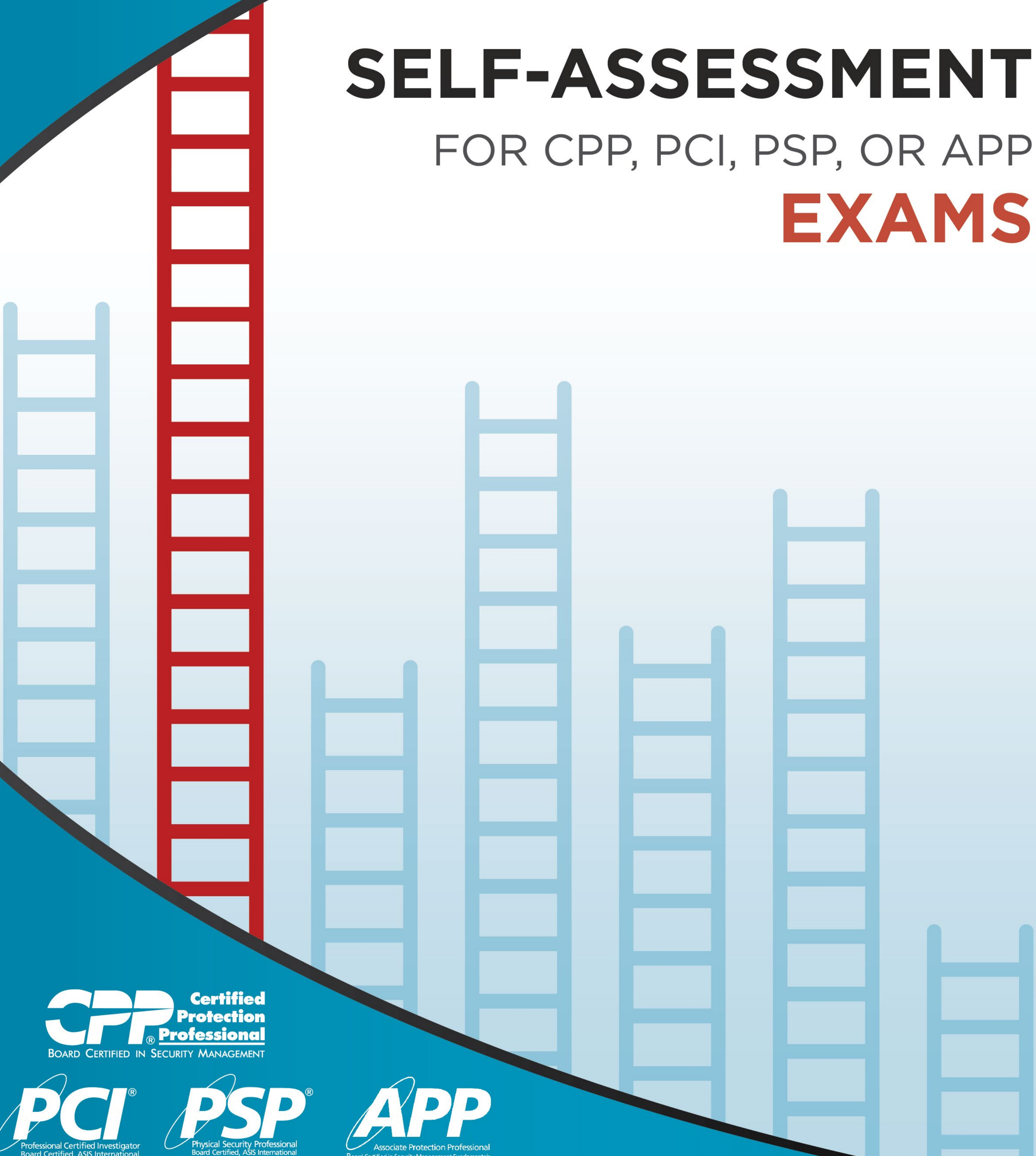
ASIS INTERNATIONAL
Advancing Security Worldwide®

2019



SELF-ASSESSMENT

FOR CPP, PCI, PSP, OR APP

EXAMS

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

PCI®
Professional Certified Investigator
Board Certified, ASIS International

PSP®
Physical Security Professional
Board Certified, ASIS International

APP
Associate Protection Professional
Board Certified in Security Management Fundamentals

ASIS International administers *CPP, PCI, PSP, and APP exams* to assist security professionals who wish to attain these designations. ASIS International provides this complimentary publication to encourage security professionals to use it for individual or group study.

This handbook is published as an electronic document to dynamically change with modifications in the CPP, PCI, PSP, and APP exams and exam structure. Ensure you have the most up-to-date version by visiting **asisonline.org/certification**.

This handbook was created on May 1, 2019. It replaces all previous editions and the formerly ASIS-published *CPP Study Guide*, *PCI Study Guide*, *PSP Study Guide,* and *Preparing for the CPP, PCI, and PSP Exams Handbook*. For information on how to apply for ASIS certification, please download the **Certification Handbook.**

Contents

Introduction

ASIS International (ASIS) is dedicated to ensuring that the Certified Protection Professional (CPP)®, Professional Certified Investigator (PCI)®, Physical Security Professional (PSP)®, and Associate Protection Professional (APP) designations are highly regarded throughout the world. The rigor of the process and the evaluation of candidates are critical in maintaining this prestige. There are no shortcuts and no easy ways to prepare. A candidate must work diligently and with purpose to succeed.

The Role of the PCB

ASIS certification programs are Board Certified. The ASIS Professional Certification Board (PCB) manages the certification programs by assuring that standards are developed and maintained, quality assurance is in place and that the test accurately reflects the duties and responsibilities of security professionals in the areas of security management, investigations and physical security.

The Value of the CPP, PCI, PSP, and APP Designations

The first and most rigorous component of becoming certified is meeting the eligibility requirements. As with most board certifications, the qualifications are strict and require *substantial experience.* While many candidates place considerable emphasis on the exam, **the eligibility requirements set board certification apart from a course certificate or a degree program.** Only those candidates who meet the rigors of the eligibility requirements may sit for the exam.

The CPP, PCI, PSP, and APP exams are assessments of a candidate's depth of knowledge. An item writing team monitored by the ASIS Professional Certification Board (PCB), a group of volunteer leaders within ASIS, constructs the exams. The exam items, or questions, relate to specific knowledge, skills, and tasks under several domains. The item writing team references each of the questions [items] to concepts and content in the resources comprising the current certification references. **See the Certification website for current listings of references or reading materials.**

The PCB and its teams develop the exam under strict confidence. The American National Standards Institute (ANSI) closely monitors the exam security process and authorizes ASIS as an accredited Certification Provider. All exam items are secure in an item bank.

Candidates sitting for the exam must sign a non-disclosure agreement before taking the exam. Candidates violating the agreement may lose their eligibility for the CPP, PCI, PSP, and APP designation.

