KPMG Learning Academy

Certified Information Security Manager (CISM)

Module 1: Information Security Governance

In this module, you will learn how to:

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Identify internal and external influences to the organisation
- Define roles and responsibilities
- Establish, monitor, evaluate, and report metrics

Module 2: Information Risk Management and Compliance

In this module, you will learn how to:

- Establish a process for information asset classification and ownership
- Identify legal, regulatory, organisational, and other applicable requirements
- Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted periodically
- Determine appropriate risk treatment options
- Evaluate information security controls
- Identify the gap between current and desired risk levels
- Integrate information risk management into business and IT processes
- Monitor existing risk
- Report noncompliance and other changes in information risk

KPMG Learning Academy

Module 3: Information Security Programme Development and Management

In this module, you will learn how to:

- Establish and maintain the information security program
- Identify, acquire, manage, and define requirements for internal and external resources
- Establish and maintain information security architectures
- Establish, communicate, and maintain organisational information security standards, procedures, and guidelines
- Establish and maintain a programme for information security awareness and training
- Integrate information security requirements into organisational processes, as well as into contracts and activities of third parties
- Establish, monitor, and periodically report programme management and operational metrics

Module 4: Information Security Incident Management

In this module, you will learn how to:

- Establish and maintain an organisational definition and severity hierarchy for information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure timely identification of information security incidents
- Establish and maintain processes to investigate and document information security incidents
- Establish and maintain incident escalation and notification processes
- Organise, train, and equip teams to effectively respond to information security incidents
- Test and review the incident response plan periodically
- Establish and maintain communication plans and processes
- Conduct post-incident reviews
- Establish and maintain integration among the incident response plan, disaster recovery plan, and business continuity plan

LEARNING TREE INTERNATIONAL