2017 ISSMP Detailed Content Outline With Weights (For Public Distribution)		
Classification	Domain/Task/Subtask	Weight
1	Leadership and Business Management	22%
1.1	Establish Security's Role in Organizational Culture, Vision, and Mission	
1.1.1	Define information security program vision and mission	
1.1.2	Align security with organizational goals, objectives, and values	
1.1.3	Explain business processes and their relationships	
1.1.4	Describe the relationship between organizational culture and security	
1.2	Align Security Program with Organizational Governance	
1.2.1	Identify and navigate organizational governance structure	
1.2.2	Recognize roles of key stakeholders	
1.2.3	Recognize sources and boundaries of authorization	
1.2.4	Negotiate organizational support for security initiatives	
1.3	Define and Implement Information Security Strategies	
1.3.1	Identify security requirements from business initiatives	
1.3.2	Evaluate capacity and capability to implement security strategies	
1.3.3	Manage implementation of security strategies	
1.3.4	Review and maintain security strategies	
1.3.5	Describe security engineering theories, concepts, and methods	
1.4	Define and Maintain Security Policy Framework	
1.4.1	Determine applicable external standards	
1.4.2	Manage data classification	
1.4.3	Establish internal policies	
1.4.4	Obtain organizational support for policies	
1.4.5	Develop procedures, standards, guidelines, and baselines	
1.4.6	Ensure periodic review of security policy framework	
1.5	Manage Security Requirements in Contracts and Agreements	
1.5.1	Evaluate service management agreements (e.g., risk, financial)	
1.5.2	Govern managed services (e.g., infrastructure, cloud services)	
1.5.3	Manage impact of organizational change (e.g., mergers and acquisitions, outsourcing)	
1.5.4	Monitor and enforce compliance with contractual agreements	
1.6	Oversee Security Awareness and Training Programs	
1.6.1	Promote security programs to key stakeholders	
1.6.2	Identify training needs by target segment	
1.6.3	Monitor and report on effectiveness of security awareness and training programs	
1.7	Define, Measure, and Report Security Metrics	
1.7.1	Identify Key Performance Indicators (KPI)	
1.7.2	Relate KPIs to the risk position of the organization	
1.7.3	Use metrics to drive security program development and operations	
1.8	Prepare, Obtain, and Administer Security Budget	
1.8.1	Manage and report financial responsibilities	
1.8.2	Prepare and secure annual budget	
1.8.3	Adjust budget based on evolving risks	
1.9	Manage Security Programs	
1.9.1	Build cross-functional relationships	
1.9.2	Identify communication bottlenecks and barriers	
1.9.3	Define roles and responsibilities	
1.9.4	Resolve conflicts between security and other stakeholders	
1.9.5	Determine and manage team accountability	
1.10	Apply Product Development and Project Management Principles	
1.10.1	Describe project lifecycle	
1.10.2	Identify and apply appropriate project management methodology	
1.10.3	Analyze time, scope, and cost relationship	
2	Systems Lifecycle Management	19%

2.1	Manage Integration of Security into System Development Lifecycle (SDLC)	
2.1.1	Integrate information security gates (decision points) and milestones into lifecycle	
2.1.2	Implement security controls into system lifecycle	
2.1.3	Oversee configuration management processes	
2.2	Integrate New Business Initiatives and Emerging Technologies into the Security Architecture	
2.2.1	Participate in development of business case for new initiatives to integrate security	
2.2.2	Address impact of new business initiatives on security	
2.3	Define and Oversee Comprehensive Vulnerability Management Programs (e.g., vulnerability scanning, penetration testing, threat analysis)	
2.3.1	Classify assets, systems, and services based on criticality to business	
2.3.2	Prioritize threats and vulnerabilities	
2.3.3	Oversee security testing	
2.3.4	Mitigate or remediate vulnerabilities based on risk	
2.4	Manage Security Aspects of Change Control	
2.4.1	Integrate security requirements with change control process	
2.4.2	Identify stakeholders	
2.4.3	Oversee documentation and tracking	
2.4.4	Ensure policy compliance	
3	Risk Management	18%
3.1	Develop and Manage a Risk Management Program	
