Certified Information Security Manager (CISM)

Course duration	32 hours
Class duration	8 hours
Delivery mode	Instructor-led (classroom/online)

Main Topic	Sub-Topic	Duration (hrs)
Introduction to Information Security Governance	Reasons for Security governance	4
	Activities and results	
	Business alignment	
	Roles and responsibilities	
	Monitoring responsibilities	
	Information Security Governance metrics	
	The security balanced scorecard	
	Business model for Information Security	
Security Strategy Development	Strategy Objectives	4
	Control frameworks	
	Risk Objectives	
	Strategy resources	
	Strategy development	
	Strategy constraints	
Risk Management Concepts	The importance of risk management	1
	Outcomes of risk management	
	Risk management technologies	
Implementing a Risk Management Program	Risk management strategy	1
	Risk management frameworks	
	Risk management context	
	Gap analysis	
	External support	
The Risk Management Life Cycle	Risk management methodologies	3
	Asset identification and valuation	
	Asset classification	
	Threat identification	
	Vulnerability identification	
	Risk identification	
	Risk, likelihood, and impact	
	Risk analysis techniques and consideration	
	Third-party risk management	

Operational Risk Management	The risk register	3
	Integration of risk management into other processes	
	Risk monitoring and reporting	
	Key risk indicators	
	Training and awareness	
	Risk documentation	
Information Security Programs	Outcomes	1
	Charter	
	Scope	
	Information security management frameworks	
	Defining a road map	
	Information security architecture	
	Continuous improvement	
Security Program Management	Security governance	
	Risk management	1
	The risk management program	
	The risk management process	
	Risk treatment	
	Audits and reviews	
	Policy development	
	Third-party risk management	
	Administrative activities	
Security Program Operations	Event monitoring	
	Vulnerability management	2
	Secure engineering and development	
	Network protection	
	Endpoint protection and management	
	Identity and access management	
	Security incident management	
	Security awareness training	
	Managed security service providers	
	Data security	
	Business continuity planning	
IT Service Management	Problem management, Change management, Configuration management, Release management, Service level management, Financial management, Capacity management, Service continuity management, Availability management, Asset management	2
Controls	Internal control objectives, information systems control objectives, general computing controls, control frameworks, controls development, control assessment	1
Metrics and Monitoring	Types of metrics, audience, continuous improvement	1
Security Incident Response Overview	Phases of incident response	1
Incident Response Plan Development	Objectives, maturity, resources, roles and responsibilities, Gap analysis, plan development	1.5

Responding to Security Incidents	Detection, initialization, evaluation, eradication, recovery, remediation, closure, post-incident review	4
Business Continuity and Disaster Recovery	Business continuity planning	1.5
	Disaster recovery planning	
	Testing BC and DR plans	
Total Course Duration (hrs)		32