IT Governance - S6

IT Governance: Managing Emerging Risks with Generative AI

Overview of IT governance as a subset of corporate governance

Specific governance areas within IT governance

Risks associated with uncontrolled use of GenAI

Mitigating these risks using COBIT and operational measures

What is Corporate Governance?

Set of rules, practices, and processes for directing and controlling an organization

Ensures alignment of business strategy with stakeholder interests

Core principles: transparency, accountability, fairness, responsibility

Involves oversight of management, financial performance, risk management, and compliance

What is IT Governance?

Subset of corporate governance focused on managing IT resources and risks

Aligns IT strategies with business goals to deliver value

Ensures efficient and secure IT operations

Manages IT risks, compliance, and resource allocation

Provides accountability and transparency in IT-related decisions

How IT Governance Relates to Corporate Governance

IT governance ensures that IT initiatives support broader business objectives

Manages risks that arise from the use of technology in the organization

IT governance enables strategic use of technology to enhance business performance

Supports corporate governance principles like accountability, compliance, and risk management

Specific Governance Areas within IT Governance

IT Risk Governance: Identifies and mitigates IT-related risks

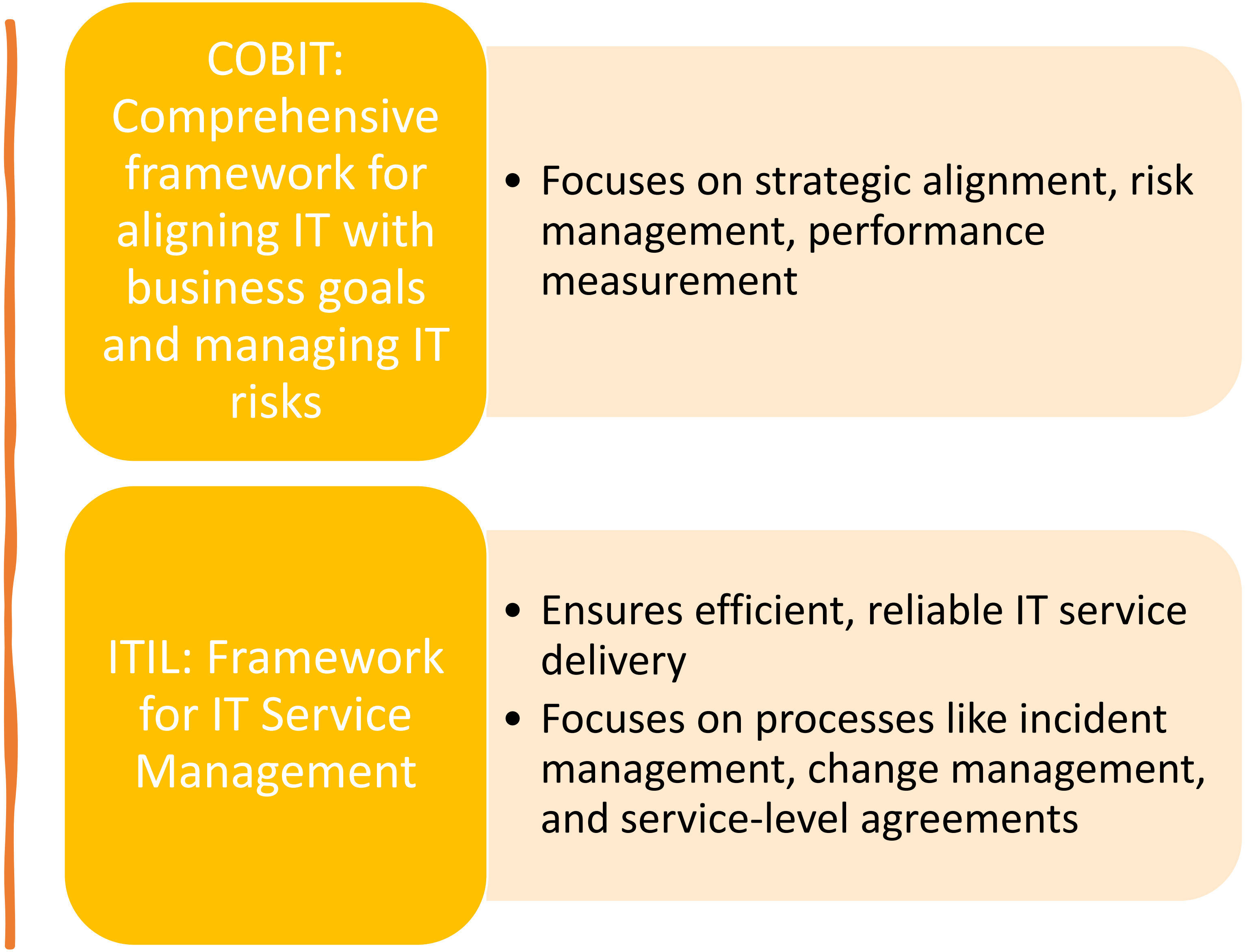
Data Governance: Ensures data security, privacy, and compliance with regulations

Information Security Governance: Protects the confidentiality, integrity, and availability of information

IT Resource Governance: Optimizes management of IT assets and personnel

Compliance Governance: Ensures compliance with laws in IT operations

Frameworks That Facilitate IT Governance



COBIT: Comprehensive framework for aligning IT with business goals and managing IT risks

- Focuses on strategic alignment, risk management, performance measurement

ITIL: Framework for IT Service Management

- Ensures efficient, reliable IT service delivery
- Focuses on processes like incident management, change management, and service-level agreements

Uncontrolled Use of GenAI as a Specific IT Governance Risk

Online Models

- Risks of data privacy, security breaches, and compliance violations
- Dependency on third-party vendors
- Limited control over model behavior and updates

Local Models

- Vulnerabilities include model exploitation, bias in outputs, and resource strains
- Risks of data poisoning, model theft, or misuse by authorized personnel

Operational Measures to Manage Risks of GenAI

- Data Governance: Enforce data anonymization and privacy policies
- Access Controls: Limit access to GenAI tools and models to authorized personnel
- Model Monitoring: Continuously monitor GenAI performance and bias
- Compliance Checks: Ensure AI usage complies with data privacy laws and regulations
- Employee Training: Train staff on responsible AI use and risk awareness

How COBIT Monitors Risks Associated with GenAI

Risk Identification and Assessment

- COBIT guides the identification of risks like data breaches and model bias
- Risk prioritization based on severity and business impact

Risk Mitigation

- COBIT recommends implementing controls such as encryption, access management, and monitoring tools

Performance Monitoring with KPIs

- Key metrics: Data breach incidents, model bias detection rates, compliance audit success rates
- Regular audits and continuous improvement cycles

Conclusion

IT governance is essential for aligning IT initiatives with corporate governance goals

GenAI introduces specific risks that require careful management

Frameworks like COBIT provide structure for monitoring, assessing, and mitigating IT risks

Operational measures like data governance, access control, and compliance monitoring are key to managing GenAI risks