Identify: Identify and prioritize critical assets and systems, as well as potential cybersecurity risks and threats.**
    - **Protect: Implement safeguards and controls to protect against identified risks, including access controls, data encryption, and security awareness training.**
    - **Detect: Deploy monitoring tools and capabilities to detect cybersecurity incidents and anomalies in real-time.**
    - **Respond: Develop and implement incident response plans to effectively respond to and mitigate the impact of cybersecurity incidents.**
    - **Recover: Develop and implement strategies to restore systems and operations following a cybersecurity incident, including data recovery and business continuity planning.**

IT RISK MANAGEMENT FRAMEWORK

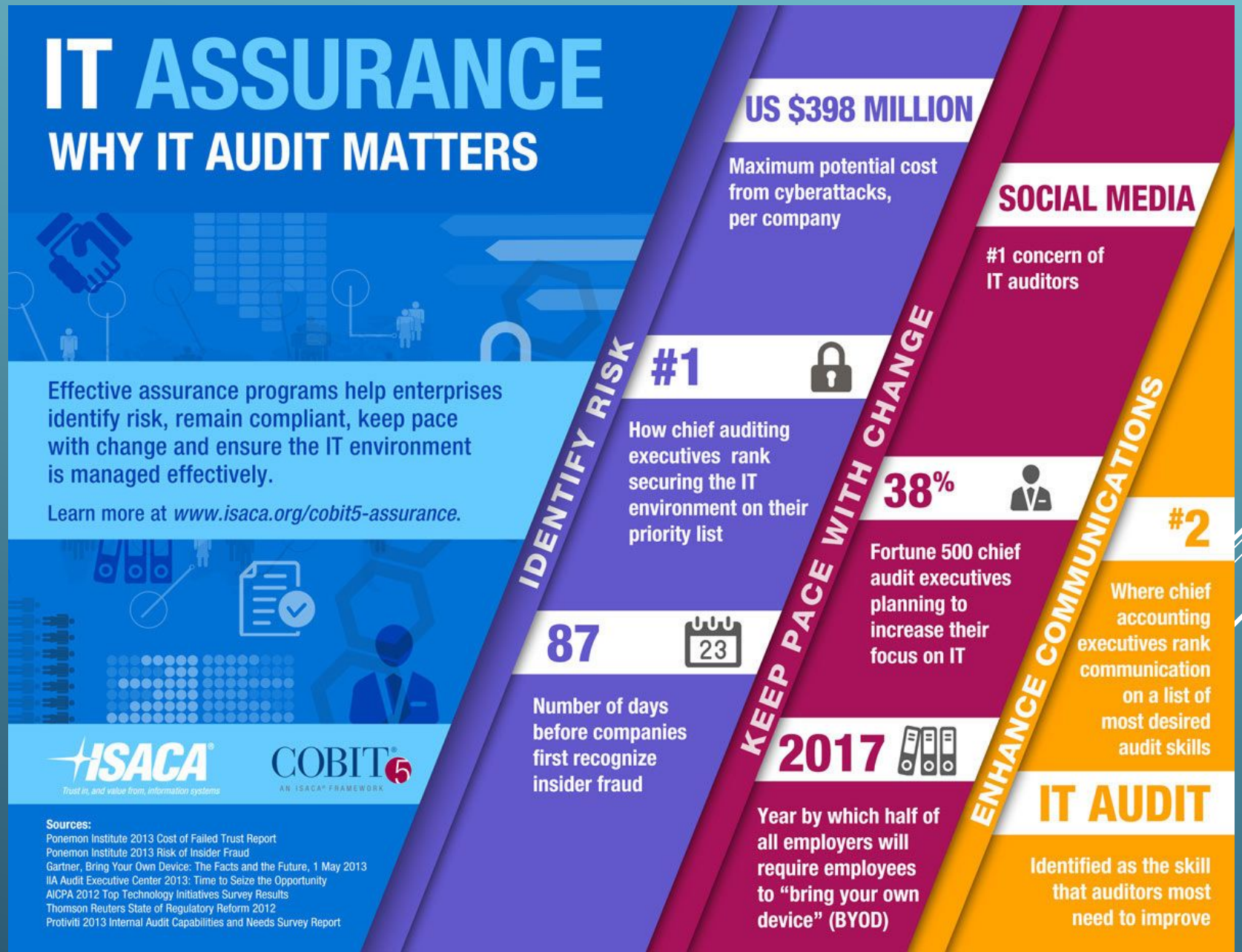
- **Frameworks :**
  - **FAIR (Factor Analysis of Information Risk)**
    - **Quantitative Risk Analysis: Utilize FAIR methodology to quantify and analyze information security risks based on factors such as asset value, threat frequency, vulnerability, and impact.**
    - **Risk Treatment Optimization: Prioritize risk treatment strategies based on cost-benefit analysis and risk tolerance thresholds determined through FAIR analysis.**
    - **Decision Support: Use FAIR-derived risk metrics to support decision-making processes related to resource allocation, risk mitigation investments, and risk acceptance.**