A Dynamic Designation

The domains and knowledge statements periodically change to reflect the current knowledge and skills expected of a security professional. At least once every five years, the PCB conducts a survey of current designation holders to determine changes in the industry. The exam is modified and questions added to incorporate any changes. These changes are usually minor and do not require major shifts in study materials.

What the PCB makes available to the public are the domains, tasks, and knowledge statements with their definitions. These statements make up the content mapping of the exam.

The Role of ASIS Learning

ASIS Learning has no more insider access to testing information than the public. ASIS volunteer members working with ASIS Learning are not members of the PCB, but they are experts in the field and have earned their Board Certifications. ASIS expects that the study materials produced by this group of security professionals are a reflection of the material developed by the PCB. These volunteer members construct study materials by reviewing domains, tasks, and knowledge statements and finding references in the resources comprising certification references (recommended reading material).

The ASIS Certification Department does not participate in review program activities or publications, case studies, exercises, practice exams, or assessment exams. Such materials or guides may be available from the review program sponsors.

Review program activities are tools to help review the concepts covered on the exams, but they are not references.

Assessment questions developed by review program faculty may also be subject to different guidelines. While these programs cover the general areas of the certification domains, they are not linked to test questions. Assessment questions used on any practice exams are never the same as the proctored certification exam. Do not underestimate the difficulty of the exams—passing an assessment test does not guarantee a passing score on the certification exam. It is important to invest the required time to study and grasp the ***concepts*** covered in the domains of security.

Candidates using any study material developed by ASIS International or ASIS chapters must understand the importance of reviewing the recommended reference resources. Questions or items used in any ASIS study material are not part of the actual exam. Any similarity to actual exam questions is purely coincidental.

Eligibility Requirements

CPP Exam Eligibility Requirements

Those who earn the CPP are ASIS Board Certified in security management. This credential provides demonstrable proof of knowledge and management skills in several key domains of security. CPP candidates must meet the following requirements:

a. Nine years of security work experience, with at least three of those years in responsible charge of a security function*

-or-

b. A bachelor's degree or higher and seven years of security work experience, with at least three of those years in responsible charge of a security function*

PCI Exam Eligibility Requirements

Those who earn the PCI are ASIS Board Certified in investigations. This credential provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. PCI candidates must meet the following requirements:

a. A high school diploma or GED equivalent and five years of investigations experience, including at least two years in case management**

PSP Exam Eligibility Requirements

Those who earn the PSP are ASIS Board Certified in physical security. This credential provides demonstrable knowledge and experience in threat assessment and risk analysis; integrated physical security systems; and the appropriate identification, implementation, and ongoing evaluation of security measures. PSP candidates must meet the following requirements:

a. A high school diploma, GED equivalent, or associate degree and six years of progressive physical security experience***

-or-

b. A bachelor's degree or higher and four years of progressive physical security experience***

* "Responsible charge" is defined as the charge exercised by an individual in a management position who makes decisions for the successful completion of objectives without reliance upon directions from a superior as to specific methods. However, an applicant need not have held a supervisory position, as long as the positions on which the application relies have specifically included responsibility for independent decisions or actions. If "responsible charge" is not based on supervisory responsibilities, then security program management responsibilities and duties must be clearly shown. Generally, this excludes such positions as patrol officer or the equivalent.

** "Investigation" is the logical collection of information through inquiry and examination for the purpose of developing evidence leading to problem resolution. "Case management" is the coordination and direction of an investigation utilizing various disciplines and resources, the findings of which would be assessed to establish the facts/findings of the investigation as a whole; the management process of investigation.

*** "Physical security" is defined as the various physical measures designed to safeguard personnel, property, and information. "Progressive" means that the experience has included increasingly more difficult assignments or responsibilities over the work period.

APP Exam Eligibility Requirements

The Associate Protection Professional (APP) designation is intended for those with one to four years of security management experience. The exam will measure the professional's knowledge of security management fundamentals, business operations, risk management, and response management. The candidate needs a combination of experience and education to apply for the APP.

Security Management Experience	Education
One year	Master's degree (or international equivalent) in Security Management
Two years	Bachelor's degree (or international equivalent) in Security Management
Three years	Bachelor's degree (or international equivalent) in any discipline
Four years	No higher education degree

For complete information on application policies, visit the ASIS International website's Certification section (asisonline.org) or email: **certification@asisonline.org**.

Creating a Study Plan

Self-Assessment for CPP, PCI, PSP, and APP Exams provides assistance for all types of learners with varying resources for study. Candidates should determine the best study tools and method for their success.

What should you expect?

- Start early
  - Plan on more than 250 study hours in a six- to eight-month period.
  - There is direct correlation to passing the exam and the time spent studying.

- Schedule time to study
  - Study as if the designation is a job requirement. Studying is an obligation.
  - Put time aside each week as part of your regular schedule.
  - Set responsible blocks of time—two to three hours.

The strongest predictor of success is study time. Putting in the hours makes a difference. Pass rates increase significantly for those putting in 250 hours. However, those candidates studying more than 360 hours have a lower pass rate. Knowing what to study and knowing what to review will determine success.

An exam consists of multiple-choice questions covering tasks, knowledge, and skills in the domains identified by CPPs, PCIs, PSPs, and APPs as the major areas involved in security management, investigations and case management, or physical security. Candidates are encouraged to refer to the references or their reading materials as they prepare for the exam. After carefully reviewing the domains of study and identifying individual learning needs, candidates may use additional references and study opportunities as necessary.

Conduct a Self-Assessment

Any educator or security professional will tell you that it is important to do an assessment before you try to design an effective study plan. Self-assessments are nothing more than understanding what you know versus what you do not know. It does not require a formal evaluation. Without the assessment, how do you know what topics you need to study?

An assessment at the start will save you time, and it gives you a study map toward succeeding.

- Make effective use of your time by studying areas of weakness.
- Review areas of strength, but do not over analyze familiar content, because it will waste valued time.

Remember, the domains, tasks, and knowledge statements found on each exam are developed by security managers working in the field. These are considered best practices by your peers but may differ from how you conduct security-related business in your own organization.

An Assessment Tool

ASIS has constructed the following Self-Assessment tool using the current exam content as the elements within the assessment tool. For those with interest in the CPP, the self-assessment begins on page 6. The PCI assessment starts on page 15. The PSP assessment begins on page 19. The APP assessment begins on page 24.

Consider each task and knowledge statement in the assessment for your depth of understanding of the subject. Score your knowledge of each task on a 1-to-5 scale, with 1 "I do not know what this task is" to 5 "I can clearly explain the task to someone else." The low scores are the tasks and domains that you should study thoroughly.

