ASIS INTERNATIONAL
Advancing Security Worldwide®

2025 Self-Assessment For CPP, PCI, PSP, APP Exams

ASIS International administers the CPP, PCI, PSP, and APP programs to elevate the professional standing of the security profession and improve the practice of security through the testing and certification of those security practitioners who, by meeting prescribed standards of performance, knowledge, and conduct, have demonstrated established levels of competence in security management or specialty areas of knowledge.

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 updated on 20 May 2025. It replaces all previous editions. For information on how to apply for ASIS certification, please download the **Board Certification Handbook**.

TABLE OF 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 ensuring that standards are developed and maintained, quality assurance is in place, and 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 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 relates each of the 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 body. All exam items are secure in an item bank.

Candidates sitting for the exam must sign a nondisclosure 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. Approximately 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.

The domains, tasks, and knowledge statements with their definitions are made available to the public by the PCB.

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 using the certification reference materials.

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

This credential provides demonstrable proof of knowledge and management skills in several key domains of security. CPP candidates must meet the following requirements:

> Five to seven years of security work experience depending on the level of education completed. Experience must include at least three years in responsible charge of a security function*.

PCI EXAM ELIGIBILITY REQUIREMENTS

This credential provides demonstrable proof of an individual's knowledge and experience in professional responsibility, investigative techniques and procedures, and case presentation. PCI candidates must meet the following requirements:

> Three to five years of experience depending on level of education completed. Experience must include at least two years of case management**.

PSP EXAM ELIGIBILITY REQUIREMENTS

This credential provides demonstrable knowledge and experience in physical security assessment; application, design, and integration of physical security systems; and implementation of physical security measures. PSP candidates must meet the following requirements:

> Three to five years of experience depending on level of education completed.

* "Responsible charge" means that the applicant has the authority to make independent decisions and take independent actions to determine operational methodology and manage execution of a security-related project or process. This definition does not require the individual to supervise others and generally excludes such positions as patrol officer or the equivalent.

** "Case management" is defined as the coordination and direction of an investigation using various disciplines and resources, the finding of which would be assessed to establish the facts findings of the investigation as a whole; the management process of investigation.

APP EXAM ELIGIBILITY REQUIREMENTS

This designation is intended for those with one or more years of compensated security experience. Candidates who have already achieved another, approved, related certification, may be eligible to be approved for the APP with only six-months of compensated security experience. The exam will measure the professional's knowledge of security fundamentals, business operations, risk management, and response management.

Security Experience	Education
One year	No higher education degree
Six months	With approved, related Certification

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 various study resources. Candidates should determine the best study tools and methods for their success.

Study Plan Recommendations

- **Start early**
  - Plan on 50 to 250 study hours, depending on your work experience.
  - 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.
  - Study in blocks of time, such as two to three hours.

The strongest predictor of success is study time. Putting in the hours makes a difference. 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

This designation is intended for those with one or 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 to guide you toward success.

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

AN ASSESSMENT TOOL

ASIS has constructed the following self-assessment tool using the current exam content. For those with interest in the CPP, the self-assessment begins on page 9. The PCI assessment starts on page 18. The PSP assessment begins on page 22. The APP assessment begins on page 27.

Consider your depth of understanding for each task and knowledge statement in the assessment. Score your knowledge of each task on a 1-to-5 scale, with 1 as “I do not know what this task is” and 5 as “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					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
I. 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 organizations and agencies		
					2.	Methods for creating effective working relationships		
					3.	Liaison techniques and protocols		
					4.	Local, national, and international public/private partnerships		

Rate Understanding					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 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)		
					II. 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)		

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 4. Knowledge of:	**Develop, implement, and manage security staffing processes and personnel development programs to achieve organizational objectives.**		
					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. Knowledge of:	**Monitor and ensure an acceptable ethical climate in accordance with regulatory requirements and organizational culture.**		
					1.	Governance standards		
					2.	Guidelines for individual and corporate conduct		
					3.	Generally accepted ethical principles		
					4.	Confidential information protection techniques and methods		
					5.	Legal and regulatory compliance		
					Task 6. Knowledge of:	**Develop performance requirements and contractual terms for security vendors/suppliers.**		
					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		

