Certified Protection Professional
Board Certified in Security Management

CPP Body of Knowledge

To be awarded the CPP designation, a candidate must pass a comprehensive examination consisting of approximately 225 multiple-choice questions: 200 "live," scoreable questions and up to 25 pre-test questions. Knowledge in seven major areas (domains) is tested.

The importance of each domain, and the tasks, knowledge, and skills within it, determine the specifications of the CPP examination. The relative order of importance of the domains determines the percentage of the total exam questions.

DOMAIN ONE

Security Principles and Practices (22%)

TASK 1: Plan, develop, implement, and manage the organization's security program to protect the organization's assets.

Knowledge of

1. Principles of planning, organization, and control
2. Security theory, techniques, and processes (e.g., artificial intelligence, IoT)
3. Security industry standards (e.g., ASIS/ISO)
4. Continuous assessment and improvement processes
5. Cross-functional organizational collaboration
6. Enterprise Security Risk Management (ESRM)

TASK 2: Develop, manage, or conduct the security risk assessment process.

Knowledge of

1. Quantitative and qualitative risk assessments
2. Vulnerability, threat, and impact assessments
3. Potential security threats (e.g., "all hazards," criminal activity, terrorism, consequential)

TASK 3: Evaluate methods to improve the security program on a continuous basis through the use of auditing, review, and assessment.

Knowledge of

1. Cost-benefit analysis methods
2. Risk management strategies (e.g., avoid, assume/accept, transfer, spread)
3. Risk mitigation techniques (e.g., technology, personnel, process, facility design)
4. Data collection and trend analysis techniques

TASK 4: Develop and manage professional relationships with external organizations to achieve security objectives.

Knowledge of

1. Roles and responsibilities of external organization and agencies
2. Methods for creating effective working relationships
3. Techniques and protocols of liaison
4. Local and national public/private partnerships

TASK 5: Develop, implement, and manage workforce security awareness programs to achieve organizational goals and objectives.

Knowledge of

1. Training methodologies
2. Communication strategies, techniques, and methods
3. Awareness program objectives and program metrics
4. Elements of a security awareness program (e.g., roles and responsibilities, physical risk, communication risk, privacy)

DOMAIN TWO

Business Principles and Practices (15%)

TASK 1: Develop and manage budgets and financial controls to achieve fiscal responsibility.

Knowledge of

1. Principles of management accounting, control, audits, and fiduciary responsibility
2. Business finance principles and financial reporting
3. Return on Investment (ROI) analysis
4. The lifecycle for budget planning purposes

TASK 2: Develop, implement, and manage policies, procedures, plans, and directives to achieve organizational objectives.

Knowledge of

1. Principles and techniques of policy/procedures development
2. Communication strategies, methods, and techniques
3. Training strategies, methods, and techniques
4. Cross-functional collaboration
5. Relevant laws and regulations

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

Knowledge of

1. Techniques for quantifying productivity/metrics/key performance indicators (KPI)
2. Data analysis techniques and cost-benefit analysis
3. Improvement techniques (e.g., pilot/beta testing programs, education, training)

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

Knowledge of

1. Interview techniques for staffing
2. Candidate selection and evaluation techniques
3. Job analysis processes

4. Pre-employment background screening
5. Principles of performance evaluations, 360 reviews, and coaching/mentoring
6. Interpersonal and feedback techniques
7. Training strategies, methodologies, and resources
8. Retention strategies and methodologies
9. Talent management and succession planning

TASK 5: Monitor and ensure an acceptable ethical climate in accordance with regulatory requirements and organizational culture.

Knowledge of

1. Governance standards
2. Guidelines for individual and corporate behavior
3. Generally accepted ethical principles
4. Confidential information protection techniques and methods
5. Legal and regulatory compliance

TASK 6: Develop performance requirements and contractual terms for security vendors/suppliers.

