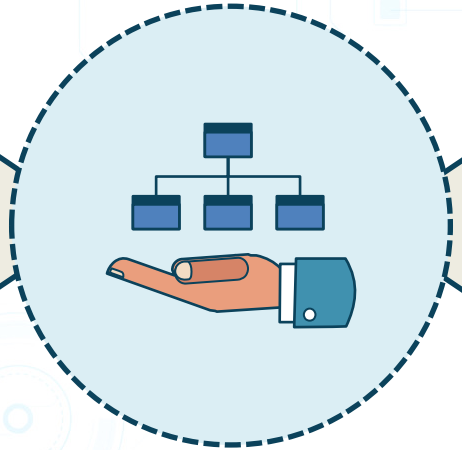
IT Governance

IT solutions



Business objectives

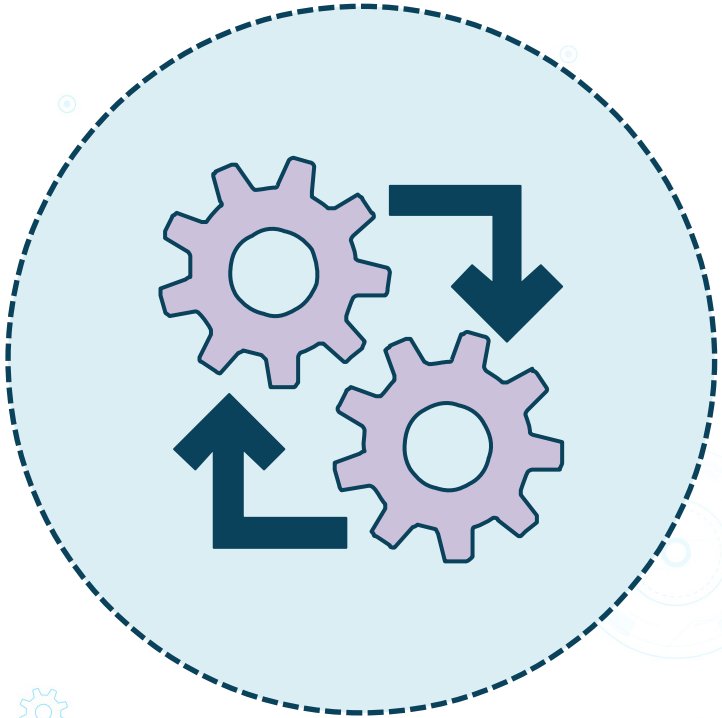
IT Governance

- A formal framework to align technology with business goals
  - Responsibility falls to the Board of Directors and executive management
- Why?
  - Data privacy
  - Financial accountability
  - Shareholder and market pressure

Common IT Governance Frameworks

- ITIL
- COBIT
- ISO/IEC 38500: International Standard for Corporate Governance of IT

COBIT



- Control Objectives for Information and Related Technologies
- Risk management
- Derive value from IT investments
- Improve IT system and data quality

COBIT

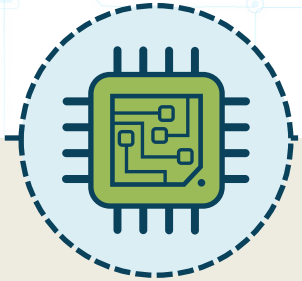

Identify assets and risks
Identify stakeholder needs
Identify business goals
IT changes

COBIT 5

Lifecycle phases

1. Drivers
2. Identify current state
3. Identify future state
4. Plans and activities
5. Plan execution
6. Maintain improvement
7. Review and continuous improvement

Information Technology Infrastructure Library (ITIL)



IT service management best practices

- How does IT fit in to provide the best value in achieving business goals?
- Improve quality and reliability of IT services
- Effective IT practices can affect the bottom line

ITIL Lifecycle

1. Service strategy

- Financial and demand management
- Business relationship management
- Service automation

2. Service design

- Service catalog management
- Capacity and availability
- IT service continuity

ITIL Lifecycle

3. Service transition

- Change management
- Release and deployment
- Service testing

4. Service operation

- Operational health
- Incident management
- Request fulfillment

ITIL Lifecycle

5. Continual service improvement

- Service measurement
- Continual assessment
- Continuous improvement

ITIL and IS Audit Outcomes

- Increased profitability
- Increased service levels
- Compliance with laws, regulations, and contractual obligations

