

2016

CPP Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

PCI[®]
Professional Certified Investigator
Board Certified, ASB International

PSP[®]
Physical Security Professional
Board Certified, ASB International

Self-Assessment for CPP, PCI, or PSP Exams



ASIS
INTERNATIONAL
Advancing Security Worldwide[®]

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

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

This handbook was created on March 1, 2016. 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*.

Contents

Introduction 1
 The Role of the PCB 1

The Value of the CPP, PCI, and PSP Designations 1
 A Dynamic Designation 2
 The Role of ASIS Education 2

Eligibility Requirements 3

Creating a Study Plan 4
 Conduct a Self-Assessment 4
 An Assessment Tool 5

Self-Assessment Tool for Creating a Study Plan 6
 Domains and Tasks of the CPP Certification Exam 6
 Domains and Tasks of the PCI Certification Exam 16
 Domains and Tasks of the PSP Certification Exam 20

The Study Plan 24
 How to Implement Your Plan 24

ASIS Review Courses 25
 Group Study 25
 Who Leads a Study Group? 25
 Guidance for Study Groups 26
 Sample Problem-Solving Exercise 27

Are You Ready? (Things to Consider) 28
 Testing Strategy 28
 The Biology of Test Taking 28
 The Attack Plan 29

About the Exams 30
 Exam Development 30
 About the CPP Exam 32
 About the PCI Exam 32
 About the PSP Exam 32
 Scheduling an Exam 33

Fees and Policies 34
 Prometric Fees for Rescheduling Exams 35

Introduction

ASIS International (ASIS) is dedicated to ensuring that the Certified Protection Professional (CPP)[®], Professional Certified Investigator (PCI)[®], and Physical Security Professional (PSP)[®] 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, and PSP 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, and PSP 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. Even the retired items are not released.

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, or PSP designation.

A Dynamic Designation

The domains and knowledge statements periodically change to reflect the current duties 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 Education

ASIS Education has no more insider access to testing information than the public. ASIS volunteer members working with ASIS Education 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 (reading material).

The certification department does not participate in review program activities or publications, case studies, exercises, practices 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 exam, 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 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***

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

* "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.

Creating a Study Plan

Self-Assessment for CPP, PCI, or PSP 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 over 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 over 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 broad domains identified by CPPs, PCIs, and PSPs as the major areas involved in security management, investigations and case management, or physical security, respectively. 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 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 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, as it will waste valued time.

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 16. The PSP assessment begins on page 20.


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 which you should study thoroughly.

Important Update for CPP Exams (Effective May 2016)


The CPP exam domains have been revised based on the completion of a 2014 job analysis. This important analysis is undertaken for all of the ASIS certification programs approximately every five years. It is an essential process as it helps to ensure the exam content remains current and accurately reflects job-related activities, competencies, and professional standards. [View FAQs](#)


Please note: These changes will not take effect until May 16, 2016.


Self-Assessment Tool for Creating a Study Plan

Rate Understanding						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 1.01. Plan, develop, implement, and manage the organization’s security program to protect the organization’s assets Knowledge of:			
					1.01.01. Principles of planning, organization, and control			
					1.01.02. Security theory, techniques, and processes			
					1.01.03. Security industry standards			
					1.01.04. Continuous assessment and improvement processes			
					1.01.05. Cross-functional organizational collaboration			
					Task 1.02. Develop, manage, or conduct the security risk assessment process Knowledge of:			
					1.02.01. Quantitative and qualitative risk assessments			
					1.02.02. Vulnerability, threat, and impact assessments			
					1.02.03. Potential security threats (e.g., all hazards, criminal activity)			
					Task 1.03. Evaluate methods to improve the security program on a continuous basis through the use of auditing, review, and assessment Knowledge of:			
					1.03.01. Cost-benefit analysis methods			
					1.03.02. Risk management strategies (e.g., avoid, assume/accept, transfer, spread)			
					1.03.03. Risk mitigation techniques (e.g., technology, personnel, process, facility design)			
					1.03.04. Data collection and trend analysis techniques			


Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 1.04. Develop and manage external relations programs with public sector law enforcement or other external organizations to achieve security objectives Knowledge of:			
					1.04.01. Roles and responsibilities of external organization and agencies			
					1.04.02. Methods for creating effective working relationships			
					1.04.03. Techniques and protocols of liaison			
					1.04.04. Local and national Public/Private Partnerships (e.g., Fusion Centers)			
					Task 1.05. Develop, implement, and manage employee security awareness programs to achieve organizational goals and objectives Knowledge of:			
					1.05.01. Training methodologies			
					1.05.02. Communication strategies, techniques, and methods			
					1.05.03. Awareness program objectives and program metrics			
					1.05.04. Elements of a security awareness program (e.g., roles and responsibilities, physical risk, communication risk, privacy)			
II. Business Principles and Practices (13%)								
					Task 2.01. Develop and manage budgets and financial controls to achieve fiscal responsibility Knowledge of:			
					2.01.01. Principles of management accounting, control, and audits			
					2.01.02. Business finance principles and financial reporting			
					2.01.03. Return on Investment (ROI) analysis			
					2.01.04. The lifecycle for budget planning purposes			
					Task 2.02. Develop, implement, and manage policies, procedures, plans, and directives to achieve organizational objectives Knowledge of:			
					2.02.01. Principles and techniques of policy/procedures development			
					2.02.02. Communication strategies, methods, and techniques			
					2.02.03. Training strategies, methods, and techniques			
					2.02.04. Cross-functional collaboration			
					2.02.05. Relevant laws and regulations			
					Task 2.03. Develop procedures/techniques to measure and improve organizational productivity Knowledge of:			
					2.03.01. Techniques for quantifying productivity/metrics/key performance indicators (KPI)			


Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress		
1	2	3	4	5			Hours of Study	Date Study Complete	
					2.03.02.	Data analysis techniques and cost-benefit analysis			
					2.03.03.	Improvement techniques (e.g., pilot programs, education and training)			
					Task 2.04. Develop, implement, and manage security staffing processes and personnel development programs in order to achieve organizational objectives				
					Knowledge of:				
					2.04.01.	Interview techniques for staffing			
					2.04.02.	Candidate selection and evaluation techniques			
					2.04.03.	Job analysis processes			
					2.04.04.	Pre-employment background screening			
					2.04.05.	Principles of performance evaluations, 360° reviews, and coaching			
					2.04.06.	Interpersonal and feedback techniques			
					2.04.07.	Training strategies, methodologies, and resources			
					2.04.08.	Retention strategies and methodologies			
					2.04.09.	Talent management and succession planning			
					Task 2.05. 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:				
					2.05.01.	Good governance standards			
					2.05.02.	Guidelines for individual and corporate behavior			
					2.05.03.	Generally accepted ethical principles			
					2.05.04.	Confidential information protection techniques and methods			
					2.05.05.	Legal and regulatory compliance			
					Task 2.06. Provide advice and assistance to management and others in developing performance requirements and contractual terms for security vendors/suppliers				
					Knowledge of:				
					2.06.01.	Key concepts in the preparation of requests for proposals and bid reviews/evaluation			
					2.06.02.	Service Level Agreements (SLA) definition, measurement, and reporting			
					2.06.03.	Contract law, indemnification, and liability insurance principles			
					2.06.04.	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 (10%)								
					Task 3.01. Identify, develop, implement, and manage investigative functions Knowledge of:			
					3.01.01. Principles and techniques of policy and procedure development			
					3.01.02. Organizational objectives and cross-functional collaboration			
					3.01.03. Types of investigations (e.g., incident, misconduct, compliance)			
					3.01.04. Internal and external resources to support investigative functions			
					3.01.05. Report preparation for internal purposes and legal proceedings			
					3.01.06. Laws pertaining to developing and managing investigative programs			
					Task 3.02. Manage or conduct the collection and preservation of evidence to support investigation actions Knowledge of:			
					3.02.01. Evidence collection techniques			
					3.02.02. Protection/preservation of crime scene			
					3.02.03. Requirements of chain of custody			
					3.02.04. Methods for preservation of evidence			
					3.02.05. Laws pertaining to the collection and preservation of evidence			
					Task 3.03. Manage or conduct surveillance processes Knowledge of:			
					3.03.01. Surveillance techniques			
					3.03.02. Technology/equipment and human resources			
					3.03.03. Laws pertaining to managing surveillance processes			
					Task 3.04. Manage and conduct investigations requiring specialized tools, techniques, and resources Knowledge of:			
					3.04.01. Techniques, tools, and resources related to: <ul style="list-style-type: none"> ▪ financial and fraud related crimes ▪ intellectual property and industrial espionage crimes ▪ arson and property crimes ▪ cybercrimes 			
					Task 3.05. Manage or conduct investigative interviews Knowledge of:			
					3.05.01. Methods and techniques of eliciting information			

Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
						3.05.02. Techniques for detecting deception		
						3.05.03. The nature of non-verbal communication and cultural considerations		
						3.05.04. Rights of interviewees		
						3.05.05. Required components of written statements		
						3.05.06. Laws pertaining to managing investigative interviews		
						Task 3.06. Provide coordination, assistance, and evidence such as documentation and testimony to support legal counsel in actual or potential criminal and/or civil proceedings		
						Knowledge of:		
						3.06.01. Statutes, regulations, and case law governing or affecting the security industry and the protection of people, property, and information		
						3.06.02. Criminal law and procedures		
						3.06.03. Civil law and procedures		
						3.06.04. Employment law (e.g., wrongful termination, discrimination, and harassment)		
IV. Personnel Security (12%)								
						Task 4.01. Develop, implement, and manage background investigations for hiring, promotion, or retention of individuals		
						Knowledge of:		
						4.01.01. Background investigations and personnel screening techniques		
						4.01.02. Quality and types of information sources		
						4.01.03. Screening policies and guidelines		
						4.01.04. Laws and regulations pertaining to personnel screening		
						Task 4.02. Develop, implement, manage, and evaluate policies, procedures, programs and methods to protect individuals in the workplace against human threats (e.g., harassment, violence)		
						Knowledge of:		
						4.02.01. Protection techniques and methods		
						4.02.02. Threat assessment		
						4.02.03. Prevention, intervention, and response tactics		
						4.02.04. Educational and awareness program design and implementation		
						4.02.05. Travel security programs		
						4.02.06. Laws, government, and labor regulations regarding organizational efforts to reduce employee substance abuse		

Rate Understanding						Domains and Tasks of the CPP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 4.03. Develop, implement, and manage executive protection programs Knowledge of:			
					4.03.01. Executive protection techniques and methods			
					4.03.02. Risk analysis			
					4.03.03. Liaison and resource management techniques			
					4.03.04. Selection, costs, and effectiveness of proprietary and contract executive protection personnel			
V. Physical Security (25%)								
					Task 5.01. Conduct facility surveys to determine the current status of physical security Knowledge of:			
					5.01.01. Security protection equipment and personnel			
					5.01.02. Survey techniques			
					5.01.03. Building plans, drawings, and schematics			
					5.01.04. Risk assessment techniques			
					5.01.04. Gap analysis			
					Task 5.02. Select, implement, and manage physical security strategies to mitigate security risks Knowledge of:			
					5.02.01. Fundamentals of security system design			
					5.02.02. Countermeasures			
					5.02.03. Budgetary projection development process			
					5.02.04. Bid package development and evaluation process			
					5.02.05. Vendor qualification and selection process			
					5.02.06. Final acceptance and testing procedures			
					5.02.07. Project management techniques			
					5.02.08. Cost-benefit analysis techniques			
					5.02.09. Labor-technology relationship			
					Task 5.03. Assess the effectiveness of the security measures by testing and monitoring Knowledge of:			
					5.03.01. Protection personnel, technology, and processes			
					5.03.02. Audit and testing techniques			
					5.03.03. Preventive and corrective maintenance for systems			

