APP®
Associate Protection Professional
Board Certified in Security Management Fundamentals

Associate Protection Professional (APP®) Body of Knowledge

DOMAIN ONE

Security Fundamentals (35%)

TASK 1: Implement and coordinate the organization's security program(s) to protect the organization's assets

Knowledge of

1. Security theory and terminology
2. Project management techniques
3. Security industry standards
4. Protection techniques and methods
5. Security program and procedures assessment
6. Security principles of planning, organization, and control

TASK 2: Implement methods to improve the security program on a continuous basis through the use of auditing, review, and assessment

Knowledge of

1. Data collection and intelligence analysis techniques
2. Continuous assessment and improvement processes
3. Audit and testing techniques

TASK 3: Develop and coordinate external relations programs with public sector law enforcement or other external organizations to achieve security objectives

Knowledge of

1. Roles and responsibilities of external organizations and agencies
2. Local, national, and international public/private partnerships
3. Methods for creating effective working relationships

TASK 4: Develop, implement, and coordinate employee security awareness programs

Knowledge of

1. The nature of verbal and non-verbal communication and cultural considerations
2. Security industry standards
3. Training methodologies
4. Communication strategies, techniques, and methods
5. Security awareness program objectives and metrics

TASK 5: Implement and/or coordinate an investigative program

Knowledge of

1. Report preparation for internal purposes and legal proceedings
2. Components of investigative processes
3. Types of investigations (e.g., incident, misconduct, compliance)
4. Internal and external resources to support investigative functions

TASK 6: Provide coordination, assistance, and evidence such as documentation and testimony to support legal proceedings

Knowledge of

1. Required components of effective documentation (e.g., legal, employee, procedural, policy, compliance)
2. Evidence collection and protection techniques
3. Relevant laws and regulations regarding records management, retention, legal holds, and destruction practices (Note: No country-specific laws will be on the APP exam)

TASK 7: Conduct background investigations for hiring, promotion, and/or retention of individuals

Knowledge of

1. Background investigations and personnel screening techniques
2. Quality and types of information and data sources
3. Criminal, civil, and employment law and procedures

TASK 8: Develop, implement, coordinate, and evaluate policies, procedures, programs and methods to protect individuals in the workplace against human threats (e.g., harassment, violence)

Knowledge of

1. Principles and techniques of policy and procedure development
2. Protection personnel, technology, and processes
3. Regulations and standards governing or affecting the security industry and the protection of people, property, and information
4. Educational and awareness program design and implementation

TASK 9: Conduct and/or coordinate an executive/personnel protection program

Knowledge of

1. Travel security program components
2. Executive/personnel protection program components
3. Protection personnel, technology, and processes

TASK 10: Develop and/or maintain a physical security program for an organizational asset

Knowledge of

1. Resource management techniques
2. Preventive and corrective maintenance for systems
3. Physical security protection equipment, technology, and personnel
4. Security theory, techniques, and processes
5. Fundamentals of security system design

TASK 11: Recommend, implement, and coordinate physical security controls to mitigate security risks

Knowledge of

1. Risk mitigation techniques (e.g., technology, personnel, process, facility design, infrastructure)
2. Physical security protection equipment, technology, and personnel
3. Security survey techniques

TASK 12: Evaluate and integrate technology into security program to meet organizational goals

Knowledge of

1. Surveillance techniques and technology
2. Integration of technology and personnel
3. Plans, drawings, and schematics
4. Information security theory and systems methodology

TASK 13: Coordinate and implement security policies that contribute to an information security program

Knowledge of

1. Practices to protect proprietary information and intellectual property
2. Information protection technology, investigations, and procedures
3. Information security program components (e.g., asset protection, physical security, procedural security, information systems security, employee awareness, and information destruction and recovery capabilities)
4. Information security threats

DOMAIN TWO

Business Operations (22%)

TASK 1: Propose budgets and implement financial controls to ensure fiscal responsibility

Knowledge of

1. Data analysis techniques and cost-benefit analysis
2. Principles of business management accounting, control, and audits
3. Return on Investment (ROI) analysis
4. Fundamental business finance principles and financial reporting
5. Budget planning process
6. Required components of effective documentation (e.g., budget, balance sheet, vendor work order, contracts)

TASK 2: Implement security policies, procedures, plans, and directives to achieve organizational objectives

Knowledge of

1. Principles and techniques of policy/procedure development
2. Guidelines for individual and corporate behavior
3. Improvement techniques (e.g., pilot programs, education, and training)

TASK 3: Develop procedures/techniques to measure and improve departmental productivity

Knowledge of

1. Communication strategies, methods, and techniques
2. Techniques for quantifying productivity/metrics/key performance indicators (KPI)
3. Project management fundamentals tools and techniques
4. Principles of performance evaluations, 360 reviews, and coaching

