

ASIS INTERNATIONAL
**BOARD
CERTIFICATION
HANDBOOK**



CPP

PCI **PSP** **APP**

ASIS INTERNATIONAL CONTACT INFORMATION

ASIS is here to help! This Handbook covers all the information on ASIS' four certification programs. If you have questions after reviewing the Handbook, please contact the Certification Team at:

EMAIL: certification@asisonline.org

PHONE: +1 703.519.6200

WEBSITE: asisonline.org

ADDRESS:

ASIS International
1625 Prince Street
Alexandria, Virginia
22314-2882, USA

OFFICE HOURS: Monday through Friday,
9:00 am to 5:00 pm, Eastern Standard Time (except holidays).

CONTENTS

ASIS International Board Certifications	6
ASIS Professional Certification Board (PCB).....	6
ASIS International Certification Programs	6
Certification vs. Certificate Programs	7
Why Choose an ASIS Certification?.....	7
Which Exam is Right for You?	7
Eligibility Requirements for all Applicants	8
APP: Board Certification in Security Management Fundamentals.....	9
APP Eligibility Requirements.....	9
APP Eligibility Requirements with an ASIS Certification	9
APP Body of Knowledge.....	10
CPP: Board Certification in Security Management	15
CPP Eligibility Requirements.....	15
CPP Body of Knowledge	16
PCI: Board Certification in Investigations	21
PCI Eligibility Requirements	21
PCI Body of Knowledge	22
PSP: Board Certification in Physical Security	24
PSP Eligibility Requirements	24
PSP Body of Knowledge	25
Program Changes and Updates	28
Applying for the Exams	28
Application Documents You'll Need:	28
Deadline Reminders.....	28
Application Fees.....	28
Refunds	28
Retesting	28
Approval Notification from ASIS	28

Appealing a Declined Application	29
PCB Certificant Relations Appeal Process	29
Scheduling Your Exam	29
Making Your Exam Appointment	29
Testing Accommodations for Candidates with Disabilities and Other Special Considerations ..	30
Extension Policies – Exam Applications	30
“No Shows”	30
On Exam Day	31
Check-in Procedures	31
What to Bring and Not Bring	32
During the Exam	32
Exam Results	32
Weather Emergencies	32
How Are the Exams Structured?	32
Scoring the Exam	33
Studying for the Exam	33
Exam Preparation Resources	33
Free Study Tools	34
I Passed the Exam, Now What?	34
Recertification	35
ASIS Application and Certificant Policies	35
Statement of Impartiality	35
ASIS Certification Code of Professional Responsibility	35
Attestation of Continued Eligibility for Certification	35
Revocation of Certification	36
Lifetime Designation	36
Release of Candidate and Certificant Information	37
ASIS Certificates	37
Filing a Complaint	37
About Our Testing Partner	37

About This Handbook

This Handbook contains all the policies and procedures of ASIS's four certification programs. All those applying to take an ASIS certification exam must agree to comply with the information contained in this manual. **This handbook was updated 3 May 2019 and supersedes all previous versions.**

ASIS INTERNATIONAL BOARD CERTIFICATIONS

ASIS International was the first organization to offer a credential specifically for security managers, and our programs remains the global standard. Developed by practitioners for practitioners, ASIS board certifications provide you with a competitive edge.

Distinguished by their global development and application, ASIS certifications are transferable across all industry sectors and geographic borders. The role and tasks of security managers are researched and documented to define each certification. In addition, a job analysis is routinely conducted to ensure the exams reflect current practices.

Our requirements are demanding and consequently, our certifications are held only by a distinguished group of professionals. Earning your CPP®, PCI®, PSP®, or APP conveys to your peers, employees, and employer that you possess substantial, relevant experience as well as demonstrated and tested competence.



AN INTERNATIONALLY RECOGNIZED, GLOBALLY ACCREDITED PROGRAM

ASIS board certifications are developed and maintained through a rigorous process exemplified through the program's accreditation by the American National Standards Institute (ANSI) against the International Organization for Standardization (ISO) 17024.

ASIS will apply for ANSI/ISO 17024 accreditation for the new Associate Protection Professional (APP) program once we have met the minimum requirements.



THE SAFETY ACT DESIGNATION

ASIS board-certified professionals, their employers, and their customers are protected from lawsuits involving the ASIS certification process that arise out of an act of terrorism.



The American Council on Education® has reviewed and recommended college credit equivalency for the ASIS International certifications CPP, PCI, and PSP programs.*

*The ACE CREDIT logo is a federally registered trademark of the American Council on Education and cannot be used or reproduced without the express written permission of the American Council on Education.

ASIS PROFESSIONAL CERTIFICATION BOARD (PCB)

The ASIS certification programs are governed by the Professional Certification Board (PCB). The PCB establishes all policies related to the program including eligibility requirements, body of knowledge, and exam development. All PCB members are CPP, PCI, PSP and/or APP certified.

Members of the Professional Certification Board (PCB) manage the certification programs by assuring that standards are developed and maintained, quality assurance is in place, and the exams accurately reflect the duties and responsibilities of security professionals in the areas of security management, investigations, and physical security. The PCB is a committee of the ASIS Board of Directors. Members of the PCB are chosen through a nomination process. The board meets three times per year.

ASIS INTERNATIONAL CERTIFICATION PROGRAMS

Certification serves as a visible acknowledgment of your demonstrated mastery of core security principles and skills essential to the best practice of security management.

However, not all certifications are equal. To truly set yourself apart, you need a certification that encourages professional growth. One that is globally recognized as the standard for professionalism. You need an ASIS Board Certification.