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

Rate Understanding					Domains and Tasks of the CPP Certification Exam	Track Progress	
1	**2**	**3**	**4**	**5**		**Hours of Study**	**Date Study Complete**
					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:		
					1. Interview and interrogation techniques		
					2. Techniques for detecting deception		
					3. Nonverbal communication and cultural considerations		
					4. Rights of interviewees		
					5. Required components of written statements		
					6. 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)		
					IV. 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 techniques		

Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					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. Knowledge of:	**Develop, implement, and manage executive protection programs.**		
					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		
						V. Physical Security (16%)		
					Task 1. Knowledge of:	**Conduct facility surveys to determine the current status of physical security.**		
					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. Knowledge of:	**Select, implement, and manage physical security strategies to mitigate security risks.**		
					1.	Fundamentals of security program 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		

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. **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		
					VI. 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, equipment, and procedures (e.g., interoperability)		
					7. Information security threats and vulnerabilities		
					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		

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 3. **Implement and manage an integrated information security program.** Knowledge of:			
					1. Information security including confidentiality, integrity, and availability			
					2. Information security systems methodology			
					3. Authentication techniques (e.g., multi-factor, biometrics)			
					4. Continuous evaluation and improvement programs			
					5. Ethical hacking and penetration testing techniques and practices			
					6. Encryption and datamasking techniques (e.g., cryptography)			
					7. Systems integration techniques (e.g., interoperability, licensing, networking)			
					8. Cost-benefit analysis methodology			
					9. Project management techniques			
					10. Budget review process (e.g., system development lifecycle)			
					11. Vendor evaluation and selection process			
					12. Final acceptance and testing procedures			
					13. Protection technology and forensic investigations			
					14. Training and awareness programs to mitigate threats and vulnerabilities (e.g., phishing, social engineering, ransomware, insider threats)			
VII. 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)			

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 2.	**Prepare and plan how the organization will 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		

CPP Exam Domains

Security Principles and Practices	22%
Business Principles and Practices	15%
Investigations	9%
Personnel Security	11%
Physical Security	16%
Information Security	14%
Crisis Management	13%

Rate Understanding					Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
I. Professional Responsibility (28%)							
					Task 1. **Analyze case for applicable ethical conflicts.** Knowledge of:		
					1. Nature/types/categories of ethical issues related to cases (e.g., fiduciary, conflict of interest, potential for dual role bias/ discrimination, attorney-client, specific area competency)		
					2. The role of applicable laws, regulations, codes, and organizational policies/administrative guidelines in conducting investigations		
					Task 2. **Assess case elements, strategies, and risks.** Knowledge of:		
					1. Case categories (e.g., cyber, financial, criminal, civil, internal, workplace violence)		
					2. Qualitative and quantitative analytical methods and tools		
					3. Strategic/operational analysis		
					4. Criminal intelligence analysis		
					5. Risk identification and impact		
					6. Stakeholder identification		
					Task 3. **Determine investigative goals and develop strategy.** Knowledge of:		
					1. Initial projected case type (e.g., criminal, administrative)		
					2. Cost-benefit analysis		
					3. Procedural options		
					4. Case flow / investigative plan		
					5. Investigative methods		
					Task 4. **Determine and manage investigative resources.** Knowledge of:		
					1. Resource requirements (e.g., personnel, internal and external liaisons, equipment)		
					2. Resource allocations (e.g., time, budget)		
					3. Case management practices (e.g., chain of custody procedures, documentation requirements, case closure)		
					Task 5. **Identify, evaluate, and implement investigative process improvements.** Knowledge of:		
					1. Process improvement techniques (e.g., gap analysis, project management techniques)		
					2. Internal review (e.g., management, legal, human resources, internal liaisons)		