Rate Understanding						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 6.01. Conduct surveys of information asset facilities, processes, systems, and services to evaluate current status of information security program Knowledge of:			
					6.01.01. Elements of an information security program, including physical security, procedural security, information systems security, employee awareness, and information destruction and recovery capabilities			
					6.01.02. Survey techniques			
					6.01.03. Quantitative and qualitative risk assessments			
					6.01.04. Risk mitigation strategies (e.g., technology, personnel, process, facility design)			
					6.01.05. Cost-benefit analysis methods			
					6.01.06. Protection technology, equipment, and procedures			
					6.01.07. Information security threats			
					6.01.08. Building and system plans, drawings, and schematics			
					Task 6.02. 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:			
					6.02.01. Principles of management			
					6.02.02. Information security theory and terminology			
					6.02.03. Information security industry standards (e.g., ISO, PII, PCI)			
					6.02.04. Relevant laws and regulations regarding records management, retention, legal holds, and destruction practices			
					6.02.05. Practices to protect proprietary information and intellectual property			
					6.02.06. 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 6.03. Develop and manage a program of integrated security controls and safeguards to ensure information asset protection including confidentiality, integrity, and availability Knowledge of:			
					6.03.01. 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			
					6.03.02. Information security theory and systems methodology			
					6.03.03. Multi-factor authentication techniques			
					6.03.04. Threats and vulnerabilities assessment and mitigation			
					6.03.05. Ethical hacking and penetration testing techniques and practices			
					6.03.06. Encryption and data masking techniques			
					6.03.07. Systems integration techniques			
					6.03.08. Cost-benefit analysis methodology			
					6.03.09. Project management techniques			
					6.03.10. Budget development process			
					6.03.11. Vendor evaluation and selection process			
					6.03.12. Final acceptance and testing procedures, information systems, assessment, and security program documentation			
					6.03.13. Protection technology, investigations, and procedures			
					6.03.14. 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 7.01. Assess and prioritize threats to mitigate potential consequences of incidents Knowledge of:			
					7.01.01. Threats by type, likelihood of occurrence, and consequences			
					7.01.02. "All hazards" approach to assessing threats			
					7.01.03. Cost-benefit analysis			
					7.01.04. Mitigation strategies			
					7.01.05. Risk management and business impact analysis methodology			
					7.01.06. Business Continuity standards (e.g., ISO 22301)			
					Task 7.02. Prepare and plan how the organization will respond to incidents Knowledge of:			
					7.02.01. Resource management techniques			
					7.02.02. Emergency planning techniques			
					7.02.03. Triage and damage assessment techniques			
					7.02.04. Communication techniques and notification protocols			
					7.02.05. Training and exercise techniques			
					7.02.06. Emergency operations center (EOC) concepts and design			
					7.02.07. Primary roles and duties in an incident command structure			
					Task 7.03. Respond to and manage an incident Knowledge of:			
					7.03.01. Resource management techniques			
					7.03.02. EOC management principles and practices			
					7.03.03. Incident management systems and protocols			
					Task 7.04. Recover from incidents by managing the recovery and resumption of operations Knowledge of:			
					7.04.01. Resource management techniques			
					7.04.02. Short and long-term recovery strategies			
					7.04.03. Recovery assistance resources			
					7.04.04. 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						Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
I. Case Management (29%)								
					Task 1.01. Analyze case for applicable ethical conflicts Knowledge of:			
					1.01.01. Conflict resolution elements			
					1.01.02. Nature/types/categories of ethical issues related to cases (fiduciary, conflict of interest, attorney-client)			
					1.01.03. Applicable aspects of laws, codes, and regulations			
					Task 1.02. Analyze and assess case elements and strategies Knowledge of:			
					1.02.01. Case categories (computer, white collar, financial, criminal, etc.)			
					1.02.02. Analytical methods for data			
					1.02.03. Strategic/operational analysis			
					1.02.04. Lethality of crime intelligence			
					Task 1.03. Determine need and develop strategy by reviewing procedural options Knowledge of:			
					1.03.01. Case flow			
					1.03.02. Negotiation process			
					1.03.03. Investigative methods			
					1.03.04. Cost-benefit analysis			
					1.03.05. Applicable areas of laws, codes, and regulations			
					Task 1.04. Manage and implement investigative resources necessary to address case objectives Knowledge of:			
					1.04.01. Manpower and assignment			
					1.04.02. Time management			
					1.04.03. Quality assurance process			
					1.04.04. Review chain of custody procedures			
					Task 1.05. Identify and evaluate investigative process improvement opportunities Knowledge of:			
					1.05.01. Management/legal review			
					1.05.02. Liaison resources			
					1.05.03. Internal and external analysis			
					1.05.04. Resolution			