3.1.1	Communicate risk management objectives with risk owners and other stakeholders	
3.1.2	Understand principles for defining risk tolerance	
3.1.3	Determine scope of organizational risk program	
3.1.4	Obtain and verify organizational asset inventory	
3.1.5	Analyze organizational risk management requirements	
3.1.6	Determine the impact and likelihood of threats and vulnerabilities	
3.1.7	Determine countermeasures, compensating and mitigating controls	
3.1.8	Recommend risk treatment options and when to apply them	
3.2	Conduct Risk Assessments (RA)	
3.2.1	Identify risk factors	
3.2.2	Manage supplier, vendor, and third-party risk	
3.2.3	Understand supply chain security management	
3.2.4	Conduct Business Impact Analysis (BIA)	
3.2.5	Manage risk exceptions	
3.2.6	Monitor and report on risk	
3.2.7	Perform cost–benefit analysis	
4	Threat Intelligence and Incident Management	17%
4.1	Establish and Maintain Threat Intelligence Program	
4.1.1	Synthesize relevant data from multiple threat intelligence sources	
4.1.2	Conduct baseline analysis	
4.1.3	Review anomalous behavior patterns for potential concerns	
4.1.4	Conduct threat modeling	
4.1.5	Identify ongoing attacks	
4.1.6	Correlate related attacks	
4.1.7	Create actionable alerting to appropriate resources	
4.2	Establish and Maintain Incident Handling and Investigation Program	
4.2.1	Develop program documentation	
4.2.2	Establish incident response case management process	
4.2.3	Establish Incident Response Team (IRT)	
4.2.4	Understand and apply incident management methodologies	
4.2.5	Establish and maintain incident handling process	
4.2.6	Establish and maintain investigation process	
4.2.7	Quantify and report financial and operational impact of incidents and investigations to stakeholders	
4.2.8	Conduct Root Cause Analysis (RCA)	
5	Contingency Management	10%

5.1	Oversee Development of Contingency Plans (CP)	
5.1.1	Analyze challenges related to the Business Continuity (BC) process (e.g., time, resources, verification)	
5.1.2	Analyze challenges related to the Disaster Recovery (DR) process (e.g., time, resources, verification)	
5.1.3	Analyze challenges related to the Continuity of Operations Plan (COOP)	
5.1.4	Coordinate with key stakeholders	
5.1.5	Define internal and external incident communications plans	
5.1.6	Define incident roles and responsibilities	
5.1.7	Determine organizational drivers and policies	
5.1.8	Reference Business Impact Analysis (BIA)	
5.1.9	Manage third-party dependencies	
5.1.10	Prepare security management succession plan	
5.2	Guide Development of Recovery Strategies	
5.2.1	Identify and analyze alternatives	
5.2.2	Recommend and coordinate recovery strategies	
5.2.3	Assign recovery roles and responsibilities	
5.3	Maintain Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP)	
5.3.1	Plan testing, evaluation, and modification	
5.3.2	Determine survivability and resiliency capabilities	
5.3.3	Manage plan update process	
5.4	Manage Recovery Process	
5.4.1	Declare disaster	
5.4.2	Implement plan	
5.4.3	Restore normal operations	
5.4.4	Gather lessons learned	
5.4.5	Update plan based on lessons learned	
6	Law, Ethics, and Security Compliance Management	14%
6.1	Understand the Impact of Laws and Regulations that Relate to Information Security	
6.1.1	Understand global privacy laws	
6.1.2	Understand legal jurisdictions the organization operates within (e.g., trans-border data flow)	
6.1.3	Understand export laws	
6.1.4	Understand intellectual property laws	
6.1.5	Understand industry regulations affecting the organization	
6.1.6	Advise on potential liabilities	
6.2	Understand Management Issues as Related to the (ISC)2 Code of Ethics	
6.3	Validate Compliance in Accordance with Applicable Laws, Regulations, and Industry Best Practices	
6.3.1	Obtain leadership buy-in	
6.3.2	Select compliance framework(s)	
6.3.3	Implement validation procedures outlined in framework(s)	
6.3.4	Define and utilize security compliance metrics to report control effectiveness and potential areas of improvement	
6.4	Coordinate with Auditors, and Assist with the Internal and External Audit Process	
6.4.1	Prepare	
6.4.2	Schedule	
6.4.3	Perform audit	
6.4.4	Evaluate findings	
6.4.5	Formulate response	
6.4.6	Validate implemented mitigation and remediation actions	
6.5	Document and Manage Compliance Exceptions	