



Agenda

CISM Revision Workshop – Northern Chapter 28 – 30 April 2010

Day 1

Wednesday 28 April 2010

9.30 -10.00 Registration

CISM Examination Logistics

- The format of CISM questions
- The examination structure
- Time management in exam conditions
- Strategies for successfully completing the CISM examination

Information Security Governance (ISG)

1. Develop an Information Security Strategy aligned with business goals & objectives.
2. Align the Information Security Strategy with Corporate Governance.
3. Develop business cases justifying investment in Information Security.
4. Identify current & potential legal/regulatory requirements affecting Information Security.
5. Identify drivers affecting the organisation (e.g. technology, business environment, risk tolerance, geographic location) & their impact on Information Security.
6. Obtain senior management commitment on Information Security.
7. Define roles & responsibilities for Information Security throughout the organisation.
8. Establish internal/external reporting & communication channels that support Information Security.

12.30 – 1.30 Lunch

ISG Knowledge Statements

1. Business goals & objectives
2. IS concepts
3. Components that comprise an IS strategy (e.g. processes, people, technologies, architectures)
4. Relationship between IS & business functions
5. Scope & charter of IS governance
6. Concepts of corporate & IS governance
7. Methods of integrating IS governance into the overall governance framework
8. Budgetary planning strategies & reporting methods
9. Methodologies for business case development
10. Types/impact of internal & external drivers (e.g. technology, business environment, risk tolerance) that may affect organizations & IS
11. Regulatory requirements & potential business impact from an IS standpoint
12. Common liability management strategies & insurance options (e.g. crime or fidelity insurance, business interruptions)
13. Third-party relationships & their impact on IS (e.g. mergers & acquisitions, partnerships, outsourcing)
14. Methods used to obtain senior management commitment to IS
15. Establishment/operation of an IS steering group
16. IS management roles, responsibilities & general organizational structures
17. Approaches for linking policies to business objectives
18. Generally accepted international standards for IS management
19. Centralized & distributed methods of coordinating IS activities
20. Methods for establishing reporting & communication channels throughout an organization

ISG Sample Examination Questions & Discussion

Review of the Day

4.30

Day 2
Thursday 29 April 2010

9.30 Start

Risk Management (RM)

1. Develop a systematic, analytical and continuous risk management process.
2. Ensure that risk identification, analysis and mitigation activities are integrated into life cycle processes.
3. Apply risk identification and analysis methods.
4. Define strategies and prioritize options to mitigate risk to levels acceptable to the enterprise.
5. Report significant changes in risk to appropriate levels of management on both a periodic and event-driven basis.

RM Sample Examination Questions & Discussion

12.30 – 1.30 Lunch

Information Security Programme Development (ISPD)

1. Develop/maintain plans to implement Information Security strategy
2. Specify activities to be performed within Information Security program
3. Ensure alignment between Information Security program & other assurance functions (e.g. physical, HR, quality, IT)
4. Identify int. & external resources (finance, people, equipment, systems) required to execute IS program
5. Ensure development of Information Security architectures (people, processes, technology)
6. Establish, communicate & maintain Information Security policies that support Information Security Strategy
7. Design & develop a program for Information Security awareness, training/education
8. Ensure development./communication. & maintenance of standards, procedures & other documents (e.g. guidelines, baselines, codes of conduct) that support Information Security policies
9. Integrate Information Security requirements into processes (e.g., change control, mergers & acquisitions) & life cycle activities (e.g., development, employment, procurement)

10. Develop process to integrate Information Security controls into contracts (e.g. joint ventures, outsourced providers, business partners, customers, third parties)
11. Establish metrics to evaluate effectiveness of Information Security program

ISPD Sample Examination Questions & Discussion

Review of the Day 4.30

Day 3
Friday 30 April 2010

9.30 Start

**Information Security Program
Management (ISPM)**

1. Manage internal & external resources required to execute the Information Security program
2. Ensure that processes/procedures are compliance with Information Security policies/standards
3. Ensure the performance of contractually agreed Information Security controls
4. Ensure that Information Security is an integral part of systems development/acquisition processes
5. Ensure that Information Security is maintained throughout processes & life cycle activities
6. Provide Information Security advice and guidance
7. Provide Information Security awareness, training & education to stakeholders
8. Monitor, measure, test & report on effectiveness/efficiency of Information Security controls & compliance with Information Security policies
9. Ensure noncompliance issues/variances are resolved in a timely manner

**ISPM Sample Examination
Questions & Discussion**

12.30 – 1.30 Lunch

**Incident Management & Response
(IMR)**

1. Develop/implement processes to detect, identify, analyze & respond to Information Security incidents.
2. Establish escalation/communication processes & lines of authority.
3. Develop plans to respond to & document Information Security incidents.
4. Establish capability to investigate Information Security incidents.
5. Develop a process to communicate with internal parties & external organisations
6. Integrate Information Security incident response plans with DRP/ BCP.
7. Organize, train, & equip teams to respond to Information Security incidents.
8. Periodically test/ refine Information Security incident response plans.

9. Manage response to Information Security incidents.
10. Conduct reviews to identify causes of Information Security incidents, develop corrective actions & reassess risk.

15.00 – 16.00 - Mock Examination

Review of the Course 4.30