Rate Understanding						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 2.01. Conduct surveillance by physical and electronic means in order to obtain relevant information Knowledge of:			
					2.01.01. Methods of surveillance			
					2.01.02. Types of surveillance			
					2.01.03. Types of surveillance equipment			
					2.01.04. Pre-surveillance routines			
					2.01.05. Applicable aspects of laws, codes, and regulations			
					2.01.06. Documentation of surveillance activities			
					Task 2.02. Conduct interviews/interrogations of witnesses and subjects to obtain relevant information Knowledge of:			
					2.02.01. Interview and interrogation techniques (electronic, face-to-face, telephone)			
					2.02.02. Techniques for detecting deception (e.g., non-verbal communication)			
					2.02.03. Methods and techniques of eliciting admission and/or confession			
					2.02.04. Documentation and completion of witness/subject statement			
					2.02.05. Applicable aspects of laws, codes, and regulations (e.g., individual rights, privacy, interrogation)			
					Task 2.03. Collect and preserve objects and data for assessment and analysis Knowledge of:			
					2.03.01. Requirements of chain of custody			
					2.03.02. Methods/procedures for seizure of various types of evidence			
					2.03.03. Methods/procedures for preserving various types of evidence			
					2.03.04. Forensic opportunities and resources			
					2.03.05. Applicable aspects of laws, codes, and regulations (e.g., rules of evidence and discovery)			
					Task 2.04. Conduct research by physical and electronic means and analyze data to obtain relevant information Knowledge of:			
					2.04.01. Methods of research using physical resources			
					2.04.02. Methods of research using electronic resources			
					2.04.03. Methods of analysis of research results			
					2.04.04. Documentation and reporting of analytical efforts			
					2.04.05. Applicable aspects of laws, codes, and regulations			