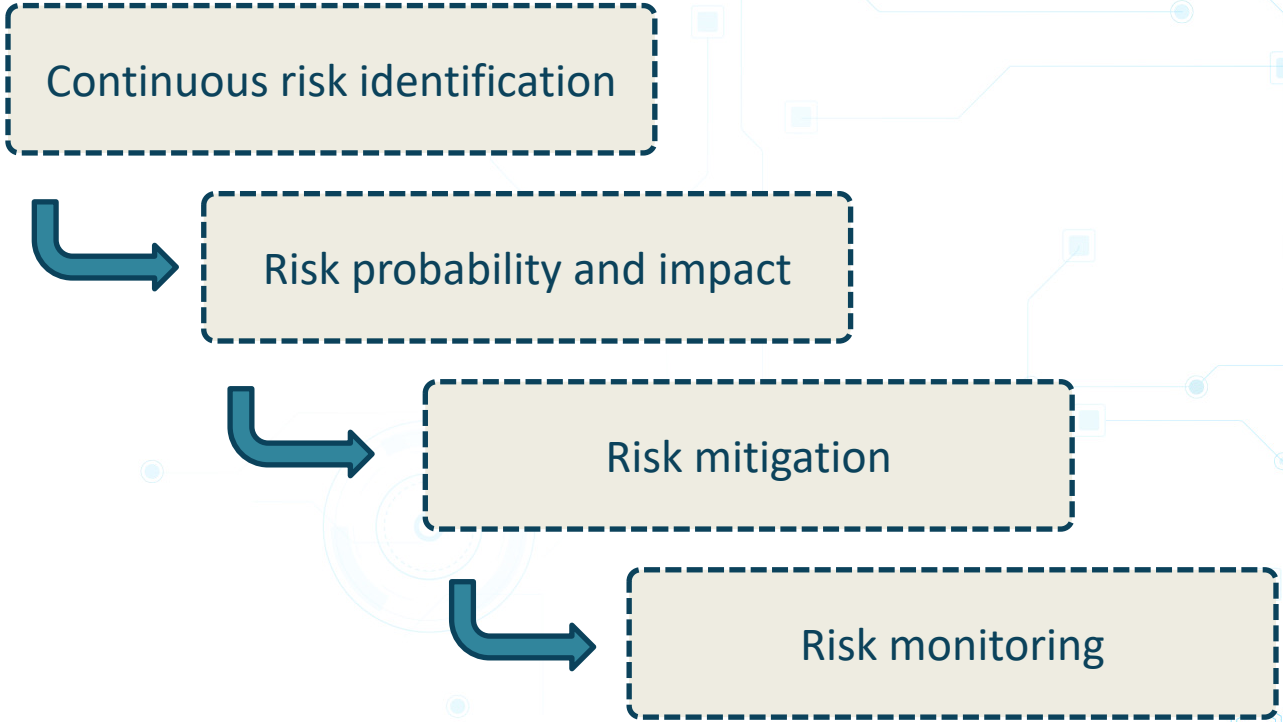
ISO/IEC Standards

- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- IS planning, implementation, maintenance, and continual improvement
- ISO/IEC 27000 family of standards
  - Security of digital information assets
  - Certification provides assurances in the supply chain