IT RISK MANAGEMENT FRAMEWORK

- **Frameworks :**
  - **COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management)**
    - **Risk Governance: Establish a risk governance structure and processes aligned with COSO ERM principles to oversee and manage IT risks effectively.**
    - **Risk Culture: Foster a risk-aware culture within the organization, promoting accountability and responsibility for managing IT risks at all levels.**
    - **Integration with Strategic Objectives: Align IT risk management activities with the organization's strategic objectives and risk appetite, ensuring that IT risks are considered in strategic decision-making processes.**

AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Audit Processes :**



AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Audit Processes :**

  a. Planning: This involves defining the scope, objectives, and methodology of the audit. It includes identifying key risks, assessing the adequacy of existing controls, and determining the resources needed for the audit.

  b. Fieldwork: During this phase, auditors collect evidence through interviews, document reviews, and testing of controls. They evaluate the design and operating effectiveness of IT controls against established criteria, such as industry standards or regulatory requirements.

AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Audit Processes :**

  c. Reporting: Auditors document their findings, including identified control deficiencies, areas of non-compliance, and recommendations for improvement. Reports typically include an executive summary, detailed findings, and management's response to the audit findings.

  d. Follow-up: After issuing the audit report, follow-up activities may be conducted to ensure that management has implemented corrective actions to address identified deficiencies. This helps to verify the effectiveness of remediation efforts and track progress over time.

AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Assurance Mechanisms :**

  a. Internal Audits: Internal audit functions independently assess the adequacy and effectiveness of IT controls, providing assurance to management and the board of directors. Internal auditors evaluate compliance with policies and procedures, assess the reliability of financial and operational data, and identify opportunities for improvement.

  b. External Audits: External auditors, such as independent accounting firms, examine an organization's financial statements and IT controls to provide assurance to external stakeholders, such as investors, creditors, and regulatory agencies. External audits may include attestation engagements to validate the effectiveness of IT controls.

AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Assurance Mechanisms :**

  c. Compliance Reviews: Compliance reviews assess adherence to relevant laws, regulations, and industry standards governing IT operations and data protection. These reviews ensure that IT practices align with legal requirements and industry best practices, reducing the risk of non-compliance penalties and reputational damage.

  Integration with Strategic Objectives: Align IT risk management activities with the organization's strategic objectives and risk appetite, ensuring that IT risks are considered in strategic decision-making processes.

AUDIT AND ASSURANCE IN IT GOVERNANCE

- **Continuous Monitoring :**
  - **Continuous monitoring involves the real-time or near-real-time assessment of IT systems and controls to detect and respond to security incidents, compliance violations, and operational anomalies. It leverages automated monitoring tools, intrusion detection systems, and security information and event management (SIEM) solutions to collect and analyze data from IT environments.**
  - **Continuous monitoring enables organizations to proactively identify emerging threats, detect unauthorized activities, and strengthen incident response capabilities. It provides stakeholders with ongoing assurance regarding the security and integrity of IT operations, reducing the likelihood of costly breaches and disruptions.**

CASE STUDY

- **Case Study:**

  Background: A multinational corporation operating in the financial services sector recognizes the need to enhance its IT governance practices to mitigate cybersecurity risks and comply with regulatory requirements.

  Approach:

- **The organization establishes a dedicated IT audit function responsible for conducting periodic audits of IT systems and controls.**
- **Internal auditors collaborate with IT stakeholders to develop a risk-based audit plan focusing on critical IT assets, processes, and emerging threats.**
- **As part of the audit process, continuous monitoring capabilities are implemented to enhance the organization's ability to detect and respond to cybersecurity incidents in real-time.**

CASE STUDY

- Automated monitoring tools are deployed to collect and analyze logs, network traffic, and security events across the enterprise IT infrastructure.
- Dashboards and reports are developed to provide stakeholders with visibility into key risk indicators, such as unauthorized access attempts, malware infections, and system vulnerabilities.
- The internal audit team conducts regular reviews of monitoring data to identify trends, patterns, and anomalies that may indicate potential security breaches or compliance issues.
- Audit findings and recommendations are communicated to senior management and the board of directors to facilitate informed decision-making and prioritize resource allocation for risk mitigation efforts.

CASE STUDY

Pilih salah satu topik berikut yang berkaitan dengan manajemen risiko TI:

a. Kerangka ISO 27001/27002
b. Kerangka Keamanan Siber NIST
c. FAIR (Analisis Faktor Risiko Informasi)
d. COSO ERM

Tugas :

Lakukan penelitian kepada salah satu framework yang anda pilih diatas dengan fokus pada

1. Konsep-konsep utama.
2. Metodologi.
3. Manfaat dan tantangan implementasi.
4. Penerapan praktis dan contoh dunia nyata atau studi kasus yang mengilustrasikan penerapannya.

THANK YOU