KPMG Learning Academy

CompTIA Cybersecurity Analyst CySA+ Certification Training Course Outline

Information Security Governance –

- Establish and maintain an information security strategy, and align the strategy with corporate governance
- Establish and maintain an information security governance framework
- Establish and maintain information security policies
- Develop a business case
- Identify internal and external influences to the organisation
- Obtain management commitment
- Define roles and responsibilities
- Establish, monitor, evaluate, and report metrics

Information Risk Management and Compliance –

- 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

Information Security Program Development and Management –

- Establish and maintain the information security program
- Ensure alignment between the information security program and other business functions
- 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 program for information security awareness and training
- Integrate information security requirements into organisational processes
- Integrate information security requirements into contracts and activities of third parties
- Establish, monitor, and periodically report program management and operational metrics

Information Security Incident Management –

- Establish and maintain an organisational definition of, and severity hierarchy for, information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure the 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 amongst the incident response plan, disaster recovery plan, and business continuity plan

LEARNING TREE INTERNATIONAL