CISM TIMETABLE (4 DAYS)

ISACA-CISM

Day 1

	Course introduction	**09.00**	**09.30**
01	Overview of the CISM certification	**09.30**	**10.30**
02	**Domain 1 - Information Security Governance** Learning objectives Domain Task and Knowledge Statements • Priorities for the CISM • Corporate Governance • Information Security Strategy • Information Security Program • Elements of a Security Program • Roles and Responsibilities • Evaluating a Security Program • Reporting and Compliance • Ethics • Summary & Conclusion	**11.15**	**13.00**
	Lunch	**13.00**	**13.30**
02	Domain 1 - Information Security Governance ctn.	**13.30**	**16.30**
	Recap Day 1	**16.30**	**17.00**

Day 2

	Review Day 1	**09:00**	**09:15**
03	**Domain 2 - Information Risk Management and Compliance** Learning objectives Domain Task and Knowledge Statements • Information Asset Classification • Identify regulatory, legal and other requirements • Identify risk, threats and vulnerabilities • Risk treatment • Evaluate security controls • Integrate risk management into business processes • Report non-compliance and other changes in risk • Summary & Conclusion	**09:15**	**13:30**
	Lunch	**13:00**	**13:30**
03	Domain 2 - Information Risk Management and Compliance ctn.	**13:30**	**16:30**
	Recap Day 2	**16.30**	**17.00**

Day 3

	Review Day 2	**09:00**	**09:15**
04	**Domain 3 - Information Security Program Development and Management** Learning objectives Domain Task and Knowledge Statements • Security Program Development Objectives • Role of the Information Security Manager • Information Security Program Development • Elements of a Security Program • Information Security Concepts • Technology and Tools, Security Models • Integrating Security into the Business • Summary & Conclusion	**09:15**	**13:30**
	Lunch	**13:00**	**13:30**
04	**Domain 3 - Information Security Program Development and Management ctn.**	**13:30**	**16:30**
	Recap Day 3	**16.30**	**17.00**

Day 4

	Review Day 3	**09:00**	**09:15**
05	**Domain 4 - Information Security Incident Management** Learning objectives Domain Task and Knowledge Statements • Controls • SDLC Process • Business Risk versus Project Risk • High Level SDLC phases • Project risk • PM tools and techniques • Transaction Data, Compliance, Process, Continuous Monitoring • Cause and Effect Diagram • Summary & Conclusion	**09:00**	**13:00**
	Lunch	**13:00**	**13:30**
05	Domain 4 - Information Security Incident Management ctn.	**13:30**	**16:30**
	Recap Day 4	**16.30**	**17.00**