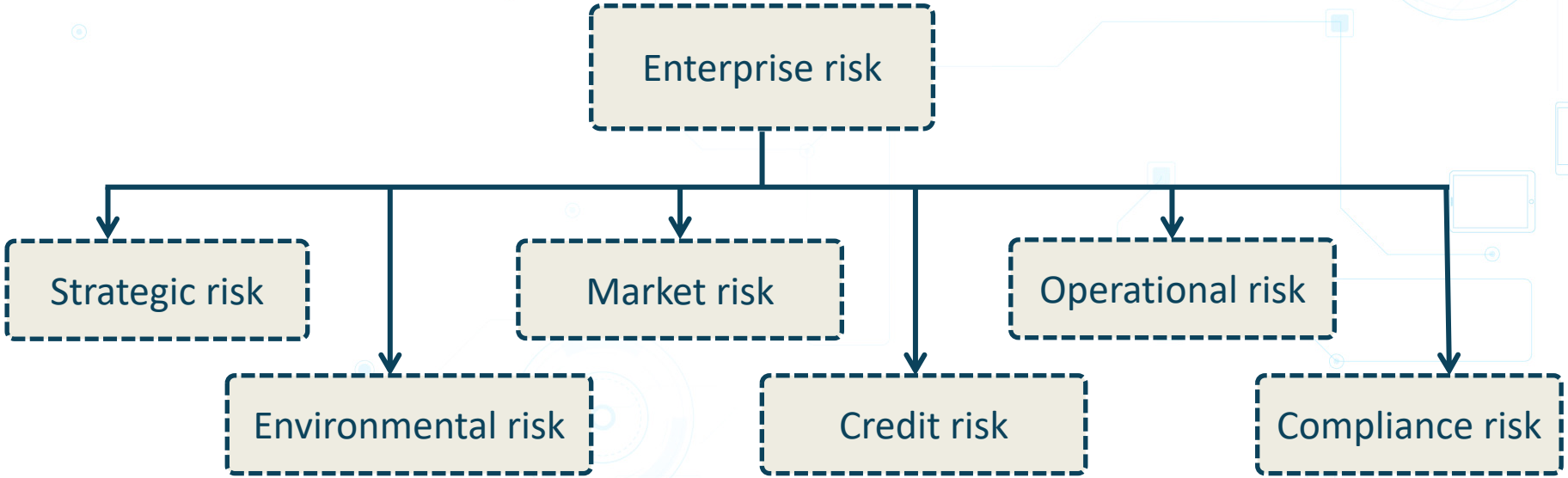
ISO/IEC 27001:2013

- Information Security Management System (ISMS)
  - CIA security triad; manage risk
- Vulnerabilities
- Risk assessment and treatment
- Periodic audits

Risk Management



IT-related Risks



Risk Register

- Central list of identified risks
  - For a business unit or for a project
- Risks are assigned a severity level
  - Probability and impact
- Risk owners are listed
- Risk mitigations are described

Risk Treatment

Organizational risk appetite

Define risk owner

Risk Treatment

Risk acceptance

- Also called *risk retention*
- The risk is known; loss is acceptable should the risk materialize

Risk avoidance

- Risk cannot be transferred
- The risk is unacceptable to the organization
- Choosing to not engage in the activity or project

Risk Treatment

Risk reduction

- Lessen risk frequency and impact (mitigation)
- Implement a strong risk management framework
- Continuous monitoring of security controls

Risk transfer

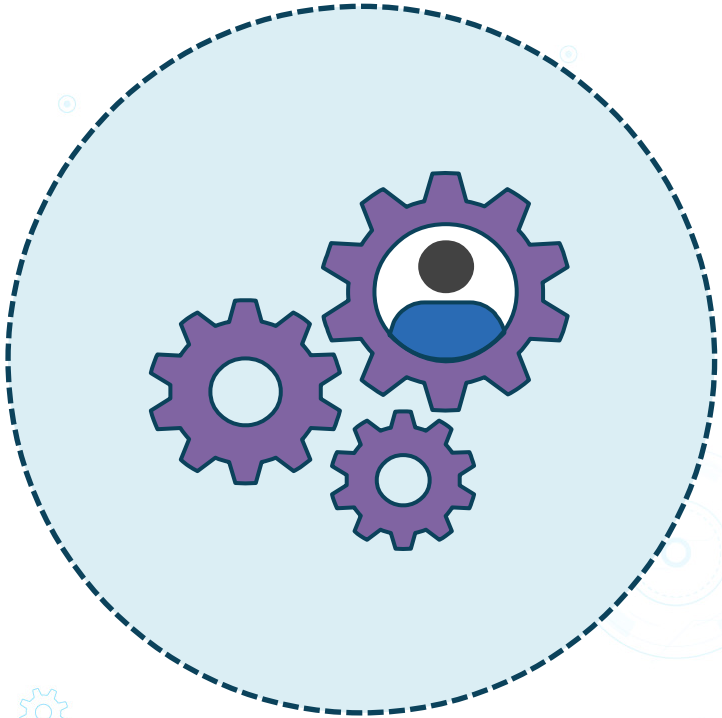
- Also called *risk sharing*
- Use when risk mitigation is not feasible
- Outsourcing
  - Cloud computing and subcontracting
- Insurance
  - Cybersecurity incidents

Business Model for Information Security (BMIS)

- IS security management from a business perspective
  - Interaction of users, technology, and business processes
- Common misconception
  - Security is somebody else's responsibility

Remember, businesses now almost entirely rely on IT solutions

Business Model for Information Security (BMIS)



- Common definition of security among all departments
- Organizations must recognize the need for information security and related time and resources
- An overarching holistic view of security supporting business objectives is needed

Information Technology Assurance Framework (ITAF)

- General standards
- Performance standards
- Reporting standards

Information Technology Assurance Framework (ITAF)

- General standards refers to
  - IS Audit and Assurance Standards
  - 1001: Audit Charter
  - 1005: Due Professional Care
  - IS auditor ethics and objectivity, competency

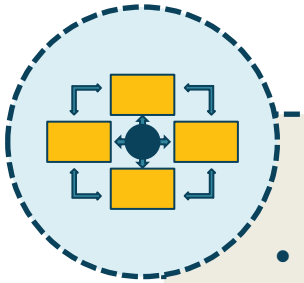
Information Technology Assurance Framework (ITAF)

- Performance standards refers to
  - IS Audit and Assurance Standards
  - 1201: Engagement planning
  - 1202: Risk Assessment in Planning
  - 1204: Materiality

Information Technology Assurance Framework (ITAF)