Rate Understanding						Domains and Tasks of the PCI Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 2.05. Collect and report relevant information Knowledge of:			
					2.05.01. Obtaining information from federal, state, and local agencies			
					2.05.02. Obtaining information from companies and private/public enterprises (e.g., mutual aid)			
					2.05.03. Documentation and reporting of information			
					2.05.04. Applicable aspects of laws, codes, and regulations			
					Task 2.06. Use computers/digital media to gather information/evidence Knowledge of:			
					2.06.01. Concepts and principles of computer operations and digital media			
					2.06.02. Concepts and principles of digital forensics			
					2.06.03. Computers to retrieve, store and document digital information			
					2.06.04. Documentation and reporting of information			
					2.06.05. Applicable aspects of laws, codes, and regulations			
					Task 2.07. Use special investigative techniques to gather critical information/evidence Knowledge of:			
					2.07.01. Concepts, principles, and methods of polygraph examinations			
					2.07.02. Concepts, principles, and methods of video/audio recordings			
					2.07.03. Concepts, principles, and methods of forensic analysis (e.g., handwriting documents, fingerprints, DNS, biometrics, chemicals, fluids, etc.)			
					2.07.04. Concepts, principles, methods of undercover investigations			
					2.07.05. Documentation and reporting of information			
					2.07.06. Applicable aspects of laws, codes, and regulations			
					2.07.07. Development 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 (21%)								
					Task 3.01. Prepare report to substantiate investigative findings Knowledge of:			
					3.01.01. Critical elements and format of an investigative report			
					3.01.02. Investigative terminology			
					3.01.03. Logical sequencing of information			
					3.01.04. Applicable aspects of laws, codes, and regulations			
					Task 3.02. Prepare and present testimony by reviewing case files, meeting with counsel, and presenting relevant facts Knowledge of:			
					3.02.01. Witness preparation			
					3.02.02. Types of testimony			
					3.02.03. Applicable aspects of laws, codes, and regulations (e.g., applicable privileges, hearsay, rules of procedure)			


PCI Exam Domains

Case Management	29%
Investigative Techniques and Procedures	50%
Case Presentation	21%

Rate Understanding						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 (33%)								
					Task 1.01. Identify assets to determine their value loss impact and criticality Knowledge of:			
					1.01.01. The nature and types of assets (tangible and intangible)			
					1.01.02. Valuing various types of assets			
					1.01.03. Definitions and terminology related to assets, value, loss impact and criticality			
					1.01.04. Core functions of the place			
					1.01.05. Current security programs and security management of the place process			
					Task 1.02. Assess the nature of threats so that the scope of the problem can be determined Knowledge of:			
					1.02.01. The nature, categories, and types of threats (e.g., natural, man-made)			
					1.02.02. Different environmental types and severity (e.g., natural disasters, criminal events, terrorism, socio-political, cultural)			
					1.02.03. Demographics (crime population)			
					1.02.04. Critical business operations of various types of places or processes			
					1.02.05. External organizations and their potential impact on facility's security program			
					1.02.06. Other external factors (legal, loss of reputation, economics, etc.) and their impact on the facility's security program			
					Task 1.03. Conduct a physical security survey in order to identify the vulnerabilities of the organization Knowledge of:			
					1.03.01. Security survey techniques			
					1.03.02. Qualitative and quantitative risk assessments			
					1.03.03. Crime prevention through environmental design (CPTED)			
					1.03.04. Situational crime prevention			
					1.03.05. Security technologies and equipment applications			
					1.03.06. Interpretation of building plans, drawings and schematics			
					1.03.07. Nature and types of data to be collected			
					1.03.08. Methods of collecting relevant data			
					1.03.09. Existing equipment, physical security systems, personnel, and procedures			
					1.03.10. Fault tolerance (i.e., ability of a system to withstand failure)			
					1.03.11. Applicable standards/regulations/codes and where to find them			
					1.03.12. Environmental conditions that impact the security level of the place or process			

