Information Security Governance

Functional Area Overview
Introduction
Developing an Information Security Strategy in Support of Business Strategy and Direction
Senior Management Commitment and Support
Definitions of Roles and Responsibilities
Obtaining Senior Management Commitment
Establish Reporting Communications That Support Information Security Governance Activities
Legal and Regulatory Issues
Establish and Maintain Information Security Policies
Ensure the Development of Procedures and Guidelines
Develop Business Case and Enterprise Value Analysis Support
Summary
Questions

Information Security Risk Management

Functional Area Overview
Introduction
Develop a Systematic and Continuous Risk Management Process
Ensure Risk Identification, Analysis, and Mitigation Activities Are Integrated Into the Life Cycle Process
Apply Risk Identification and Analysis Methods
Define Strategies and Prioritize Options to Mitigate Risks to Levels Acceptable to the Enterprise
Report Significant Changes in Risk
Knowledge Statements
Summary
Questions

Information Security Programme Management

Functional Area Overview
CISM® Mapping
Introduction
The OSI Model
The TCP/IP Model
IP Addressing
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
Internet Control Message Protocol (ICMP)
CIA Triad
PPPN
Threats
Controls
Buffer Overflows versus Application Security
Virtual Private Networks (VPNs)
Web Server Security versus Internet Security
Security Testing
Summary
Questions
Information Security Management

Functional Area Overview
Introduction
Information Systems Comply
Ensure the Administrative Procedures for Information Systems Comply with the
Enterprise’s Information Security Policy
Ensure Services Outsourced Are Consistent
Measure, Monitor, and Report on the Effectiveness and Efficiency of the Controls and
Compliance with Information Security Policies
Ensure That Information Security Is Not Compromised Throughout the Change Management
Process
Perform Vulnerability Assessments to Evaluate Effectiveness of Existing Controls
Ensure That Non-compliance Issues and Other Variances are Resolved in a Timely Manner
Information Security Awareness and Education
Summary
Questions

Response Management

Functional Area Overview
CISM Mapping
Introduction
Threat Source Information
Business Continuity Planning and Disaster Recovery Planning
Incident Response
Summary
Questions
Index