Self-Assessment Tool for Creating a Study Plan

Rate Understanding					Certified Protection Professional BOARD CERTIFIED IN SECURITY MANAGEMENT	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						I. Security Principles and Practices (21%)		
					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		
					3.	Security industry standards		
					4.	Continuous assessment and improvement processes		
					5.	Cross-functional organizational collaboration		
					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)		
					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 external relations programs with public sector law enforcement or other 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 (e.g., Fusion Centers)		

Rate Understanding					CPP Certified Protection Professional Board Certified in Security Management	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 5.	**Develop, implement, and manage employee 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)		
						II. Business Principles and Practices (13%)		
					Task 1.	**Develop and manage budgets and financial controls to achieve fiscal responsibility.** Knowledge of:		
					1.	Principles of management accounting, control, and audits		
					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)		

Rate Understanding					CPP Certified Protection Professional® Board Certified in Security Management	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					2.	Data analysis techniques and cost-benefit analysis		
					3.	Improvement techniques (e.g., pilot programs, education and 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		
					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 a sound, ethical climate in accordance with regulatory requirements and the organization's directives and standards to support and promote proper business practices.** Knowledge of:		
					1.	Good 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.	**Provide advice and assistance to management and others in developing performance requirements and contractual terms for security vendors/suppliers.** Knowledge of:		
					1.	Key concepts in the preparation of requests for proposals and bid reviews/evaluation		
					2.	Service Level Agreements (SLA) definition, measurement, and reporting		
					3.	Contract law, indemnification, and liability insurance principles		
					4.	Monitoring processes to ensure that organizational needs and contractual requirements are being met		

Rate Understanding					Certified Protection Professional ® Board Certified in Security Management	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
III. Investigations (10%)								
					Task 1. Knowledge of:	**Identify, develop, implement, and manage investigative functions.**		
					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)		
					4.	Internal and external resources to support investigative functions		
					5.	Report preparation for internal purposes and legal proceedings		
					6.	Laws pertaining to developing and managing investigative programs		
					Task 2. Knowledge of:	**Manage or conduct the collection and preservation of evidence to support investigation actions.**		
					1.	Evidence collection techniques		
					2.	Protection/preservation of crime scene		
					3.	Requirements of chain of custody		
					4.	Methods for preservation of evidence		
					5.	Laws pertaining to the collection and preservation of evidence		
					Task 3. Knowledge of:	**Manage or conduct surveillance processes.**		
					1.	Surveillance techniques		
					2.	Technology/equipment and human resources		
					3.	Laws pertaining to managing surveillance processes		
					Task 4. Knowledge of:	**Manage and conduct investigations requiring specialized tools, techniques, and resources.**		
					1. 2. 3. 4.	Financial and fraud related crimes Intellectual property and industrial espionage crimes Arson and property crimes Cybercrimes		
					Task 5. Knowledge of:	**Manage or conduct investigative interviews.**		
					1.	Methods and techniques of eliciting information		

Rate Understanding					CPP Certified Protection Professional ® BOARD CERTIFIED IN SECURITY MANAGEMENT	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					2.	Techniques for detecting deception		
					3.	The nature of non-verbal communication and cultural considerations		
					4.	Rights of interviewees		
					5.	Required components of written statements		
					6.	Laws pertaining to managing investigative interviews		
					Task 6. Knowledge of:	**Provide coordination, assistance, and evidence such as documentation and testimony to support legal counsel in actual or potential criminal and/or civil proceedings**		
					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., wrongful termination, discrimination, and harassment)		
						IV. Personnel Security (12%)		
					Task 1. Knowledge of:	**Develop, implement, and manage background investigations for hiring, promotion, or retention of individuals.**		
					1.	Background investigations and personnel screening techniques		
					2.	Quality and types of information sources		
					3.	Screening policies and guidelines		
					4.	Laws and regulations pertaining to personnel screening		
					Task 2. Knowledge of:	**Develop, implement, manage, and evaluate policies, procedures, programs and methods to protect individuals in the workplace against human threats (e.g., harassment, violence).**		
					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 programs		
					6.	Laws, government, and labor regulations		
					7.	Organizational efforts to reduce employee substance abuse		

Rate Understanding					Certified Protection Professional ® Board Certified in Security Management	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 3.	**Develop, implement, and manage executive protection programs.** Knowledge of:		
					1.	Executive protection techniques and methods		
					2.	Risk analysis		
					3.	Liaison and resource management techniques		
					4.	Selection, costs, and effectiveness of proprietary and contract executive protection personnel		
						V. Physical Security (25%)		
					Task 1.	**Conduct facility surveys to determine the current status of physical security.** Knowledge of:		
					1.	Security protection equipment and personnel		
					2.	Survey techniques		
					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		
					3.	Budgetary projection development process		
					4.	Bid package development and evaluation process		
					5.	Vendor qualification and selection process		
					6.	Final acceptance and testing procedures		
					7.	Project management techniques		
					8.	Cost-benefit analysis techniques		
					9.	Labor-technology relationship		
					Task 3.	**Assess the effectiveness of the security measures by testing and monitoring.** Knowledge of:		
					1.	Protection personnel, technology, and processes		
					2.	Audit and testing techniques		
					3.	Preventive and corrective maintenance for systems		

Rate Understanding					Certified Protection Professional Board Certified in Security Management	Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
VI. Information Security (9%)								
					Task 1.	**Conduct surveys of information asset facilities, processes, systems, and services to evaluate current status of information security program.** 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, equipment, and procedures		
					7.	Information security threats		
					8.	Building and system plans, drawings, and schematics		
					Task 2.	**Develop and implement policies and procedures to ensure information is evaluated and protected against all forms of unauthorized/inadvertent access, use, disclosure, modification, destruction, or denial.** Knowledge of:		
					1.	Principles of management		
					2.	Information security theory and terminology		
					3.	Information security industry standards (e.g., ISO, PII, PCI)		
					4.	Relevant laws and regulations regarding records management, retention, legal holds, and destruction practices		
					5.	Practices to protect proprietary information and intellectual property		
					6.	Protection measures, equipment, and techniques; including information security processes, systems for physical access, data control, management, and information destruction		

Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 3.	**Develop and manage a program of integrated security controls and safeguards to ensure information asset protection including confidentiality, integrity, and availability.** Knowledge of:		
					1.	Elements of information asset protection including confidentiality, integrity, and availability, authentication, accountability, and audit ability of sensitive information and associated information technology resources, assets, and investigations		
					2.	Information security theory and systems methodology		
					3.	Multi-factor authentication techniques		
					4.	Threats and vulnerabilities assessment and mitigation		
					5.	Ethical hacking and penetration testing techniques and practices		
					6.	Encryption and data masking techniques		
					7.	Systems integration techniques		
					8.	Cost-benefit analysis methodology		
					9.	Project management techniques		
					10.	Budget development process		
					11.	Vendor evaluation and selection process		
					12.	Final acceptance and testing procedures, information systems, assessment, and security program documentation		
					13.	Protection technology, investigations, and procedures		
					14.	Training and awareness methodologies and procedures		
Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						VII. Crisis Management (10%)		
					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		
					3.	Cost-benefit analysis		
					4.	Mitigation strategies		
					5.	Risk management and business impact analysis methodology		
					6.	Business Continuity standards (e.g., ISO 22301)		