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
					3.	External review (e.g., regulatory bodies, accreditation agency, external liaisons)		
					4.	Investigative resources (e.g., administrative records, Open-Source Intelligence [OSINT])		
					5.	Investigative tools (e.g., digital forensic software, data collection software, case management software)		
						II. Investigative Techniques and Procedures (52%)		
					Task 1.	**Conduct surveillance by physical, behavioral, digital, and electronic means.** Knowledge of:		
					1.	Surveillance authorization and restrictions (e.g., legal considerations, types of surveillance)		
					2.	Surveillance tools (e.g., equipment, software, analytics, metadata, system logs)		
					3.	Pre-surveillance activities (e.g., planning, logistics, resources, advance assessment)		
					4.	Procedures for documenting surveillance activities (e.g., secure storage, case management solutions, privacy concerns)		
					Task 2.	**Conduct interviews of individuals.** Knowledge of:		
					1.	Interview types (e.g., subject, witness, person of interest)		
					2.	Interview techniques		
					3.	Special considerations (e.g., environment, in-person vs. remote, interview subject's mental health, translator)		
					4.	Indicators of deception (e.g., non-verbal communication, word choice, evasiveness)		
					5.	Subject statement documentation (e.g., audio, video, written)		
					6.	Representation considerations (e.g., legal counsel, union representation, juvenile advocacy)		
					Task 3.	**Collect and preserve evidence.** Knowledge of:		
					1.	Sources of evidence (e.g., physical, digital, biological)		
					2.	Methods/procedures for collection of various types of evidence		
					3.	Methods/procedures for preservation of various types of evidence (e.g., computer operations, digital media, biological)		
					4.	Chain of custody considerations and requirements (e.g., physical, digital, biological)		

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**
					Task 4. Knowledge of:	**Conduct research by physical, digital, and electronic means.**		
					1.	Methods of research using physical, information technology, and operational technology resources		
					2.	Information sources (e.g., government, proprietary, open source, databases, digital media)		
					3.	Methods of analysis of research results		
					4.	Research documentation (e.g., findings)		
					Task 5. Knowledge of:	**Collaborate with and obtain information from other agencies and organizations.**		
					1.	External information sources		
					2.	Liaison development and maintenance		
					3.	Liaison techniques (e.g., formal, informal)		
					4.	Techniques for using and synthesizing external information (e.g., redacting, protecting sources and sensitivities, documented vs. undocumented)		
					Task 6. Knowledge of:	**Use investigative techniques.**		
					1.	Legal, administrative, and organizational considerations		
					2.	Concepts, principles, and methods of video/audio recordings		
					3.	Concepts, principles, and methods of forensic analysis (e.g., physical, digital, biological)		
					4.	Concepts, principles, and methods of undercover investigations		
					5.	Concepts, principles, and methods of threat and risk assessments		
					6.	Concepts, principles, and methods of applying IT/OT technologies		
					7.	Use of confidential sources		

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 (20%)		
					Task 1. **Prepare report to substantiate investigative findings.** Knowledge of:		
					1. Critical elements and format of an investigative report (e.g., audience/legal considerations, addressing privacy and confidentiality, types of report)		
					2. Investigative terminology		
					3. Logical sequencing of information		
					Task 2. **Prepare and present testimony.** Knowledge of:		
					1. Types of testimony (e.g., depositions, administrative hearings, criminal and civil proceedings)		
					2. Preparation for testimony (e.g., pre-trial rehearsal)		
					3. Testimony best practices		

PCI Exam Domains

Professional Responsibility	28%
Investigative Techniques and Procedures	52%
Case Presentation	20%

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.	Key area or critical asset identification		
					2.	Risk assessment models and considerations (e.g., inside-outward, outside-inward, site-specific risk assessment, functional approach)		
					3.	Qualitative and quantitative assessment methods		
					4.	Types of resources and guidelines needed for the assessment (e.g., stakeholders, budget, equipment, policies, standards)		
					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 for various types of assets and business operations		
					Task 3.	**Assess the nature of the threats and hazards so that the risk 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, socioeconomic environment, criminal activity, existing security countermeasures, security risk level)		
					3.	Potential impact of external organizations (e.g., competitors, organizations in immediate proximity) on facility's security program		
					4.	Other internal and external factors (e.g., legal, loss of reputation, economic, supply chain) 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, incident reports, crime statistics, personnel issues, benchmarking)		
					2.	Effectiveness of current security technologies/equipment, personnel, and procedures		
					3.	Evaluation of building plans, drawings, and schematics		
					4.	Applicable standards/regulations/codes and where to find them		
					5.	Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security		