Rate Understanding						Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					Task 1.04. Perform a risk analysis so that appropriate countermeasures can be developed Knowledge of:			
					1.04.01. Risk analyses strategies and methods			
					1.04.02. Risk management principles			
					1.04.03. Methods for analysis and interpretation of collected data			
					1.04.04. Threat and vulnerability identification			
					1.04.05. Loss event profile analyses			
					1.04.06. Methods of evaluating criticality and probability			
					1.04.07. Appropriate countermeasures related to specific threats			
					1.04.08. Cost-benefit analysis (e.g., return on investment [ROI] analysis, total cost of ownership)			
					1.04.09. Legal issues related to various countermeasures/security applications			
II. Application, Design, and Integration of Physical Security Systems (38%)								
					Task 2.01. Establishing security system requirements and performance specifications Knowledge of:			
					2.01.01. Design constraints (e.g., regulations, budget, cost, technical capability, systems design capacities and limitations; materials, equipment and system compatibility)			
					2.01.02. Applicability of risk analysis results			
					2.01.03. Relevant security terminology and concepts			
					2.01.04. Applicable codes, standards and guidelines			
					2.01.05. Methods of setting priorities			
					2.01.06. Types of security measures			
					2.01.07. Functional requirements			
					2.01.08. Performance requirements			
					2.01.09. Commissioning requirements			
					2.01.10. Success metrics			
					Task 2.02. Apply physical security measures and select appropriate system components Knowledge of:			
					2.02.01. Barriers (e.g., fencing, doors, gates, beams, bollards, barriers)			
					2.02.02. Security lighting			
					2.02.03. Biometrics and credentials			

Rate Understanding						Domains and Tasks of the PSP Certification Exam	Track Progress	
1	2	3	4	5			Hours of Study	Date Study Complete
					2.02.04. Duress systems			
					2.02.05. Target hardening (e.g., blast mitigation, strategies, ballistic protection)			
					2.02.06. Access control (physical and electronic)			
					2.02.07. Intrusion detection applications (interior and exterior sensors)			
					2.02.08. Analog closed circuit television (CCTV) and IP video, cameras, controls, recording, and storage devices			
					2.02.09. Personal, package, and vehicle screening			
					2.02.10. Emergency notification systems			
					2.02.11. Security computer systems (hardware, software, peripherals)			
					2.02.12. Principles of data storage and management			
					2.02.13. Principles of network infrastructure and network security			
					2.02.14. Security audio communications (radio, telephone, intercom, IP audio)			
					2.02.15. Systems monitoring, display, and supervision types (field panels, multiplexers, control centers/consoles)			
					2.02.16. Systems redundancy alternative power sources (battery, UPS, generators, surge protection)			
					2.02.17. Signal and data transmission methods			
					2.02.18. Equipment and system maintenance requirements			
					2.02.19. System operations manpower requirements			
					2.02.20. Identity management (PII)			
					Task 2.03. System design and integration and recommendations			
					Knowledge of:			
					2.03.01. Design phases (pre-design, schematic design, design development, construction documents, and cutover plan)			
					2.03.02. Design elements (calculations, drawings, specifications, review of manufacturer's submittals and technical data)			
					2.03.03. Construction specification standards (CSI)			
					2.03.04. Systems integration (technical approach, connecting with non-security systems)			
					2.03.05. Project management strategy			
					2.03.06. Scheduling (Gantt charts, PERT charts, milestones and objectives)			
					2.03.07. Cost estimates and cost-benefit analysis			
					2.03.08. Value engineering			
					2.03.09. Passive and active designs			
					2.03.10. Major report elements			

Rate Understanding						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 (29%)								
					Task 3.01. Outline criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation Knowledge of:			
					3.01.01. Bid package components			
					3.01.02. Criteria for evaluation of bids			
					3.01.03. Technical compliance criteria			
					3.01.04. Ethics in contracting			
					Task 3.02. Procure system and implement recommended solutions to solve problems identified Knowledge of:			
					3.02.01. Project management functions and processes throughout the system life cycle			
					3.02.02. System integration			
					3.02.03. Vendor pre-qualification (interviews and due diligence)			
					3.02.04. Configuration management			
					3.02.05. Procurement process			
					Task 3.03. Conduct final acceptance testing and implement/provide procedures for ongoing monitoring and evaluation of the measures Knowledge of:			
					3.03.01. Installation/maintenance inspection techniques			
					3.03.02. Commissioning			
					3.03.03. Installation problem resolution (punchlists)			
					3.03.04. Test and acceptance criteria			
					3.03.05. Warranty types			
					3.03.06. End-user training requirements			
					3.03.07. Ongoing maintenance and inspection requirements			