Rate Understanding					Certified Protection Professional® BOARD CERTIFIED IN SECURITY MANAGEMENT Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					Task 2. Prepare and plan how the organization will respond to incidents. Knowledge of:		
					1. Resource management techniques		
					2. Emergency planning techniques		
					3. Triage and damage assessment techniques		
					4. Communication techniques and notification protocols		
					5. Training and exercise techniques		
					6. Emergency operations center (EOC) concepts and design		
					7. Primary roles and duties in an incident command structure		
					Task 3. Respond to and manage an incident. Knowledge of:		
					1. Resource management techniques		
					2. EOC management principles and practices		
					3. Incident management systems and protocols		
					Task 4. Recover from incidents by managing the recovery and resumption of operations. Knowledge of:		
					1. Resource management techniques		
					2. Short and long-term recovery strategies		
					3. Recovery assistance resources		
					4. Mitigation opportunities in the recovery process		

CPP Exam Domains

Security Principles and Practices	21%
Business Principles and Practices	13%
Investigations	10%
Personnel Security	12%
Physical Security	25%
Information Security	9%
Crisis Management	10%

Rate Understanding					PCI® Professional Certified Investigator Board Certified, ASIS International	Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						I. Case Management (35%)		
					Task 1. Knowledge of:	**Analyze case for applicable ethical conflicts.**		
					1.	Nature/types/categories of ethical issues related to cases (fiduciary, conflict of interest, attorney-client)		
					2.	The role of laws, codes, regulations and organizational governance in conducting investigations		
					Task 2. Knowledge of:	**Analyze and assess case elements, strategies and risks.**		
					1.	Case categories (computer, white collar, financial, criminal, workplace violence)		
					2.	Qualitative and quantitative analytical methods and tools		
					3.	Strategic/operational analysis		
					4.	Criminal intelligence analysis		
					5.	Risk identification and impact		
					6.	ASIS Workplace Violence standard		
					Task 3. Knowledge of:	**Determine investigative goals and develop strategy by reviewing procedural options.**		
					1.	Case flow		
					2.	Negotiation process		
					3.	Investigative methods		
					4.	Cost-benefit analysis		
					Task 4. Knowledge of:	**Determine and manage investigative resources necessary to address case objectives.**		
					1.	Quality assurance process		
					2.	Chain of custody procedures		
					3.	Resource requirements and allocation (e.g., personnel, equipment, time, budget)		
					Task 5. Knowledge of:	**Identify, evaluate and implement investigative process improvement opportunities.**		
					1.	Internal review (e.g., management, legal, human resources)		
					2.	External review (e.g., regulatory bodies, accreditation agency		
					3.	Liaison resources		
					4.	Root cause analysis and process improvement techniques		

Rate Understanding					PCI Professional Certified Investigator Board Certified, ASIS International	Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					II.	**Investigative Techniques and Procedures (50%)**		
					Task 1. Knowledge of:	**Conduct surveillance by physical, behavioral and electronic means in order to obtain relevant information.**		
					1.	Types of surveillance		
					2.	Surveillance equipment		
					3.	Pre-surveillance routine		
					4.	Procedures for documenting surveillance activities		
					Task 2. Knowledge of:	**Conduct interviews of individuals to obtain relevant information.**		
					1.	Interview techniques		
					2.	Indicators of deception (e.g., non-verbal communication)		
					3.	Subject statement documentation		
					Task 3. Knowledge of:	**Collect and preserve objects and data for assessment and analysis.**		
					1.	Forensic opportunities and resources		
					2.	Requirements of chain of custody		
					3.	Methods/procedures for seizure of various types of evidence		
					4.	Methods/procedures for preserving various types of evidence		
					5.	Concepts and principles of digital forensics		
					6.	Retrieval, storage, and documentation of digital equipment		
					7.	Concepts and principles of computer operations and digital media		
					Task 4. Knowledge of:	**Conduct research by physical and electronic means to obtain relevant information.**		
					1.	Methods of research using physical resources		
					2.	Methods of research using information technology		
					3.	Methods of analysis of research results		
					4.	Research documentation		
					5.	Information sources (e.g., government, proprietary, open)		
					6.	Digital media capabilities		

Rate Understanding					Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					Task 5. Collaborate with and obtain information from other agencies and organizations possessing relevant information. Knowledge of:		
					1. External information sources		
					2. Liaison techniques		
					3. Techniques for integrating and synthesizing eternal information		
					Task 6. Use special investigative techniques to obtain relevant information. Knowledge of:		
					1. Concepts and methods of polygraph examinations		
					2. Concepts, principles and methods of video/audio recordings		
					3. Concepts, principles and methods of forensic analysis (e.g., writing, documents, fingerprints, DNA, biometrics, chemicals, fluids, etc.)		
					4. Concepts, principles and methods of undercover investigations		
					5. Concepts, principles and methods of threat assessment		
					6. Use of confidential sources		
					7. Concepts, principles and methods of applying IT hardware and software tools		

Rate Understanding						Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					III. Case Presentation (15%)			
					Task 1. Knowledge of:	**Prepare report to substantiate findings.**		
					1.	Critical elements and format of an investigative report		
					2.	Investigative terminology		
					3.	Logical sequencing of information		
					Task 2. Knowledge of:	**Prepare and present testimony**		
					1.	Types of testimony		
					2.	Preparation for testimony		

PCI Exam Domains

Case Management	35%
Investigative Techniques and Procedures	50%
Case Presentation	15%