By earning a CPP, PCI, PSP, or APP, your employer, clients, and colleagues will instantly recognize you as the “best of the best.” Earning an ASIS certification is a milestone accomplishment that will help you reach your career goals.

Certification vs. Certificate Programs

People are often unclear about the difference between a certification program and a certificate program. The goal of both types of programs are meant for professional development of industry experts.

Professional certification (such as the CPP, PCI, PSP, or APP) is the voluntary process by which a third-party organization grants a time-limited recognition and use of a credential to an individual after verifying that he or she has met predetermined and standardized criteria, usually through eligibility requirements and an exam. Most professional certification programs require that certificants recertify their designation after a set amount of time to ensure they are remaining current and knowledgeable in the industry.

A **certificate program** is a training program on a specialized topic for which participants receive a certificate after completing the course. Some certificate programs require attendees to pass an assessment of some kind to verify they’ve learned what the class was teaching. Many certificate programs will provide a “certificate of completion” at the end of the course. ASIS offers a number of certificate programs, many of which can be used to acquire Continuing Professional Education (CPE) credits that can be used to prepare for ASIS’ certification programs or used to recertify your designation.

Why Choose an ASIS Certification?

- ◆ Elevate your professional stature and peer recognition
- ◆ Gain a competitive edge in job placement or advancement within your organization
- ◆ Realize deep personal satisfaction and professional achievement
- ◆ Broaden your knowledge base

- ◆ Keep updated on best practices
- ◆ Achieve global recognition as a highly motivated expert in your field

ASIS board certified practitioners are leaders, willing mentors, and trusted strategic partners, serving both their organizations and the profession.

Today, security professionals from 85 countries proudly maintain their ASIS board certifications.

Which Exam is Right for You?

ASIS offers four certifications for those in security-related fields:

- ◆ Certified Protection Professional (CPP)
- ◆ Professional Certified Investigator (PCI)
- ◆ Physical Security Professional (PSP)
- ◆ Associate Protection Professional (APP)

Some professionals hold one ASIS certification, some two, and some hold three (the APP cannot be held in conjunction with the CPP). Here is an overview of all four programs:

- ◆ **The Certified Protection Professional (CPP)** program is designed for those who have demonstrated competency in all areas of security management.
- ◆ **The Professional Certified Investigator (PCI)** program is designed for those whose responsibilities include case management, evidence collections, and preparation of reports and testimony to substantiate findings.
- ◆ **The Physical Security Professional (PSP)** program is designed for those whose primary responsibility is to conduct threat surveys, design integrated security systems that include equipment, procedures and people, or install, operate, and maintain those systems.
- ◆ **The Associate Protection Professional (APP)** program is designed for those with 1-4 years of experience in the fundamentals of security management.

ASIS highly recommends reviewing the body of knowledge for each program (outlined below). All questions on the exams relate to one of the domains listed in each program’s body of knowledge. Using the body of knowledge, make an honest assessment of your

own experiences in each domain. Not only will this help you decide which exam is right for you; it will also help you structure your study requirements.

ELIGIBILITY REQUIREMENTS FOR ALL APPLICANTS

The following pages outline the eligibility requirements and body of knowledge for each ASIS certification program. In addition to the specific eligibility requirements below, **all applicants and certificants must:**

- ◆ Have been employed full-time in a security-related role.
- ◆ Not have been convicted of any criminal offense that would reflect negatively on the security profession, ASIS, or the certification program
- ◆ Sign and agree to abide by the ASIS Certification Code of Professional Responsibility (see pg. 35)
- ◆ Agree to abide by the policies of the ASIS Certification programs as described in this handbook and the ASIS Recertification Guide.

Associate Protection Professional

APP: BOARD CERTIFICATION IN SECURITY MANAGEMENT FUNDAMENTALS

ASIS International is proud to announce the launch of the new Associate Protection Professional (APP) certification program, which is part of ASIS International’s ongoing strategy to offer professional development and educational opportunities for professionals at all levels of the security management field.

The **Associate Protection Professional (APP)** designation is intended for those with 1-4 years of security management experience. The exam will measure the professional’s knowledge of security management fundamentals, business operations, risk management, and response management.

APP Eligibility Requirements

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

*Security management experience is defined as the individual having been personally engaged in security or loss prevention on a full-time basis, or as a primary duty. Included is:

- A. Experience as a security professional in the protection of assets, in the public or private

- sector, criminal justice system, government intelligence, or investigative agencies.
- B. Experience with companies, associations, government, or other organizations providing services or products, including consulting firms, provided the duties and responsibilities substantively relate to the design, evaluation, and application of systems, programs, or equipment, or development and operation of services, for protection of assets in the private or public sectors.
- C. Experience as a full-time educator on the faculty of an accredited educational institution, provided the responsibilities for courses and other duties relate primarily to knowledge areas pertinent to the management and operation of protection of assets programs in the public or private sectors.

APP Eligibility Requirements with an ASIS Certification

The chart below shows how the eligibility requirements would be altered for those holding the new APP designation

CPP	With Degree	No Degree
Current Experience Requirements	7 years	9 years
With an APP	5 years	7 years
PCI	With Degree	No Degree
Current Experience Requirements	5 years	5 years
With an APP	4 years	4 years
PSP	With Degree	No Degree
Current Experience Requirements	4 years	6 years
With an APP	3 years	5 years

- 1. Other eligibility requirements for the CPP, PCI, or PSP still need to be met (e.g., responsible charge or case management)

2. The APP designation will be expired if a candidate obtains the CPP (you cannot hold both designations at the same time)
3. Those who are already PCI- and/or PSP-certified will be eligible to take the APP exam (provided they meet the requirements of the individual program)
4. **CPPs are not be permitted to take the APP exam**

APP BODY OF KNOWLEDGE

To be awarded the APP designation, a candidate must pass a comprehensive examination consisting of approximately 125 multiple-choice questions; 100 “live,” scoreable questions and up to 25 pre-test questions. Knowledge in four major areas (domains) is tested.