TASK 4: Develop, implement, and coordinate security staffing processes and personnel development programs in order to achieve organizational objectives

Knowledge of

1. Retention strategies and methodologies
2. Job analysis processes
3. Cross-functional collaboration
4. Training strategies, methods, and techniques
5. Talent management and succession planning
6. Selection, evaluation, and interview techniques for staffing

TASK 5: Monitor and ensure a sound ethical culture in accordance with regulatory requirements and organizational objectives

Knowledge of

1. Interpersonal communications and feedback techniques
2. Relevant laws and regulations
3. Governance and compliance standards
4. Generally accepted ethical principles
5. Guidelines for individual and corporate behavior

TASK 6: Provide advice and assistance in developing key performance indicators and negotiate contractual terms for securityvendors/suppliers

Knowledge of

1. Confidential information protection techniques and methods
2. Relevant laws and regulations
3. Key concepts in the preparation of requests for proposals and bid reviews/evaluations
4. Service Level Agreements (SLA) definition, measurement and reporting
5. Contract law, indemnification, and liability insurance principles
6. Monitoring processes to ensure that organizational needs and contractual requirements are being met
7. Vendor qualification and selection process

DOMAIN THREE

Risk Management (25%)

TASK 1: Conduct initial and ongoing risk assessment processes

Knowledge of

1. Risk management strategies (e.g., avoid, assume/accept, transfer, mitigate)
2. Risk management and business impact analysis methodology
3. Risk management theory and terminology (e.g., threats, likelihood, vulnerability, impact)

TASK 2: Assess and prioritize threats to address potential consequences of incidents

Knowledge of

1. Potential threats to an organization
2. Holistic approach to assessing all-hazard threats
3. Techniques, tools, and resources related to internal and external threats

TASK 3: Prepare, plan, and communicate how the organization will identify, classify, and address risks

Knowledge of

1. Risk management compliance testing (e.g., program audit, internal controls, self-assessment)
2. Quantitative and qualitative risk assessments
3. Risk management standards
4. Vulnerability, threat, and impact assessments

TASK 4: Implement and/or coordinate recommended countermeasures for new risk treatment strategies

Knowledge of

1. Countermeasures
2. Mitigation techniques
3. Cost-benefit analysis methods for risk treatment strategies

TASK 5: Establish a business continuity or continuity of operations plan (COOP)

Knowledge of

1. Business continuity standards
2. Emergency planning techniques
3. Risk analysis
4. Gap analysis

TASK 6: Ensure pre-incident resource planning (e.g., mutual aid agreements, table-top exercises)

Knowledge of

1. Data collection and trend analysis techniques
2. Techniques, tools, and resources related to internal and external threats
3. Quality and types of information and data sources
4. Holistic approach to assessing all-hazard threats

DOMAIN FOUR

Response Management (18%)

TASK 1: Respond to and manage an incident using best practices

Knowledge of

1. Primary roles and duties in an incident command structure
2. Emergency operations center (EOC) management principles and practices

TASK 2: Coordinate the recovery and resumption of operations following an incident

Knowledge of

1. Recovery assistance resources
2. Mitigation opportunities during response and recovery processes

TASK 3: Conduct a post-incident review

Knowledge of

1. Mitigation opportunities during response and recovery processes
2. Post-incident review techniques

TASK 4: Implement contingency plans for common types of incidents (e.g., bomb threat, active shooter, natural disasters)

Knowledge of

1. Short- and long-term recovery strategies
2. Incident management systems and protocols

TASK 5: Identify vulnerabilities and coordinate additional countermeasures for an asset in a degraded state following an incident

Knowledge of

1. Triage/prioritization and damage assessment techniques
2. Prevention, intervention, and response tactics

TASK 6: Assess and prioritize threats to mitigate consequences of incidents

Knowledge of

1. Triage/prioritization and damage assessment techniques
2. Resource management techniques

TASK 7: Coordinate and assist with evidence collection for post-incident review (e.g., documentation, testimony)

Knowledge of

1. Communication techniques and notification protocols
2. Communication techniques and protocols of liaison

TASK 8: Coordinate with emergency services during incident response

Knowledge of

1. Emergency operations center (EOC) concepts and design
2. Emergency operations center (EOC) management principles and practices
3. Communication techniques and protocols of liaison

TASK 9: Monitor the response effectiveness to incident(s)

Knowledge of

1. Post-incident review techniques
2. Incident management systems and protocols

TASK 10: Communicate regular status updates to leadership and other key stakeholders throughout incident

Knowledge of

1. Communication techniques and protocols of liaison
2. Communication techniques and notification protocols

TASK 11: Monitor and audit the plan of how the organization will respond to incidents

Knowledge of

1. Training and exercise techniques
2. Post-incident review techniques