Rate Understanding					PSP Physical Security Professional Board Certified, ASIS International	Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					I. Physical Security Assessment (34%)			
					Task 1.	**Develop a physical security assessment plan.** Knowledge of:		
					1.	Risk assessment models and considerations		
					2.	Qualitative and quantitative assessment methods		
					3.	Key areas of the facility or assets that may be involved in assessment		
					4.	Types of resources needed for assessment		
					Task 2.	**Identify assets to determine their value, criticality, and loss impact.** Knowledge of:		
					1.	Definitions and terminology related to assets, value, loss impact and criticality		
					2.	The nature and types of assets (tangible and intangible)		
					3.	How to determine value of various types of assets and business operations		
					Task 3.	**Assess the nature of the threats so that the scope of the problem can be determined.** Knowledge of:		
					1.	The nature, types, severity, and likelihood of threats and hazards (e.g., natural disasters, cyber, criminal events, terrorism, socio-political, cultural)		
					2.	Operating environment (e.g., geography, socio-economic environment, criminal activity)		
					3.	Potential impact of external organizations (e.g., competitors, supply chain, organizations in immediate proximity) on facility's security program		
					4.	Other external factors (e.g., legal, loss of reputation, economic) and their impact on the facility's security program		
					Task 4.	**Conduct an assessment to identify and quantify vulnerabilities of the organization.** Knowledge of:		
					1.	Relevant data and methods for collection (e.g., security survey, interviews, past incident reports, crime statistics, employee issues, issues experienced by other similar organizations)		
					2.	Qualitative and quantitative methods for assessing vulnerabilities to probable threats and hazards		
					3.	Existing equipment, physical security systems, personnel, and procedures		
					4.	Effectiveness of security technologies and equipment currently in place		
					5.	Interpretation of building plans, drawings, and schematics		
					6.	Applicable standards/regulations/codes and where to find them		
					7.	Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security		

Rate Understanding					PSP	Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 5. Knowledge of:	**Perform a risk analysis so that appropriate countermeasures can be developed.**		
					1.	Risk analyses strategies and methods		
					2.	Risk management principles		
					3.	Methods for analysis and interpretation of collected data		
					4.	Threat and vulnerability identification		
					5.	Loss event profile analyses		
					6.	Appropriate countermeasures related to specific threats		
					7.	Cost benefit analysis (e.g. return on investment (ROI) analysis, total cost of ownership		
					8.	Legal issues related to various countermeasures/security applications (e.g., video surveillance, privacy issues, personally identifiable information)		
						II. Application, Design, and Integration of Physical Security Systems (34%)		
					Task 1. Knowledge of:	**Establish security program performance requirements.**		
					1.	Design constraints (e.g. regulations, budget, cost, materials, equipment, and system compatibility)		
					2.	Applicability of risk analysis results		
					3.	Relevant security terminology and concepts		
					4.	Applicable codes, standards and guidelines		
					5.	Functional requirements (e.g., system capabilities, features, fault tolerance)		
					6.	Performance requirements (e.g., technical capability, systems design capabilities)		
					7.	Operational requirements (e.g., policies, procedures, staffing)		
					8.	Success metrics		
					Task 2. Knowledge of:	**Determine appropriate physical security measures.**		
					1.	Structural security measures (e.g., barriers, lighting, locks, blast migration, ballistic protection)		
					2.	Crime prevention through environmental design (CPTED) concepts		
					3.	Electronic security systems (e.g., access control, video surveillance, intrusion detection)		
					4.	Security staffing (e.g., officers, technicians, management)		
					5.	Personnel, package, and vehicle screening		
					6.	Emergency notification systems		

Rate Understanding					PSP	Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					7.	Principles of data storage and management		
					8.	Principles of network infrastructure and network security		
					9.	Security audio communications (e.g., radio, telephone, intercom, IP audio)		
					10.	Systems monitoring and display (control centers/consoles)		
					11.	Systems redundancy alternative power sources (e.g., battery, UPS, generators, surge protection)		
					12.	Signal and data transmission methods		
					13.	Considerations regarding Personally Identifiable Information (physical/logical/biometric)		
					14.	Visitor management systems and circulation control		
					Task 3. Knowledge of:	**Design physical system and prepare construction and procurement documentation.**		
					1.	Design phases (pre-design, schematic design, design development, construction documentation)		
					2.	Design elements (calculations, drawings, specifications, review of manufacturer's submittals and technical data)		
					3.	Construction specification standards (e.g., Construction Specifications Institute, owner's equipment standards, American Institute of Architects MasterSpec)		
					4.	Systems integration (technical approach, connecting with non-security systems)		
					5.	Project management concepts		
					6.	Scheduling (e.g., Gantt charts, PERT charts, milestones, and objectives)		
					7.	Cost estimation and cost-benefit analysis of design options		
					8.	Value engineering		

Rate Understanding					PSP® Physical Security Professional Board Certified, ASIS International	Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					III.	**Implementation of Physical Security Measures (32%)**		
					Task 1.	**Outline criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation.** Knowledge of:		
					1.	Bid package components		
					2.	Criteria for evaluation of bids		
					3.	Technical compliance criteria		
					4.	Ethics in contracting		
					Task 2.	**Procure system and implement recommended solutions to solve problems identified.** Knowledge of:		
					1.	Project management functions and processes throughout the system life cycle		
					2.	Vendor pre-qualification (interviews and due diligence)		
					3.	Procurement process		
					Task 3.	**Conduct final acceptance testing and implement/provide procedures for ongoing monitoring and evaluation of the measures.** Knowledge of:		
					1.	Installation/maintenance inspection techniques		
					2.	Systems integration		
					3.	Commissioning		
					4.	Installation problem resolution (punch lists)		
					5.	Systems configuration management		
					6.	Final acceptance testing criteria		
					7.	End-user training requirements		
					Task 4.	**Implement procedures for ongoing monitoring and evaluation throughout the system life cycle** Knowledge of:		
					1.	Maintenance inspection techniques		
					2.	Test and acceptance criteria		
					3.	Warranty types		
					4.	Ongoing maintenance, inspections and upgrade		
					5.	Ongoing training requirements		
					6.	Systems disposal and replacement processes		

Rate Understanding					Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					Task 5. Develop requirements for personnel involved in support of the security program. Knowledge of:		
					1. Roles, responsibilities and limitations of security personnel (including proprietary (in-house) and contract security staff)		
					2. Human resource management		
					3. Security personnel training, development and certification		
					4. General, post and special orders		
					5. Security personnel uniforms and equipment		
					6. Personnel performance review and improvement processes		
					7. Methods to provide security awareness training and education for non-security personnel		

PSP Exam Domains

Physical Security Assessment	34%
Application, Design, and Integration of Physical Security Systems	34%
Implementation of Physical Security Measures	32%

Rate Understanding					APP	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						I. Security Fundamentals (35%)		
					Task 1. Knowledge of:	**Implement and coordinate the organization's security program(s) to protect the organization's assets**		
					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. Knowledge of:	**Implement methods to improve the security program on a continuous basis through the use of auditing, review, and assessment**		
					1.	Data collection and intelligence analysis techniques		
					2.	Continuous assessment and improvement processes		
					3.	Audit and testing techniques		
					Task 3. Knowledge of:	**Develop and coordinate external relations programs with public sector law enforcement or other external organizations to achieve security objectives**		
					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. Knowledge of:	**Develop, implement, and coordinate employee security awareness programs**		
					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		

Rate Understanding					APP	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					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		
					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		

Rate Understanding					Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					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		

Rate Understanding					APP	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						II. 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		

Rate Understanding					Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					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 security vendors/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		

Rate Understanding					Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					III. 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		