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

DOMAIN ONE

Security Fundamentals (35%)

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

Knowledge of

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

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

Knowledge of

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

3. Audit and testing techniques

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

Knowledge of

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

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

Knowledge of

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

TASK 5: Implement and/or coordinate an investigative program

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

DOMAIN TWO

Business Operations (22%)

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

Knowledge of

1. Data analysis techniques and cost-benefit analysis
2. Principles of business management accounting, control, and audits
3. Return on Investment (ROI) analysis
4. Fundamental business finance principles and financial reporting
5. Budget planning process

6. Required components of effective documentation (e.g., budget, balance sheet, vendor work order, contracts)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Interpersonal communications and feedback techniques
2. Relevant laws and regulations
3. Governance and compliance standards
4. Generally accepted ethical principles

5. Guidelines for individual and corporate behavior

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

DOMAIN THREE

Risk Management (25%)

TASK 1: Conduct initial and ongoing risk assessment processes

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

DOMAIN FOUR

Response Management (18%)

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

Knowledge of

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

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

Knowledge of

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

TASK 3: Conduct a post-incident review

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

TASK 8: Coordinate with emergency services during incident response

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

Certified Protection Professional

CPP: BOARD CERTIFICATION IN SECURITY MANAGEMENT

The gold standard for more than 40 years, the Certified Protection Professional (CPP®) credential provides demonstrable proof of knowledge and management skills in seven key domains of security.

Earning a CPP provides independent confirmation of your ability to assume leadership responsibilities and effectively manage broad security concerns.

CPP Eligibility Requirements

Candidates wishing to take the CPP examination must meet the following eligibility requirements:

WORK EXPERIENCE

Without higher education degree:

Nine (9) years of security experience*, at least three (3) years of which shall have been in responsible* charge of a security function

OR

Hold the APP and seven (7) years of security experience*, at least three (3) years of which shall have been in responsible charge** of a security function.

With a higher education degree:

Earned a Bachelor's Degree or higher from an accredited institution of higher education and have seven (7) years of security experience*, at least three (3) years of which shall have been in responsible charge** of a security function.

OR

Hold the APP, earned a Bachelor's Degree or higher from an accredited institution of higher education and have five (5) years of security experience*, at least three (3) years of which shall have been in responsible charge** of a security function.

*Experience is defined as the individual having been personally engaged in security or loss prevention on a

full-time basis (internships are not permitted), or as a primary duty. Included is:

- a.) Experience as a security professional in the protection of assets, in the public or private sector, criminal justice system, government intelligence, or investigative agencies.
- b.) Experience with companies, associations, government, or other organizations providing services or products, including consulting firms, provided the duties and responsibilities substantively relate to the design, evaluation, and application of systems, programs, or equipment, or development and operation of services, for protection of assets in the private or public sectors.
- c.) Experience as a full-time educator on the faculty of an accredited educational institution, provided the responsibilities for courses and other duties relate primarily to knowledge areas pertinent to the management and operation of protection of assets programs in the public or private sectors.

**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.

CPP BODY OF KNOWLEDGE

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

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

DOMAIN ONE

Security Principles and Practices (21%)

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

Knowledge of

1. Principles of planning, organization, and control
2. Security theory, techniques, and processes
3. Security industry standards
4. Continuous assessment and improvement processes
5. Cross-functional organizational collaboration

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

Knowledge of

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

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

Knowledge of

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

TASK 4: Develop and manage external relations programs with public sector law enforcement or other external organizations to achieve security objectives.

Knowledge of

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

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

Knowledge of

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

DOMAIN TWO

Business Principles and Practices (13%)

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

Knowledge of

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

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

Knowledge of

6. Principles and techniques of policy/procedures development
7. Communication strategies, methods, and techniques
8. Training strategies, methods, and techniques

9. Cross-functional collaboration
10. 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 programs, education and training)

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

Knowledge of

1. Interview techniques for staffing
2. Candidate selection and evaluation techniques
3. Job analysis processes
4. Pre-employment background screening
5. Principles of performance evaluations, 360 reviews, and coaching
6. Interpersonal and feedback techniques
7. Training strategies, methodologies, and resources
8. Retention strategies and methodologies
9. Talent management and succession planning

TASK 5: Monitor and ensure a sound ethical climate in accordance with regulatory requirements and the organization's directives and standards to support and promote proper business practices.

Knowledge of

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

TASK 6: Provide advice and assistance to management and others in developing performance

requirements and contractual terms for security vendors/suppliers.

Knowledge of

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

DOMAIN THREE

Investigations (10%)

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

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)
4. Internal and external resources to support investigative functions
5. Report preparation for internal purposes and legal proceedings
6. Laws pertaining to developing and managing investigative programs

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

Knowledge of

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

TASK 3: Manage or conduct surveillance processes.

Knowledge of

1. Surveillance techniques

2. Technology/equipment and personnel to conduct surveillance
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 industrial espionage crimes
3. Arson and property crimes
4. Cybercrimes

TASK 5: Manage or conduct investigative interviews.