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. Perform a risk analysis to develop countermeasures. Knowledge of:		
					1. Risk analysis strategies and methods		
					2. Risk management principles		
					3. Analysis and interpretation of collected data		
					4. Threat/hazard and vulnerability identification		
					5. Loss event profile analyses (e.g., consequences)		
					6. Appropriate countermeasures related to specific risks		
					7. Cost-benefit analysis (e.g., return on investment [ROI], total cost of ownership)		
					8. Legal and regulatory considerations related to various countermeasures/security applications (e.g., video surveillance, privacy issues, personally identifiable information, life safety)		
II. Application, Design, and Integration of Physical Security Systems (35%)							
					Task 1. Establish security program performance requirements. Knowledge of:		
					1. Design constraints (e.g., regulations, budget, materials, system compatibility)		
					2. Incorporation of risk analysis results in design		
					3. Relevant security terminology (e.g., punch list, field test)		
					4. Relevant security concepts (e.g., CPTED, defense-in-depth, the 4 Ds—deter, detect, delay, deny)		
					5. Applicable codes, standards, and guidelines		
					6. Operational requirements (e.g., policies, procedures, staffing)		
					7. Functional requirements (e.g., system capabilities, features, fault tolerance)		
					8. Performance requirements (e.g., technical capability, systems design capacities)		
					9. Success metrics		
					Task 2. Determine appropriate physical security countermeasures. Knowledge of:		
					1. Structural security measures (e.g., barriers, lighting, locks, blast mitigation, ballistic protection)		
					2. Crime prevention through environmental design (CPTED)		
					3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)		
					4. Security staffing (e.g., officers, technicians, management, administration)		

Rate Understanding						Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					5.	Personnel, package, and vehicle screening		
					6.	Emergency notification systems (e.g., mass notifications, public address, two-way intercom)		
					7.	Principles of data storage and management (e.g., cloud, on-premise, redundancy, retention, user permissions, personally identifiable information, regulatory requirements)		
					8.	Principles of network infrastructure and physical network security (e.g., token ring, LAN/WAN, VPN, DHCP vs. static, TCP/IP)		
					9.	Security audio communications (e.g., radio, telephone, intercom)		
					10.	Systems monitoring and display (e.g., control centers/consoles, central monitoring station)		
					11.	Primary and backup power sources (e.g., grid, battery, UPS, generators, alternative/renewable)		
					12.	Signal and data transmission methods (e.g., copper, fiber, wireless)		
					13.	Visitor and vendor management policies		
					Task 3. Knowledge of:	**Design physical security systems and project documentation.**		
					1.	Design phases (e.g., pre-design, schematic, development, construction, documentation)		
					2.	Design elements (e.g., calculations, drawings, specifications, review, technical data)		
					3.	Construction specification standards (e.g., Constructions Specifications Institute, owner's equipment standards, American Institute of Architects [AIA] MasterSpec)		
					4.	Systems integration		
					5.	Project management concepts		
					6.	Scheduling (e.g., Gantt charts, PERT charts, milestones, objectives)		
					7.	Cost estimation and cost-benefit analysis of design options (e.g., value engineering)		
III. Implementation of Physical Security Measures (31%)								
					Task 1. Knowledge of:	**Outline criteria for pre-bid meeting.**		
					1.	Bid process (e.g., site visits, RFI, substitution requests, pre-bid meeting)		
					2.	Bid package types (e.g., RFP, RFQ, IFB, sole source)		
					3.	Bid package components (e.g., project timelines, costs, personnel, documentation, scope of work)		