Rate Understanding							Track Progress	
1	2	3	4	5	APP Associate Protection Professional	Domains and Tasks of the APP Certification Exam	Hours of Study	Date Study Complete
					Task 6. Knowledge of:	**Ensure pre-incident resource planning (e.g. mutual aid agreements, table-top exercises)**		
					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		
					IV. Response Management (18%)			
					Task 1. Knowledge of:	**Respond to and manage an incident using best practices**		
					1.	Primary roles and duties in an incident command structure		
					2.	Emergency operations center (EOC) management principles and practices		
					Task 2. Knowledge of:	**Coordinate the recovery and resumption of operations following an incident**		
					1.	Recovery assistance resources		
					2.	Mitigation opportunities during response and recovery processes		
					Task 3. Knowledge of:	**Conduct a post-incident review**		
					1.	Mitigation opportunities during response and recovery processes		
					2.	Post-incident review techniques		
					Task 4. Knowledge of:	**Implement contingency plans for common types of incidents (e.g. bomb threat, active shooter, natural disasters)**		
					1.	Short- and long-term recovery strategies		
					2.	Incident management systems and protocols		

Rate Understanding					APP	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 5. Knowledge of:	**Identify vulnerabilities and coordinate additional countermeasures for an asset in a degraded state following an incident**		
					1.	Triage/prioritization and damage assessment techniques		
					2.	Prevention, intervention, and response tactics		
					Task 6. Knowledge of:	**Assess and prioritize threats to mitigate consequences of incidents**		
					1.	Triage/prioritization and damage assessment techniques		
					2.	Resource management techniques		
					Task 7. Knowledge of:	**Coordinate and assist with evidence collection for post-incident review (e.g. documentation, testimony)**		
					1.	Communication techniques and notification protocols		
					2.	Communication techniques and protocols of liaison		
					Task 8. Knowledge of:	**Coordinate with emergency services during incident response**		
					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. Knowledge of:	**Monitor the response effectiveness to incident(s)**		
					1.	Post-incident review techniques		
					2.	Incident management systems and protocols		
					Task 10. Knowledge of:	**Communicate regular status updates to leadership and other key stakeholders throughout incident**		
					1.	Communication techniques and protocols of liaison		
					2.	Communication techniques and notification protocols		
					Task 11. Knowledge of:	**Monitor and audit the plan of how the organization will respond to incidents**		
					1.	Training and exercise techniques		
					2.	Post-incident review techniques		

APP Exam Domains

Security Management Fundamentals	35%
Business Operations	22%
Risk Management	25%
Response Management	18%

The Study Plan

The Self-Assessment ratings give you a guide to setting your study plan. Using your lowest scores, determine the amount of time you feel you would need to master this topic. Work your way through all the topics. This plan is a budget and you can modify it after your studies begin. Add up the total hours to see if you are being reasonable with your effort. Adjust your efforts if needed.

Next, schedule your study time. Set aside two-hour blocks of time. More than four-hour blocks are usually not effective. Determine how many hours each week you can dedicate to passing the exam. Set specific days and times. Choose a location where you will be able to concentrate on your task. Treat this study time as if it were your job—because it is.

Once you have the plan, stick to it. Make your plan an important part of your routine. Let your family and friends know your task and ask for their support in this venture.

How to Implement Your Plan

Use your ratings from the Self-Assessment list, especially the ones with your lower scores, and research each using the Table of Contents or indexes of the CPP, PCI, PSP, or APP recommended references. Using your study plan as a guide, study the relevant material. Continue to re-read each knowledge statement so that you understand the reading material in context to the exam as defined by the exam structure.

As you read the references (reading material), you may realize security is an art as well as a science. There may be multiple solutions for one situation. Remember as you study, the exam items are based on what most security professionals feel is the best solution for a given situation—not what you necessarily use in your practice. While the actual exam questions are difficult, there are no ambiguous answers to questions. Only one answer is correct on the exam.

Do not spend your time solving issues that are ambiguous or have no right answer. Those situations are not likely to be tested. Your colleagues correctly answer the exam questions more than 50 percent of the time. The test developers remove questions that are not clear or are frequently answered incorrectly from the bank of questions.

As you move through your studies, re-evaluate your progress.

- Start each study session with a review of the previous work.
- Did you improve your assessment score? Did you mitigate one threat to your success?
- Seek root statements. Identify those items that unconditionally express a key security principle.
  - "Sometimes" or "usually" suggest conditions. Unless the conditions are identified, it would be difficult to write a question with one answer.
- Don't memorize the facts, but apply the facts to a scene, so that you see it as security practice.

The exam is testing your experience and your knowledge of practices as conducted by other security professionals. This exam is not simply "book learning" or testing your memorization of the references.

ASIS Review Courses

ASIS International offers classroom and online review courses. The classroom and online review courses offered through ASIS are directed toward participants who have extensive knowledge of security and meet the application requirements. Participants in these review classes should already be familiar with the references and prepared to take the exam. The courses do not go into depth on any one topic, because the candidate should have already studied the topics of the domains. **Visit the ASIS webpage for information about the Certification Review Courses**. These courses are not designed to teach the full spectrum of any domain or topic but to highlight key concepts.

ASIS Chapter Study Groups

There is no official or recommended way to set up a chapter study group. There are as many versions as there are chapters in ASIS.

The type of study group will depend on the participants.

- Are all participants local? Is a weekly in-person meeting feasible?
- Do they have access to the Internet? Is an online study group a possibility?
- Do you have funding or the means to hire an experienced review instructor?
- How knowledgeable is the group? Is this a two-day review or an extended review that covers content from the ground up?

ASIS chapters often use longer class hours to meet with candidates over a period of weeks; for example, dedicating a full or partial Saturday to work in study groups. **Find your local chapter to inquire about certification study groups**. Sometimes several chapters in a Region form regional study groups.

Who Leads a Study Group?

ASIS prefers that a person holding a CPP, PCI, PSP, or APP act as the advisor or developer of the relevant review course to ensure the curriculum is directed toward the certification. This does not mean that an expert in a field may not instruct with proper guidance. The advisor or developer may provide advice on instructing styles, forming study groups, mentoring, and fostering study habits. Course developers may formulate original questions as a means of practice and evaluation of colleagues.

If you are forming a study group where participants instruct each other, use the domains and tasks as your reference to developing instruction.

Guidance for Study Groups

There are many ways to conduct a successful study group. Teaching someone is an exceptional way to learn. Instructors should help students identify areas of weakness and guide them in studying the appropriate material.

An excellent way to build confidence on a topic is through problem-solving exercises. The intent of the exercise is to present a series of questions based on a particular domain task and allow students to address the questions and provide supporting materials. This exercise could be a group task with each group reporting their solution and rationale.