Knowledge of

1. Methods and techniques of eliciting information
2. Techniques for detecting deception
3. The nature of non-verbal communication and cultural considerations
4. Rights of interviewees
5. Required components of written statements
6. Laws pertaining to managing investigative interviews

TASK 6: 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

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

DOMAIN FOUR

Personnel Security (12%)

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

Knowledge of

1. Background investigations and personnel screening techniques
2. Quality and types of information sources
3. Screening policies and guidelines
4. Laws and regulations pertaining to personnel screening

TASK 2: 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

1. Protection techniques and methods
2. Threat assessment
3. Prevention, intervention and response tactics
4. Educational and awareness program design and implementation
5. Travel security program
6. Laws, government, and labor regulations
7. Organizational efforts to reduce employee substance abuse

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

Knowledge of

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

DOMAIN FIVE

Physical Security (25%)

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

Knowledge of

1. Security protection equipment and personnel
2. Survey techniques
3. Building plans, drawings, and schematics

4. Risk assessment techniques
5. Gap analysis

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

Knowledge of

1. Fundamentals of security system design
2. Countermeasures
3. Budgetary projection development process
4. Bid package development and evaluation process
5. Vendor qualification and selection process
6. Final acceptance and testing procedures
7. Project management techniques
8. Cost-benefit analysis techniques
9. Labor-technology relationship

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

Knowledge of

1. Protection personnel, technology, and processes
2. Audit and testing techniques
3. Preventive and corrective maintenance for systems

DOMAIN SIX

Information Security (9%)

TASK 1: Conduct surveys of information asset facilities, processes, systems, and services to evaluate current status of information security program.

Knowledge of

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

7. Information security threats
8. Building and system plans, drawings, and schematics

TASK 2: Develop and implement policies and procedures to ensure information is evaluated and protected against all forms of unauthorized/inadvertent access, use, disclosure, modification, destruction, or denial.

Knowledge of

1. Principles of management
2. Information security theory and terminology
3. Information security industry standards (e.g., ISO, PII, PCI)
4. Relevant laws and regulations regarding records management, retention, legal holds, and destruction practices
5. Practices to protect proprietary information and intellectual property
6. Protection measures, equipment, and techniques; including information security processes, systems for physical access, data control, management, and information destruction

TASK 3: Develop and manage a program of integrated security controls and safeguards to ensure information asset protection including confidentiality, integrity, and availability.

Knowledge of

1. Elements of information asset protection including confidentiality, integrity, and availability, authentication, accountability, and audit ability of sensitive information; and associated information technology resources, assets, and investigations
2. Information security theory and systems methodology
3. Multi-factor authentication techniques
4. Threats and vulnerabilities assessment and mitigation
5. Ethical hacking and penetration testing techniques and practices
6. Encryption and data masking techniques
7. Systems integration techniques
8. Cost-benefit analysis methodology
9. Project management techniques
10. Budget development process

11. Vendor evaluation and selection process
12. Final acceptance and testing procedures, information systems, assessment, and security program documentation
13. Protection technology, investigations, and procedures
14. Training and awareness methodologies and procedures

DOMAIN SEVEN

Crisis Management (10%)

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

Knowledge of

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

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

Knowledge of

1. Resource management techniques
2. Emergency planning techniques
3. Triage and damage assessment techniques
4. Communication techniques and notification protocols
5. Training and exercise techniques
6. Emergency operations center (EOC) concepts and design
7. Primary roles and duties in an incident command structure

TASK 3: Respond to and manage an incident.

Knowledge of

1. Resource management techniques
2. EOC management principles and practices
3. Incident management systems and protocols

TASK 4: Recover from incidents by managing the recovery and resumption of operations.

Knowledge of

1. Resource management techniques
2. Short and long-term recovery strategies
3. Recovery assistance resources
4. Mitigation opportunities in the recovery process

"Earning my CPP made me more knowledgeable on the overall topic of security. I thought I knew a lot already. In fact, I did. but there really was so much more to know."

Rudolph J. Friederich, CPP, Principal,
Marshal Security Concepts LLC

Professional Certified Investigator

PCI: BOARD CERTIFICATION IN INVESTIGATIONS

The Professional Certified Investigator (PCI®) credential provides demonstrable proof of knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings.

Earning a PCI provides independent confirmation of specialized skills in security investigations, including case evaluation and review of options for case management strategies. It validates your ability to collect information through the effective use of surveillance, interviews, and interrogations.

PCI ELIGIBILITY REQUIREMENTS

Candidates wishing to take the PCI examination must meet the following eligibility requirements:

WORK EXPERIENCE

Five years of investigations experience, including at least two years in case management*

AND

EDUCATION

A high school diploma or GED 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.

OR

Hold the APP and have four (4) years of investigations experience, including at least two (2) years in case management*

The PCI Certification is applicable to a wide range of specialized investigations, including:

- ◆ Arson
- ◆ Child abuse
- ◆ Forensics
- ◆ Gaming
- ◆ Healthcare fraud
- ◆ High tech crime
- ◆ Insurance fraud
- ◆ Loss prevention
- ◆ Narcotics
- ◆ Property and casualty
- ◆ Threat assessment
- ◆ White collar crime
- ◆ Workplace violence

“When you have ‘board certified’ after your name on a business card and it’s being passed around, whether at a corporate meeting or with clients, it’s recognized. Those three letters mean something. It shows you have the knowledge and experience to handle a full range of investigative assignments”

Patrick Quillinan, PCI, Senior Security Investigator, Takeda Pharmaceuticals U.S.A., Inc.

PCI BODY OF KNOWLEDGE

To be awarded the PCI designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions; 125 “live,” scoreable questions and up to 15 pre-test questions. Knowledge in three major areas (domains) is tested.

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

DOMAIN ONE

Case Management (35%)

TASK 1: Analyze case for applicable ethical conflicts.

Knowledge of

1. Nature/types/categories of ethical issues related to cases (fiduciary, conflict of interest, attorney-client)
2. The role of laws, codes, regulations and organizational governance in conducting investigations

TASK 2: Analyze and assess case elements, strategies and risks.