Knowledge of

1. Key concepts in the preparation of requests for proposals and bid reviews/evaluations
2. Service Level Agreement (SLA) terms, metrics, and reporting
3. Contract law, indemnification, and liability insurance principles
4. Monitoring processes to ensure that organizational needs and contractual requirements are being met

DOMAIN THREE

Investigations (9%)

TASK 1: Identify, develop, implement, and manage investigative operations.

Knowledge of

1. Principles and techniques of policy and procedure development
2. Organizational objectives and cross-functional collaboration
3. Types of investigations (e.g., incident, misconduct, compliance, due diligence)
4. Internal and external resources to support investigative functions
5. Report preparation for internal/external purposes and legal proceedings
6. Laws pertaining to developing and managing investigative programs

TASK 2: Manage or conduct the collection, preservation, and disposition of evidence to support investigative actions.

Knowledge of

1. Protection/preservation of crime scene
2. Evidence collection techniques
3. Requirements of chain of custody
4. Methods for preservation/disposition of evidence
5. Laws pertaining to the collection, preservation, and disposition of evidence

TASK 3: Manage or conduct surveillance processes.

Knowledge of

1. Surveillance and counter-surveillance techniques
2. Technology/equipment and personnel to conduct surveillance (e.g., Unmanned Aircraft Systems (UAS), robotics)
3. Laws pertaining to managing surveillance processes

TASK 4: Manage and conduct investigations requiring specialized tools, techniques, and resources.

Knowledge of

1. Financial and fraud related crimes
2. Intellectual property and espionage crimes
3. Crimes against property (e.g., arson, vandalism, theft, sabotage)
4. Cybercrimes (e.g., distributed denial of service (DDoS), phishing, ransomware)
5. Crimes against persons (e.g., workplace violence, human trafficking, harassment)

TASK 5: Manage or conduct investigative interviews.

Knowledge of

6. Interview and interrogation techniques
7. Techniques for detecting deception
8. Non-verbal communication and cultural considerations
9. Rights of interviewees
10. Required components of written statements
11. Legal considerations pertaining to managing investigative interviews

TASK 6: Provide support to legal counsel in actual or potential criminal or civil proceedings.

Knowledge of

1. Statutes, regulations, and case law governing or affecting the security industry and the protection of people, property, and information
2. Criminal law and procedures
3. Civil law and procedures
4. Employment law (e.g., confidential information, wrongful termination, discrimination, harassment)

DOMAIN FOUR

Personnel Security (11%)

TASK 1: Develop, implement, and manage background investigation processes for hiring, promotion, and retention of individuals.

Knowledge of

1. Background investigations and personnel screening techniques
2. Quality and types of information sources (e.g., open source, social media, government databases, credit reports)
3. Screening policies and guidelines
4. Laws and regulations pertaining to personnel screening

TASK 2: Develop, implement, manage, and evaluate policies and procedures to protect individuals in the workplace against human threats (e.g., harassment, violence, active assailant).

Knowledge of

1. Protection techniques and methods
2. Threat assessment
3. Prevention, intervention, and response tactics
4. Educational and awareness program design and implementation
5. Travel security (e.g., flight planning, global threats, consulate services, route selection, contingency planning)
6. Industry/labor regulations and applicable laws
7. Organizational efforts to reduce employee substance abuse

TASK 3: Develop, implement, and manage executive protection programs.

Knowledge of

1. Executive protection techniques and methods
2. Threat analysis
3. Liaison and resource management techniques
4. Selection, costs, and effectiveness of proprietary and contract executive protection personnel

DOMAIN FIVE

Physical Security (16%)

TASK 1: Conduct facility surveys to determine the current status of physical security.

Knowledge of

1. Security protection equipment and personnel (e.g., Unmanned Aircraft Systems (UAS), robotics)
2. Survey techniques (e.g., document review, checklist, onsite visit, stakeholder interviews)
3. Building plans, drawings, and schematics
4. Risk assessment techniques
5. Gap analysis

TASK 2: Select, implement, and manage physical security strategies to mitigate security risks.