Sample Problem-Solving Exercise

Studying for the PSP

Domain II: Application, Design, and Integration of Physical Security Systems
Task 2.01: Establish security program performance requirements.
Knowledge of: 4. Applicable codes, standards, and guidelines

The industry continues to develop new standards through the International Standards Organization (ISO) and American National Standards Institute (ANSI) among others. While compliance to standards is voluntary, the standards set a level of practice to improve security.

1) Why are Standards important to your business practice?
2) What techniques might be used to measure against a Standard?
3) How do the indicators promote change or improvement?

Guidance: The group may wish to cite a specific Standard to examine the questions. The use of site-specific examples is encouraged. Students should prepare to show a rationale for their answers.

Evaluation through Discussion: The instructor should look for an understanding of the Standard and how it is applied to a situation.

- Is it properly used?
- Were the measures well thought through?
- Are there additional/different measures that could be employed more effectively?
- Did the group show milestones that could be used as decision-making points for change?
- Was a schedule for measurement presented?

The above problem-solving exercise is only an example of a short activity a small group might tackle in 20 minutes. The reporting out provides a learning opportunity across many topics. The importance is setting clear expectations by giving "Guidance," and knowing how you will make this a learning opportunity through defining "Evaluation" points, which provide direction for further study.

The instructor or group leader must guide the student(s) to think through a question or task, and not provide answers. It is important for candidates to be able to think through the problems and not simply try to memorize information.

Are You Ready?

There are no "trick" questions on the exam. There are difficult questions. Questions may be testing multiple pieces of information and, therefore, each exam item (question) has its own value. Each question has been tested for validity and reliability. Most of your colleagues answer each question or item correctly more frequently than not. Think of each question in terms of how your professional security colleagues would address the solution.

Testing Strategy

The day will come for you to take the exam. Do you have a strategy?

Testing strategies are not specific to any one exam. No single strategy works for everyone. Individuals need to find strategies that are right for each situation. You must make the plan.

Things to Consider

The Biology of Test Taking

- ✓ Don't test after working or studying all night. Without proper rest, you will not be able to focus on test items. For most individuals, at least eight hours of sleep a night is recommended.
- ✓ Fuel up before the exam. You need food for energy to remain alert. However, avoid heavy foods, which can make you sleepy.
- ✓ Show up early to the testing location. You don't want to worry about getting to the test site.
- ✓ Use the restroom before walking into the exam room. If you are not comfortable, you will worry about your bodily functions during the test.
- ✓ Stay positive throughout the exam period. Try to stay relaxed, yet focused. If you start to feel anxious, take a few deep breaths.

The Attack Plan

- ✓ As you begin the testing process, read all instructions thoroughly.
- ✓ Don't dwell on a problem that stumps you. Time is a factor. Decide before you go into the exam how much time you will spend on the first item if you are unsure. Stick to your plan and move on. You can go back to the item if time allows. Consider item 2, item 3, and item 4 strategies. Don't let items become a blockade. You will find items that you have mastered, so build your confidence.
- ✓ Read the entire question and pay attention to the details. Many of your colleagues make unfortunate mistakes by rushing through the question. Always read the entire item carefully before considering the answers. Don't make assumptions about what the question might be. Other parts of the test may have some information that will help you with that question.
- ✓ If you have time left when you are finished, look over your test. Make sure that you have answered all the questions. All unanswered questions are scored; therefore, answer every question.
- ✓ Consider the answer in your head before reviewing the possible answers. The choices given on the test may throw you off or introduce factors that will distract you.
- ✓ Consider all possible options before choosing your answer. There may be several possibilities that are partially correct, but only one answer is right.
- ✓ There is no guessing penalty. Always take an educated guess and select an answer. Eliminate answers you know aren't right to increase your odds.
- ✓ If you don't know an answer, mark it and return to it later if you have time.
- ✓ Don't keep on changing your answer; usually your first choice is the right one, unless you misread the question.

About the Exams

An exam consists of multiple-choice questions covering tasks, knowledge, and skills in broad domains identified by CPPs, PCIs, PSPs, and APPs as the major areas involved in security management, investigations and physical security. Candidates are encouraged to refer to the reading materials as they prepare for the exam. After carefully reviewing the domains of study and identifying individual learning needs, candidates may use additional references and study opportunities as necessary.

Exam Development

The CPP, PCI, PSP, and APP examinations are designed to assess whether a practitioner possesses the knowledge established as the basic competency level required for the chosen designation. The examination development process follows internationally accepted procedures for establishing the content validity of a test and the reliability of its scores.

ROLE DELINEATION (JOB ANALYSIS)

The first step is the role delineation, or job analysis, which identifies the areas of responsibility (domains) and important work functions required for safe and effective performance in a security position, and the relative importance in the actual practice of a profession. ASIS currently performs role delineations approximately every five years.

EXAMINATION SPECIFICATIONS

The importance of each domain and of the relevant tasks, knowledge, and skills within it, determines the specifications of the examination. The relative order of importance of the domains determines the percentage of the total test items allocated to each. The examination is based on this blueprint.

PREPARATION OF EXAMINATION ITEMS

To ensure that all exam items (questions) are aligned with the exam content and are constructed following certification development best practices, each item goes through the following phases:

1. An Item Development Group (IDG), comprised of those who have already earned the certification, is trained by ASIS's exam development vendor on the proper way to construct an exam item. The IDG not only writes the items and the correct answer but also writes plausible wrong answers, called distractors. The distractors are not designed to trick test takers but rather to identify those who have truly mastered the knowledge and skills needed to be a professional security manager. There are no "all of the above" or "none of the above" selections. Finally, item writers must provide a reference from which the correct answer was sourced. These references are included in each certification's recommended reading material.

2. Once the exam item is written, it is reviewed by a second panel of subject matter experts. The item reviewers ensure that: the correct answer has a reliable reference; the content aligns with the exam content domains; it is free from cultural bias; and it is grammatically correct.

3. After the item has been approved by the item review team, it is pretested on the actual exam. Pretest items are not included in the final score. The results of the pretest items are analyzed by ASIS's exam development vendor. If the analysis shows that an item performed well, it is included as a scoreable item on a future exam. If the item performs poorly, it is either sent back to the reviewers to rewrite (and then pretested again) or it is discarded.

DETERMINING ELIGIBILITY TO PARTICIPATE IN ITEM WRITING

ASIS invites seasoned and newly certified individuals to participate in item writing. However, not all certificants are eligible for contributing to the process. Exclusions include ASIS certified professionals who are planning to test for any other ASIS certifications within two years of item-writing participation and those who are actively involved in exam-preparation courses.

EXAMINATION FORM DEVELOPMENT

Each new form of the examination is created according to established test specifications with the appropriate number of items for each domain from the bank of available test questions.