Knowledge of

1. Case categories (computer, white collar, financial, criminal, workplace violence)
2. Qualitative and quantitative analytical methods and tools
3. Strategic/operational analysis
4. Criminal intelligence analysis
5. Risk identification and impact
6. ASIS Workplace Violence standard

TASK 3: Determine investigative goals and develop strategy by reviewing procedural options.

Knowledge of

1. Case flow
2. Negotiation process
3. Investigative methods
4. Cost-benefit analysis

TASK 4: Determine and manage investigative resources necessary to address case objectives.

Knowledge of

1. Quality assurance process
2. Chain of custody procedures
3. Resource requirements and allocation (e.g., personnel, equipment, time, budget)

TASK 5: Identify, evaluate and implement investigative process improvement opportunities.

Knowledge of

1. Internal review (e.g., management, legal, human resources)
2. External review (e.g., regulatory bodies, accreditation agency)
3. Liaison resources
4. Root cause analysis and process improvement techniques

DOMAIN TWO

Investigative Techniques and Procedures (50%)

TASK 1: Conduct surveillance by physical, behavioral, and electronic means in order to obtain relevant information.

Knowledge of

1. Types of surveillance
2. Surveillance equipment
3. Pre-surveillance routines
4. Procedures for documenting surveillance activities

TASK 2: Conduct interviews of individuals to obtain relevant information.

Knowledge of

1. Interview techniques
2. Indicators of deception (e.g., non-verbal communication)
3. Subject statement documentation

TASK 3: Collect and preserve potential evidentiary materials for assessment and analysis.

Knowledge of

1. Forensic opportunities and resources
2. Requirements of chain of custody
3. Methods/procedures for seizure of various types of evidence
4. Methods/procedures for preserving various types of evidence
5. Concepts and principles of digital forensics
6. Retrieval, storage, and documentation of digital information

7. Concepts and principles of computer operations and digital media

TASK 4: Conduct research by physical and electronic means to obtain relevant information.

Knowledge of

1. Methods of research using physical resources
2. Methods of research using information technology
3. Methods of analysis of research results
4. Research documentation
5. Information sources (e.g., government, proprietary, open)
6. Digital media capabilities

TASK 5: Collaborate with and obtain information from other agencies and organizations possessing relevant information.

Knowledge of

1. External information sources
2. Liaison techniques
3. Techniques for integrating and synthesizing external information

TASK 6: Use special investigative techniques to obtain relevant information.

Knowledge of

1. Concepts and methods of polygraph examinations
2. Concepts, principles, and methods of video/audio recordings
3. Concepts, principles, and methods of forensic analysis (e.g., writing, documents, fingerprints, DNA, biometrics, chemicals, fluids, etc.)
4. Concepts, principles, and methods of undercover investigations
5. Concepts, principles, and methods of threat assessment
6. Use of confidential sources
7. Concepts, principles, and methods of applying IT hardware and software tools

DOMAIN THREE

Case Presentation (15%)

TASK 1: Prepare report to substantiate investigative findings.

Knowledge of

1. Critical elements and format of an investigative
2. report

3. Investigative terminology
4. Logical sequencing of information

TASK 2: Prepare and present testimony.

Knowledge of

1. Types of testimony
2. Preparation for testimony

Physical Security Professional

PSP: BOARD CERTIFICATION IN PHYSICAL SECURITY

The Physical Security Professional (PSP®) credential provides demonstrable proof of knowledge and experience in threat assessment and risk analysis; integrated physical security systems; and the appropriate identification, implementation, and ongoing evaluation of security measures.

Earning a PSP demonstrates your expertise in conducting physical security surveys to identify vulnerabilities and performing cost analysis for the selection of integrated physical security measures. In addition, it confirms your specialized knowledge in systems procurement, final acceptance testing, and implementation procedures.

PSP ELIGIBILITY REQUIREMENTS

Candidates wishing to take the PSP examination must meet the following eligibility requirements:

WORK EXPERIENCE

Four years of progressive experience in the physical security* field

AND

EDUCATION

Bachelor's degree or higher from an accredited institution of higher education

OR

Hold the APP, and three (3) years of progressive experience in the physical security* field

AND

Bachelor's degree or higher from an accredited institution of higher education

OR

WORK EXPERIENCE

Six years of progressive experience in the physical security* field

AND

EDUCATION

A high school diploma, GED equivalent, or associate degree

OR

Hold the APP, and five (5) years of progressive experience in the physical security* field

AND

EDUCATION

A high school diploma, GED equivalent, or associate degree

*Physical security is defined as the various physical measures designed to safeguard personnel, property, and information.

“Beyond all other reasons for earning your certification, the most fundamental is personal growth. Making an effort to learn something and then testing one’s self against an established set of parameters is a reward in itself. The credential demonstrates the level of commitment to a chosen profession.”

Anthony Frassetta, PSP, Senior
Technology Specialist

PSP BODY OF KNOWLEDGE

To be awarded the PSP designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions; 125 “live,” scoreable questions and up to 15 pre-test questions. Knowledge in three major areas (domains) is tested.

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

DOMAIN ONE

Physical Security Assessment (34%)

TASK 1: Develop a physical security assessment plan.

Knowledge of

1. Risk assessment models and considerations
2. Qualitative and quantitative assessment methods
3. Key areas of the facility or assets that may be involved in assessment
4. Types of resources needed for assessment

TASK 2: Identify assets to determine their value, criticality, and loss impact.