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
					4.	Criteria for evaluation of bids (e.g., cost, experience, scheduling, certification, resources)		
					5.	Technical compliance criteria		
					6.	Ethics in contracting		
					Task 2. Knowledge of:	**Develop procurement plan for goods and services.**		
					1.	Vendor evaluation and selection (e.g., interviews, due diligence, reference checks)		
					2.	Project management functions and processes		
					3.	Procurement process		
					Task 3. Knowledge of:	**Manage implementation of goods and services.**		
					1.	Installation and inspection techniques		
					2.	Systems integrations		
					3.	Commissioning		
					4.	Installation problem resolution (e.g., punch lists)		
					5.	Systems configuration management (e.g., as-built drawings)		
					6.	Final acceptance testing criteria (e.g., system acceptance testing, factory acceptance testing)		
					7.	End-user training requirements		
					Task 4. Knowledge of:	**Develop requirements for personnel involved in support of the security program.**		
					1.	Roles, responsibilities, and limitations of security personnel (including proprietary [in-house] and contract security staff)		
					2.	Human resource management (e.g., establishing KPIs, performance review, improvement processes, recruiting, onboarding, progressive discipline)		
					3.	Security personnel professional development (e.g., training, certification)		
					4.	General, post, and special orders		
					5.	Security personnel uniforms and equipment		
					6.	Security awareness training and education for non-security personnel		

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
					Task 5.	**Monitor and evaluate program throughout the system life cycle.** Knowledge of:		
					1.	Maintenance of systems and hardware (e.g., preventative, corrective, upgrades, calibration, service agreements)		
					2.	Warranty types (e.g., manufacturer, installation, replacement parts, extended)		
					3.	Ongoing system training (e.g., system upgrades, manufacturer's certification)		
					4.	System evaluation and replacement process		

PSP Exam Domains

Physical Security Assessment	34%
Application, Design, and Integration of Physical Security Systems	35%
Implementation of Physical Security Measures	31%

Rate Understanding					APP Associate Protection Professional Board Certified in Security Management Fundamentals	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. **Implement and coordinate the organization's security program(s) to protect the organization's assets.** Knowledge of:			
					1. Security theory and terminology			
					2. Project management techniques			
					3. Security industry standards			
					4. Protection techniques and methods			
					5. Security program and procedures assessment			
					6. Security principles of planning, organization, and control			
					Task 2. **Implement methods to improve the security program on a continuous basis through the use of auditing, review, and assessment.** Knowledge of:			
					1. Data collection and intelligence analysis techniques			
					2. Continuous assessment and improvement processes			
					3. Audit and testing techniques			
					Task 3. **Develop and coordinate external relations programs with public sector law enforcement or other external organizations to achieve security objectives.** Knowledge of:			
					1. Roles and responsibilities of external organizations and agencies			
					2. Local, national, and international public/private partnerships			
					3. Methods for creating effective working relationships			
					Task 4. **Develop, implement, and coordinate employee security awareness programs.** Knowledge of:			
					1. The nature of verbal and nonverbal 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® Associate Protection Professional Board Certified in Security Management Fundamentals	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:	**Implement and/or coordinate an investigative program.**		
					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. Knowledge of:	**Provide coordination, assistance, and evidence such as documentation and testimony to support legal proceedings.**		
					1.	Required components of effective documentation (e.g., legal, employee, procedural, policy, compliance)		
					2.	Evidence collection and protection techniques		
					3.	Relevant laws and regulations regarding records management, retention, legal holds, and destruction practices (Note: No country-specific laws will be on the APP exam)		
					Task 7. Knowledge of:	**Conduct background investigations for hiring, promotion, and/or retention of individuals.**		
					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. Knowledge of:	**Develop, implement, coordinate, and evaluate policies, procedures, programs, and methods to protect individuals in the workplace against human threats (e.g., harassment, violence).**		
					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. Knowledge of:	**Conduct and/or coordinate an executive/personnel protection program.**		
					1.	Travel security program components		
					2.	Executive/personnel protection program components		
					3.	Protection personnel, technology, and processes		

Rate Understanding					APP® Associate Protection Professional Board Certified in Security Management Fundamentals	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 10. Knowledge of:	**Develop and/or maintain a physical security program for an organizational asset.**		
					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. Knowledge of:	**Recommend, implement, and coordinate physical security controls to mitigate security risks.**		
					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. Knowledge of:	**Evaluate and integrate technology into security program to meet organizational goals.**		
					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. Knowledge of:	**Coordinate and implement security policies that contribute to an information security program.**		
					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® Associate Protection Professional Board Certified in Security Management Fundamentals	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 communication 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		
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		