PSP Exam Domains

Physical Security Assessment	33%
Application, Design, and Integration of Physical Security Systems	38%
Implementation of Physical Security Measures	29%

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, or PSP certification 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, as 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, or PSP 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 system requirements and performance specifications**Knowledge of:** 2.01.04. 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.
- ✓ 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, and PSPs 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, and PSP 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

Questions for the examination are obtained from two sources:

- a. For the CPP and PCI: Item Development Groups and Legal Aspect Committees (ASIS). For the PSP which does not have legal questions: only the Item Development Group.
- b. Individual CPPs, PCIs, and PSPs may submit questions for their respective exam to receive recertification credit. These questions are developed with the direction of an item-writing guide available from the Certification program office.

After the questions are drafted, they are reviewed at several different stages for content, accuracy, consistency of style, appropriate reading level, psychometric soundness, and freedom from cultural bias or unequal impact.

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 of the other two ASIS certifications within 3 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 role delineation 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 testing service. From the results of the study, the PCB establishes the number of examination questions that must be answered correctly 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 role delineation 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.

SCALED SCORE

In order to maintain test security, the PCB produces multiple forms of the CPP, PCI, and PSP 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 or not 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.

ITEM ANALYSIS

Test items are evaluated after a statistically significant number of candidates answered them in an examination environment. If they are intended to be scored as part of the examination, or are included as pretest items, their performance will be examined, and any aberrant items will be called to the attention of, and reviewed by, the PCB Test Management Committee. The committee examines each item to detect any possible flaws or ambiguities. If changes need to be made in an operational question, the scoring process incorporates credit for two or more answer options in the final scoring and the item is revised before it is used again in another form.

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 number of questions they answered correctly versus the total number of question in the domain.

About the CPP Exam

The CPP exam consists of 200 scored multiple-choice questions and may contain 25 “pre-test” (unscored) questions randomly distributed throughout the examination for a total of 225 questions. The time allowed takes into consideration the review of pre-test 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 “pre-test” (unscored) questions randomly distributed throughout the examination for a total of 140 questions. The time allowed takes into consideration the review of pre-test 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 (29%)
- Investigative Techniques and Procedures (50%)
- Case Presentation (21%)

About the PSP Exam

The PSP exam consists of 125 multiple-choice questions and may contain 25 “pre-test” (unscored) questions randomly distributed throughout the examination for a total of 140 questions. The time allowed takes into consideration the review of pre-test 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 (33%)
- Application, Design, and Integration of Physical Security Systems (38%)
- Implementation of Physical Security Measures (29%)

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.

- Approved candidates should 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 to be taken to the testing center at the time of the exam.
- Exam can also be scheduled through a secure website <http://www.prometric.com/asis>.

Fees and Policies

ASIS exams are offered at Prometric testing locations across the globe. Pencil and Paper tests are available in certain locations.

Computer-Based Test

- ASIS members: \$300
- Nonmembers: \$450

Paper and Pencil Exams

Only available in Australia (Queensland), Costa Rica, Ecuador, Jamaica, Nigeria (Lagos and Port Harcourt), Panama, and Trinidad/Tobago

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

- ASIS members: \$200
- Nonmembers: \$350

Computer-Based Retest

- ASIS members: \$200
- Nonmembers: \$200

Paper and Pencil Retest

Only available in Australia (Queensland), Costa Rica, Ecuador, Jamaica, Nigeria (Lagos and Port Harcourt), Panama, and Trinidad/Tobago

- ASIS members: \$100
- 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 non-members. The Paper and Pencil test refund is currently \$100 for members and \$250 for non-members. Testing fees will be returned or credited to your account.

G.I. Bill

Qualified U.S. applicants may receive reimbursement for the certification exams through the G.I. Bill. An application is available at www.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 \$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.



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