Knowledge of

1. Definitions and terminology related to assets, value, loss impact, and criticality
2. The nature and types of assets (tangible and intangible)
3. How to determine value of various types of assets and business operations

TASK 3: Assess the nature of the threats so that the scope of the problem can be determined.

Knowledge of

1. The nature, types, severity, and likelihood of threats and hazards (e.g., natural disasters, cyber, criminal events, terrorism, socio-political, cultural)
2. Operating environment (e.g., geography, socio-economic environment, criminal activity)
3. Potential impact of external organizations (e.g., competitors, supply chain,

organizations in immediate proximity) on facility’s security program

4. Other external factors (e.g., legal, loss of reputation, economic) and their impact on the facility’s security program

TASK 4: Conduct an assessment to identify and quantify vulnerabilities of the organization.

Knowledge of

1. Relevant data and methods for collection (e.g., security survey, interviews, past incident reports, crime statistics, employee issues, issues experienced by other similar organizations)
2. Qualitative and quantitative methods for assessing vulnerabilities to probable threats and hazards
3. Existing equipment, physical security systems, personnel, and procedures
4. Effectiveness of security technologies and equipment currently in place
5. Interpretation of building plans, drawings, and schematics
6. Applicable standards/regulations/codes and where to find them
7. Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security

TASK 5: Perform a risk analysis so that appropriate countermeasures can be developed.

Knowledge of

1. Risk analyses strategies and methods
2. Risk management principles
3. Methods for analysis and interpretation of collected data
4. Threat and vulnerability identification
5. Loss event profile analyses
6. Appropriate countermeasures related to specific threats
7. Cost benefit analysis (e.g., return on investment (ROI) analysis, total cost of ownership)
8. Legal issues related to various countermeasures/security applications (e.g.,

video surveillance, privacy issues, personally identifiable information)

DOMAIN TWO

Application, Design, and Integration of Physical Security Systems (34%)

TASK 1: Establish security program performance requirements.

Knowledge of

1. Design constraints (e.g., regulations, budget, cost, materials, equipment, and system compatibility)
2. Applicability of risk analysis results
3. Relevant security terminology and concepts
4. Applicable codes, standards and guidelines
5. Functional requirements (e.g., system capabilities, features, fault tolerance)
6. Performance requirements (e.g., technical capability, systems design capabilities)
7. Operational requirements (e.g., policies, procedures, staffing)
8. Success metrics

TASK 2: Determine appropriate physical security measures.

Knowledge of

1. Structural security measures (e.g., barriers, lighting, locks, blast migration, ballistic protection)
2. Crime prevention through environmental design (CPTED) concepts
3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)
4. Security staffing (e.g., officers, technicians, management)
5. Personnel, package, and vehicle screening
6. Emergency notification systems
7. Principles of data storage and management

8. Principles of network infrastructure and network security
9. Security audio communications (e.g., radio, telephone, intercom, IP audio)
10. Systems monitoring and display (control centers/consoles)
11. Systems redundancy alternative power sources (e.g., battery, UPS, generators, surge protection)
12. Signal and data transmission methods
13. Considerations regarding Personally Identifiable Information (physical/logical/biometric)
14. Visitor management systems and circulation control

TASK 3: Design physical system and prepare construction and procurement documentation.

Knowledge of

1. Design phases (pre-design, schematic design, design development, construction documentation)
2. Design elements (calculations, drawings, specifications, review of manufacturer's submittals and technical data)
3. Construction specification standards (e.g., Construction specifications Institute, owner's equipment standards, American Institute of Architects MasterSpec)
4. Systems integration (technical approach, connecting with non-security systems)
5. Project management concepts
6. Scheduling (e.g., Gantt charts, PERT charts, milestones, and objectives)
7. Cost estimation and cost-benefit analysis of design options
8. Value engineering

DOMAIN THREE

Implementation of Physical Security Measures (32%)

TASK 1: Outline criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation.

Knowledge of

1. Bid package components
2. Criteria for evaluation of bids
3. Technical compliance criteria
4. Ethics in contracting

TASK 2: Procure system and implement recommended solutions to solve problems identified.

Knowledge of

1. Project management functions and processes throughout the system life cycle
2. Vendor pre-qualification (interviews and due diligence)
3. Procurement process

TASK 3: Conduct final acceptance testing and implement/provide procedures for ongoing monitoring and evaluation of the measures.

Knowledge of

1. Installation/maintenance inspection techniques
2. Systems integration
3. Commissioning
4. Installation problem resolution (punchlists)
5. Systems configuration management
6. Final acceptance testing criteria
7. End-user training requirements

TASK 4: Implement procedures for ongoing monitoring and evaluation throughout the system life cycle.

Knowledge of

1. Maintenance inspection techniques
2. Test and acceptance criteria

3. Warranty types
4. Ongoing maintenance, inspections and upgrade
5. Ongoing training requirements
6. Systems disposal and replacement processes

TASK 5: Develop requirements for personnel involved in support of the security program.

Knowledge of

1. Roles, responsibilities and limitations of security personnel (including proprietary (in-house) and contract security staff)
2. Human resource management
3. Security personnel training, development and certification
4. General, post and special orders
5. Security personnel uniforms and equipment
6. Personnel performance review and improvement processes
7. Methods to provide security awareness training and education for non-security personnel

PROGRAM CHANGES AND UPDATES

Every five years, following best practices for certification programs, ASIS conducts a job analysis study to ensure that the body of knowledge still aligns with the work being performed by certified professionals. In May 2016, the results of the CPP® job analysis study were incorporated into the exam. In November 2017 the results of both a PSP® and PCI® job analysis study first appeared on exams.

Because no major changes were made to the PCI or PSP, those studying to take these exams may use existing study materials.