ESTABLISHMENT OF PASSING SCORE

After a new job analysis study is conducted and new examination specifications developed, a passing point study is performed by the PCB for the first new form according to widely accepted procedures, under the guidance of the ASIS exam development vendor. From the results of the study, the PCB establishes the passing score in order to meet the "minimum competency" certification standard.

EQUATING OF EXAMINATION FORMS

Once the PCB establishes the passing score, all additional forms developed according to the most current job analysis study are "equated" in order to make them of comparable difficulty to the original. "Equating" is a statistical process that is used to adjust for difficulty among forms that are constructed to be similar in difficulty level and content. The process enables the scores on any two forms to be equivalent. The difficulty of each exam item is set after the item has been pretested.

SCALED SCORE

In order to maintain test security, the PCB produces multiple forms of the CPP, PCI, PSP, and APP examinations with different questions on each form. Individual scores are reported as "scaled scores." These "scaled scores" are derived from raw scores through mathematical conversion so that scores from different forms can be reported on a common scale and, therefore, represent the same level of competence. Scaled scores, used widely in the certification and licensing fields, ensure that all candidates are required to demonstrate the same level of ability to pass the test regardless of whether they took an easier or more difficult test form. Certified public accountants, human resource professionals, and building inspectors are only a few of the many professions receiving scaled examination scores.

EXAMINATION SCORING AND REPORTING

After all analyses are complete, the examinations are scored. Candidates will receive notification of passing or failing the exam and score reports containing a breakdown, by domain, of the percentage of questions they answered correctly.

About the CPP Exam

The CPP exam consists of 200 scored multiple-choice questions and may contain 25 "pretest" (unscored) questions randomly distributed throughout the examination for a total of 225 questions. The time allowed takes into consideration the review of pretest items. The CPP exam is 4 hours.

The exam covers tasks, knowledge, and skills in eight broad domains that have been identified by CPPs as the major areas involved in security management.

Security Principles and Practices (21%)
Business Principles and Practices (13%)
Investigations (10%)
Personnel Security (12%)
Physical Security (25%)
Information Security (9%)
Crisis Management (10%)

About the PCI Exam

The PCI exam consists of 125 multiple-choice questions and may contain 15 "pretest" (unscored) questions randomly distributed throughout the examination for a total of 140 questions. The time allowed takes into consideration the review of pretest items. The PCI exam is 2½ hours.

The exam covers tasks, knowledge, and skills in three primary domains that have been identified by professional investigators as the required areas of competency in this field.

Case Management (35%)
Investigative Techniques and Procedures (50%)
Case Presentation (15%)

About the PSP Exam

The PSP exam consists of 125 multiple-choice questions and may contain 15 "pretest" (unscored) questions randomly distributed throughout the examination for a total of 140 questions. The time allowed takes into consideration the review of pretest items. The PSP exam is 2½ hours.

The exam covers tasks, knowledge, and skills in three broad domains that have been identified by PSPs as the major areas involved in physical security management.

Physical Security Assessment (34%)
Application, Design, and Integration of Physical Security Systems (34%)
Implementation of Physical Security Measures (32%)

About the APP Exam

The APP exam consists of 100 multiple-choice questions and may contain 25 "pretest" (unscored) questions randomly distributed throughout the examination for a total of 125 questions. The time allowed takes into consideration the review of pretest items. The APP exam is 2 hours.

The exam covers the tasks, knowledge, and skills in four primary domains that have been identified by those with one to four years of experience in security management.

Security Management Fundamentals (35%)
Business Operations (22%)
Risk Management (25%)
Response Management (18%)

Scheduling an Exam

ASIS engages Prometric, an internationally recognized testing institution, to conduct and proctor the ASIS certification exams. With few exceptions, the exams are presented as computer-based tests. Prometric has testing facilities throughout the world. Candidates are expected to arrange for testing at a convenient facility and time. Candidates must be approved by ASIS to take an exam before they can schedule a date and time for testing.

- Exam can be scheduled through a secure 24-hour website **prometric.com/asis**.
- Approved candidates can also arrange for a test date and location by calling Prometric at +1.800.699.4975.
  - Monday through Friday, 8:00 am - 8:00 pm (EST)
  - Saturday, 8:00 am - 4:00 pm (EST)
- A Prometric representative will help a candidate
  - select the optimal test date
  - identify a test location
  - provide specific instructions, such as proper identification and testing protocols
  - driving directions
- The candidate will receive a confirmation number via email to be taken to the testing center at the time of the exam.

Policies and Procedures

All exam applicants are required to abide by the policies and procedures of the ASIS Certification Program. In addition, on the application all applicants must sign an attestation verifying that they've read the **Certification Handbook**, which outlines all policies and procedures of the program.

Fees

ASIS computer-based exams are offered at Prometric testing locations across the globe. Internet-based tests are available in certain locations.

Computer-Based Test for CPP, PCI, and PSP

- ASIS members: $300
- Nonmembers: $450

Computer-Based Test for APP

- ASIS members: $200
- Nonmembers: $350

Internet-Based Exams

Only available in Australia (Queensland), Costa Rica, Ecuador, Jamaica, Paraguay, and Panama

These exams are offered biannually on the first Saturday of May and November.

- ASIS members: $200
- Nonmembers: $350

Computer-Based Retest for CPP, PCI, and PSP

- ASIS members and nonmembers: $200

Computer-Based Retest for APP

- ASIS members and nonmembers: $150

Internet-Based Retest

Only available in Australia (Queensland), Costa Rica, Ecuador, Jamaica, Paraguay, and Panama.

- ASIS members and nonmembers: $100

Fees include a $100 nonrefundable application fee. If your application is rejected for any reason, only the testing fee portion will be refunded.

The computer-based test refund is currently $200 for members and $350 for nonmembers.

G.I. Bill

Qualified U.S. applicants may receive reimbursement for the certification exams through the G.I. Bill. An application is available at **gibill.va.gov** *or call +1.888.442.4551 and request VA Form 22-0823.*

Prometric Fees for Rescheduling Exams

Due to frequent cancellations and short notification rescheduling, Prometric has expressed concern that there may be inadequate capacity at centers where the ASIS International examinations are administered. In order to provide a first choice experience for all candidates, Prometric instituted a reschedule/cancel fee. This fee will be assessed either at the Prometric website if the candidate reschedules or cancels online, or via phone (+1.800.699.4975) by Prometric customer service.

The fee will be applied as follows:

- If a candidate reschedules or cancels 31 or more days before the scheduled test day, there is no charge.
- If a candidate reschedules or cancels 3 to 30 days before the scheduled test day, there is a charge of $62.50 per reschedule.
- If a candidate reschedules or cancels less than 3 days before the scheduled test date, the full candidate-testing fee is charged.

All test rescheduling and payment of related fees (if applicable) are to be made directly through Prometric.

ASIS
INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314-2882
USA
Phone: +1.703.519.6200
Fax: +1.703.519.6299
asisonline.org