Knowledge of

1. Fundamentals of security system design
2. Countermeasures (e.g., policies, technology, procedures)
3. Budgetary projection development process (e.g., technology, hardware, labor)
4. Bid package development and evaluation process
5. Vendor qualification and selection process
6. Testing procedures and final acceptance (e.g., commissioning, factory acceptance test)
7. Project management techniques
8. Cost-benefit analysis techniques
9. Labor-technology relationship

TASK 3: Assess the effectiveness of physical security measures by testing and monitoring.

Knowledge of

1. Protection personnel, hardware, technology, and processes
2. Audit and testing techniques (e.g., operation testing)
3. Predictive, preventive, and corrective maintenance

DOMAIN SIX

Information Security (14%)

TASK 1: Conduct surveys to evaluate current status of information security programs.

Knowledge of

1. Elements of an information security program, including physical security; procedural security; information systems security; employee awareness; and information destruction and recovery capabilities.
2. Survey techniques
3. Quantitative and qualitative risk assessments
4. Risk mitigation strategies (e.g., technology, personnel, process, facility design)
5. Cost-benefit analysis methods
6. Protection technology, security threats equipment, and procedures (e.g., interoperability)
7. Information security threats
8. Integration of facility and system plans, drawings, and schematics

TASK 2: Develop policies and procedures to ensure information is evaluated and protected against vulnerabilities and threats.

Knowledge of

1. Principles of information security management
2. Information security theory and terminology
3. Information security industry standards (e.g., ISO, PII, PCI)
4. Laws and regulations regarding records management including collection, retention, legal holds, and disposition practices (e.g., General Data Protection Regulation (GDPR), biometric information)
5. Practices to protect proprietary information and intellectual property
6. Information protection measures including security processes, physical access systems, and data management

TASK 3: Implement and manage an integrated information security program

Knowledge of

7. Information security including confidentiality, integrity, and availability
8. Information security systems methodology
9. Authentication techniques (e.g., multi-factor, biometrics)
10. Continuous evaluation and improvement programs
11. Ethical hacking and penetration testing techniques and practices
12. Encryption and data masking techniques (e.g., cryptography)
13. Systems integration techniques (e.g., interoperability, licensing, networking)
14. Cost-benefit analysis methodology
15. Project management techniques
16. Budget review process (e.g., system development lifecycle)
17. Vendor evaluation and selection process
18. Final acceptance and testing procedures
19. Protection technology and forensic investigations
20. Training and awareness programs to mitigate threats and vulnerabilities (e.g., phishing, social engineering, ransomware, insider threats)

DOMAIN SEVEN

Crisis Management (13%)

TASK 1: Assess and prioritize threats to mitigate potential consequences of incidents.

Knowledge of

1. Threats by type, likelihood of occurrence, and consequences
2. "All hazards" approach to assessing threats (e.g., natural disaster, chemical, biological, radiological, nuclear, explosives (CBRNE))
3. Cost-benefit analysis
4. Mitigation strategies
5. Risk management and business impact analysis methodology
6. Business continuity standards (e.g., ASIS ORM.1, ISO 22301)

TASK 2: Prepare and plan how the organization respond to incidents.

Knowledge of

1. Resource management techniques (e.g., mutual aid agreements, MOUs)
2. Emergency planning techniques
3. Triage and damage assessment techniques
4. Communication techniques and notification protocols (e.g. interoperability, common operating terms, emergency notification system)
5. Training and exercise techniques (e.g., tabletop and full-scale exercises)
6. Emergency operations center (EOC) concepts and design
7. Primary roles and duties in an Incident Command Structure (ICS) (e.g., information dissemination, liaison, Public Information Officer (PIO))

TASK 3: Respond to and manage an incident.

Knowledge of

1. Resource allocation
2. Emergency Operations Centre (EOC) management principles and practices
3. Incident management systems and protocols

TASK 4: Manage incident recovery and resumption of operations.

Knowledge of

1. Resource management
2. Short- and long-term recovery strategies
3. Recovery assistance resources (e.g., mutual aid, employee assistance program (EAP), counseling)
4. Mitigation opportunities in the recovery process