APPLYING FOR THE EXAMS

The certification application must be filled out [online](#).

Once your application has been reviewed and approved, you will receive an Authorization to Test email with instructions on how to schedule your exam. Please allow approximately two to three weeks for your application to be reviewed.

Make sure the name you submit on your application EXACTLY matches the name of your government-issued photo ID. If they do not match, you will not be permitted to take the exam.

Application Documents You'll Need:

- ◆ Unofficial transcription from an accredited institution of higher education (if applicable)
- ◆ Resumé or CV detailing your work experience as it relates to the security industry and aligns with the domains of the certification exam you for which are applying
- ◆ Names and contact information for three references who can verify your work experience
- ◆ Name of supervisor who can verify your employment

Deadline Reminders

ASIS will send periodic reminders about deadlines (e.g., scheduling an exam, requests for additional information); **however, meeting and adhering to deadlines are ultimately the responsibility of the applicant.** ASIS cannot guarantee that you have received and/or read any correspondence.

Please make sure your contact information – especially your email address – is current in your online account. Also make sure to whitelist emails from asisonline.org.

APPLICATION FEES

ASIS exams are offered at Prometric test centers throughout the world. For certain regions where Prometric doesn't have a test center, ASIS offers an internet-based exam. Information about internet-based exams can be found on page 30 of the handbook.

The cost for submitting a **CPP, PCI, or PSP** certification application are:

\$300 ASIS members

\$450 nonmembers

The cost for submitting an **APP** certification application are:

\$200 ASIS members

\$350 nonmembers

Refunds

If your application is denied for any reason, you will receive a refund of your fee minus a \$100 nonrefundable processing fee.

If your application is approved and you fail to schedule and take the exam within the two-year eligibility (candidacy) period, you will not receive a refund.

Note: These fees are non-refundable for internet-based exams once the exam site has been scheduled.

Retesting

Candidates may only take the exam up to three times in their two-year eligibility period. In addition, there must be 90 days between each testing date. Those who fail the exam three times may reapply to take exam after their eligibility period ends.

RETEST FEES:

ASIS members: \$200

Nonmembers: \$200

(APP retest takers: \$150)

Approval Notification from ASIS

If you are approved to take an ASIS certification exam, an Authorization to Test letter will be emailed to you. This letter will include:

- ◆ Your eligibility ID, which you'll need to schedule your exam date
- ◆ Instructions for scheduling your exam
- ◆ Studying suggestions

You have two years and up to three attempts from the date of the Authorization to Test to take and pass your exam before you must reapply.

Remember the name on your IDs must exactly match the name on your Authorization to Test Letter.

Appealing a Declined Application

Appeals will be considered within 30 days of an applicant receiving notification of an adverse decision, with day one as the date of the applicant's notification email. Please follow these instructions when filing an appeal:

- ◆ A letter must be submitted explaining action being requested to certification@asisonline.org
- ◆ Appeals must be sent by mail or email. If sent by mail, ASIS strongly suggests sending by certified or express mail so the package can be traced
- ◆ Appeal must be submitted to the PCB Certificant Relations Committee
- ◆ Appeals must identify the adverse decision being appealed and state the reasons for the appeal. Also, any new or additional information for consideration should be included in the letter

Appeals should be sent to:

PCB Certificant Relations Committee
c/o ASIS International
1625 Prince Street
Alexandria, VA 22314
Attn: Certification Department
certification@asisonline.org

PCB Certificant Relations Appeal Process

The PCB Certificant Relations Committee will review and consider a properly filed appeal via teleconference or during its annual meetings.

When necessary, the PCB Certificant Relations Committee has the authority to seek legal advice regarding any aspect of the applicant's appeal.

The ASIS certification staff, on behalf of the PCB Certificant Relations Committee, will notify the applicant of the PCB Certificant Relations Committee's decision, and the reasons therefore, as specified in the appeals time frame. (An initial response should be provided within 30 days, acknowledging receipt of complaint. There should be a 60-day investigative review process, renewable for another 60-day period based on findings.)

The PCB Certificant Relations Committee's decision is final.

SCHEDULING YOUR EXAM

ASIS exams are offered at Prometric computer-based test (CBT) centers throughout the world. Go to prometric.com/asis to locate the nearest testing facility. Our CBT exams are offered year-round. Please remember that you cannot schedule your exam until you have been approved to take the exam and have received the Authorization to Test letter.

Making Your Exam Appointment

After receiving your authorization letter, candidates should contact Prometric, the test contractor retained by ASIS, to locate the nearest testing location and schedule the exam.

Online scheduling

The exam can be scheduled online prometric.com/asis

You will be asked for:

- ◆ Your Eligibility ID, which can be found on your Authorization to Test letter (your ASIS Contact Number or Member ID)
- ◆ The first four letters of your last (sur) name

Scheduling by Phone

Prometric: +1.800.699.4975, Monday – Friday, 8:00 am - 8:00 pm (EST) and Saturday 8:00 am - 4:00 pm (EST)

Prometric will help you select the optimal test date, location, and answer questions about the testing process. Candidates will be given a confirmation number to bring to the testing center at the time of the exam.

Confirmation Email from Prometric

Once your exam appointment is confirmed, Prometric will send you an email with your exam time and confirmation number. **Make sure to print out this letter and bring with you to the test center along with two government-issued photo identifications** (e.g., driver's license, passport). Social Security cards are not accepted. Your ID must include your signature.

Scheduling an Internet-based Exam

Candidates in these areas must take an internet-based exam.

- ◆ Australia (Queensland)
- ◆ Ecuador
- ◆ Jamaica
- ◆ Paraguay
- ◆ Panama

Internet-based exams are offered biannually on the first Saturday of May and November. Applications for internet-based exams are due March 1 and August 1.