Rate Understanding					Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5		Hours of Study	Date Study Complete
					Task 3. Prepare, plan, and communicate how the organization will identify, classify, and address risks. Knowledge of:		
					1. Risk management compliance testing (e.g., program audit, internal controls, self-assessment)		
					2. Quantitative and qualitative risk assessments		
					3. Risk management standards		
					4. Vulnerability, threat, and impact assessments		
					Task 4. Implement and/or coordinate recommended countermeasures for new risk treatment strategies. Knowledge of:		
					1. Countermeasures		
					2. Mitigation techniques		
					3. Cost-benefit analysis methods for risk treatment strategies		
					Task 5. Establish a business continuity or continuity of operations plan (COOP). Knowledge of:		
					1. Business continuity standards		
					2. Emergency planning techniques		
					3. Risk analysis		
					4. Gap analysis		
					Task 6. Ensure pre-incident resource planning (e.g., mutual aid agreements, table-top exercises). Knowledge of:		
					1. Data collection and trend analysis techniques		
					2. Techniques, tools, and resources related to internal and external threats		
					3. Quality and types of information and data sources		
					4. Holistic approach to assessing all-hazard threats		

Rate Understanding					APP® Associate Protection Professional Board Certified in Security Management Fundamentals	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
IV. Response Management (18%)								
					Task 1. **Respond to and manage an incident using best practices.** Knowledge of:			
					1. Primary roles and duties in an incident command structure			
					2. Emergency operations center (EOC) management principles and practices			
					Task 2. **Coordinate the recovery and resumption of operations following an incident.** Knowledge of:			
					1. Recovery assistance resources			
					2. Mitigation opportunities during response and recovery processes			
					Task 3. **Conduct a post-incident review.** Knowledge of:			
					1. Mitigation opportunities during response and recovery processes			
					2. Post-incident review techniques			
					Task 4. **Implement contingency plans for common types of incidents (e.g., bomb threat, active shooter, natural disasters).** Knowledge of:			
					1. Short- and long-term recovery strategies			
					2. Incident management systems and protocols			
					Task 5. **Identify vulnerabilities and coordinate additional countermeasures for an asset in a degraded state following an incident.** Knowledge of:			
					1. Triage/prioritization and damage assessment techniques			
					2. Prevention, intervention, and response tactics			
					Task 6. **Assess and prioritize threats to mitigate consequences of incidents.** Knowledge of:			
					1. Triage/prioritization and damage assessment techniques			
					2. Resource management techniques			

Rate Understanding					APP	Domains and Tasks of the APP Certification Exam	Track Progress	
1	2	3	4	5	Associate Protection Professional Board Certified in Security Management Fundamentals		Hours of Study	Date Study Complete
					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 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 those topics. 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. Blocks over four hours 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 can 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 (recommended 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 tests 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. These courses 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 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.
- ✓ 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 as incorrect; therefore, answer <u>every</u> 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 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 answers 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 security professional. 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, that the content aligns with the exam content domains, that it is free from cultural bias, and that 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 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 be notified whether they passed or failed the exam. Failing score reports also contain a breakdown, by domain, of the percentage of questions they answered correctly.

SCHEDULING AN EXAM

ASIS engages Prometric, an internationally recognized testing administrator, to conduct and proctor the ASIS certification exams. Test takers have two options for testing:

1. Take the exam at one of more than 450 Prometric Test Centers worldwide.

2. Take the exam in your own home using Prometric's ProProctor platform.

Candidates must apply for and be approved to take the exams by ASIS. Online applications are available on the ASIS website.

- The 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)
- 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

The Certification Handbook contains all the policies and procedures of the ASIS certification program including eligibility requirements, fees, study options, and more. When submitting their application, all applicants are required to sign an attestation agreeing to abide by the policies of the program.

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.*

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
certification@asisonline.org