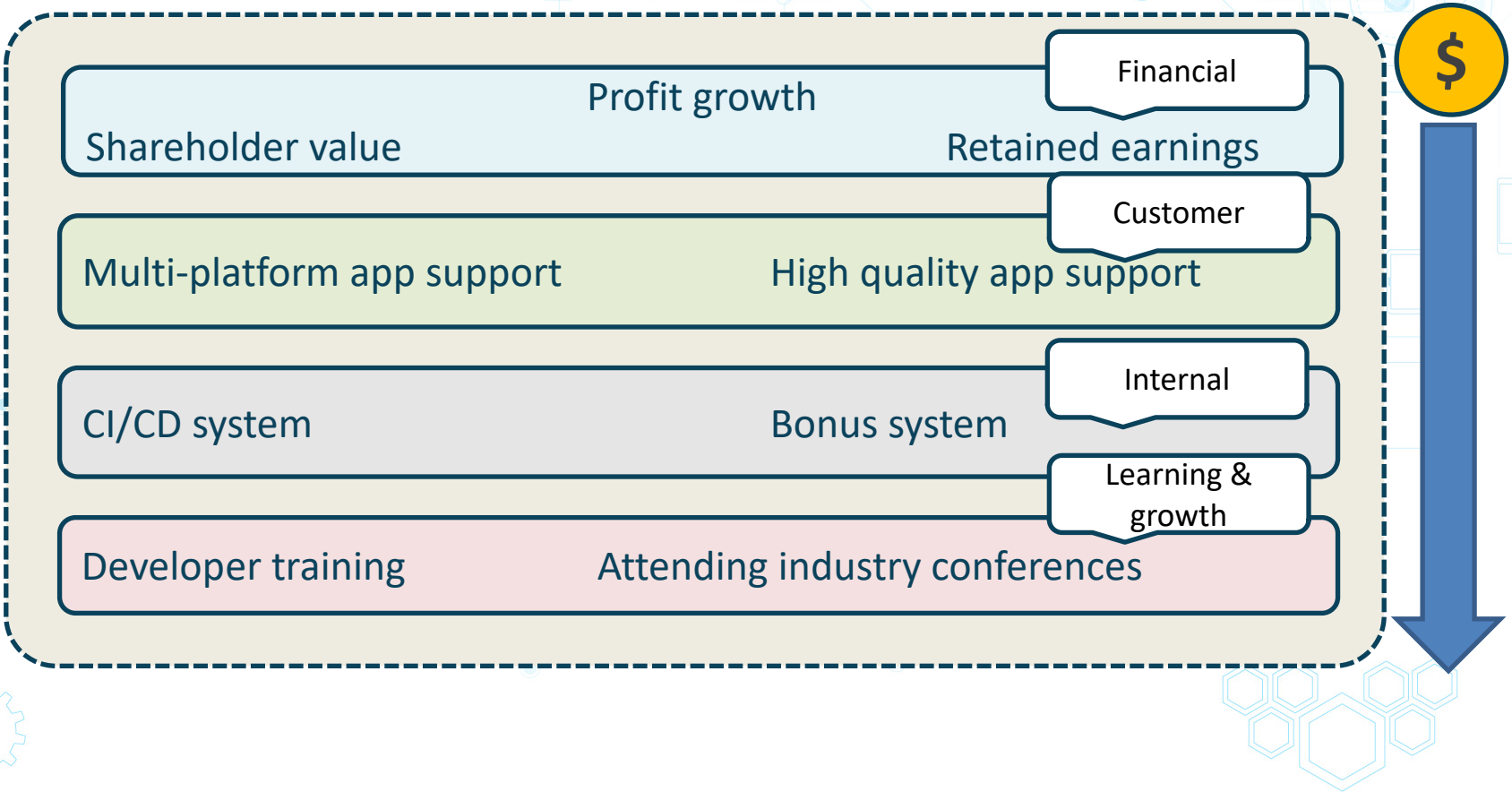
- Reporting standards refers to
  - 1401: Reporting
  - 1402 Follow-up Activities
  - Types of reports, communication

IT Balanced Scorecard (IT BSC)



- Originally a performance management system
- Common language used to convey strategy on one page
- Compare current performance against previously benchmarked values

Sample Software Development Scorecard



In this exercise, you will

- Describe IT governance
- Explain the purpose of COBIT
- List ITIL phases
- List risk treatment options

IT Governance

- Aligning IT solutions with business needs
- Getting the most out of IT investments
  - Increase efficiency and efficacy
  - Reduce waste

COBIT

- An IT governance framework
- Risk management
- Derive value from IT investments
- Improve IT system and data quality

ITIL Phases

1. Service strategy
2. Service design
3. Service transition
4. Service operation
5. Continual service improvement

Risk Treatment

- Risk acceptance
- Risk avoidance
- Risk reduction
- Risk transfer