Sponsoring an Internet-Based exam

Internet-based exams are administered in locations that don't have an official Prometric Test Center. Internet-based exams must be sponsored by an ASIS Chapter. There must be at least 10 approved candidates to hold an internet-based exam. No exceptions. Sponsors must alert their members that once an exam is scheduled, all fees are non-refundable.

To apply for a sponsorship:

- ◆ Complete the [Request to Sponsor Form](#) for CPP, PCI, PSP, and/or APP examinations
- ◆ Email completed form to the Certification team at certification@asisonline.org

Choosing Your Exam (English or Spanish)

The CPP, PCI, and PSP exams are administered in English and Spanish. For the Spanish-language exams, you are also given an English translation. During the online application process, you will choose the language for your exam (English or Spanish).

Testing Accommodations for Candidates with Disabilities and Other Special Considerations

All ASIS programs comply with the Americans with Disabilities Act and are non-discriminatory. If specific testing arrangements are needed due a disability condition, candidates may request special accommodations by checking the "Disabled/Special Access Required" on the online application and explaining the accommodation needed in the text box provided when completing their application. **Special testing accommodations must be approved by ASIS prior to scheduling your exam. You will be required to provide documentation before ASIS can approve your request.** Requests are reviewed and approved on a case-by-case basis.

PROMETRIC CUSTOMER SERVICE

For general questions about Prometric services, including how to receive a copy of your score report (if you didn't receive one at the test center) call +1.800.853.6769.

Extension Policies – Exam Applications

ASIS does not grant extensions due to job demands, company budgets, employment status, personal finances, changes in marital status, changes in mailing

address, and other personal or professional reasons. Extensions may be granted if there is a severe hardship such as a major medical emergency in the immediate family, a natural disaster, or if on active military duty and deployed into a remote or hazardous area. The applicant is required to provide documentation of extenuating circumstances (e.g., doctor's note). Military personnel will need to verify their deployment status by submitting a copy of official deployment orders. This does not apply to individuals who are military contractors. Severe hardship must be documented and verifiable.

Cancellation Policy

Due to frequent cancellations and short notification rescheduling, Prometric has indicated that there may be inadequate capacity at centers where the ASIS International examinations are administered. Managing the process of scheduling and rescheduling appointments is critical to ensure that all candidates can obtain a testing appointment on the date and time requested.

To provide a first-choice experience for all candidates, Prometric will charge a reschedule/cancellation fee. This fee will be assessed either at Prometric.com/ASIS if the candidate reschedules or cancels online, or via phone +1.800.699.4975 through Prometric's customer service.

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 4-30 days before the scheduled test day, there is a fee of \$62.50 per reschedule. Candidates cannot reschedule three or less days before their scheduled testing date. All rescheduling or cancellation fees are to be made directly through Prometric.

If a candidate is a "no show" and does not adhere to the above procedures, the full candidate testing fee is forfeited. You may schedule a new exam and pay the \$200 retest fee.

Note that you may only take the exam up to three times during your two-year candidacy. Once your two-year candidacy has expired, you must reapply to take the exam and pay the applicable fees.

Prometric makes NO exceptions to this rule.

"No Shows"

If you fail to cancel or reschedule your exam, you will be considered a "no show" and all testing fees will be forfeited. ASIS understands that emergencies do

happen. If you do not appear for your exam for any of the following reasons, you will have 14 days from your scheduled appointment day to provide the documentation below and reschedule your exam:

1. **Death in the immediate family**

- ◆ Death certificate or doctor's note, which must be signed by a licensed physician or mortician and include contact information

2. **Serious injury or disabling injury (to yourself or immediate family member)**

Doctor's note, with date of medical visit. The documentation:

- ◆ Should explain that the onset of the illness or injury was 24 hours before the exam
- ◆ Must be signed by a licensed physician and include contact information
- ◆ Does not need to include details of the illness or emergency, but the doctor should indicate that the condition prevented the candidate from testing

3. **Court appearance or jury duty**

- ◆ Court or jury summons, subpoena, which must include date and your name

4. **Military duty**

- ◆ Duty letter, which must include date and your name

ASIS reserves the right to request additional evidence to support your reason for failing to appear. If ASIS and Prometric accept the explanation, you will be permitted to schedule a new appointment within your eligibility period without paying the rescheduling fee.

ON EXAM DAY

Plan to arrive at the testing center 30 minutes before the scheduled appointment to allow time for check-in procedures. If you will be driving, identify in advance the exact location, the best route, and where to park.

If you arrive more than 15 minutes late, Prometric Testing Center staff may choose not to seat you if doing so would disrupt other exam takers. If this occurs, your exam registration fees **will not be refunded. There are no exceptions to this rule.**

Check-in Procedures

You must have the following items, or you will not be admitted to the exam:

Two forms of identification, one of which must be a government-issued photo ID (such as a passport or

driver's license); **both must have the candidate's signature.** (A Social Security card is not an acceptable form of identification.)

- Only your first and last/surname on your approval letter from ASIS and identifications must match EXACTLY or you may NOT be permitted to test. This includes abbreviated or hyphenated names.

Prometric Confirmation Email and Number (from the email you get when you schedule your exam).

If you are testing outside your country of citizenship, you must present a valid passport. If you are testing in your country of citizenship, you may present a passport, driver's license, national ID, or military ID. Expired IDs will not be accepted.

If you fail to bring the proper identification, you will not be allowed to take the exam and will forfeit the exam fee.

Security Measures

Prometric testing staff are not allowed to pat down a candidate during the check-in process and they will use a security wand (similar to those used at airports), to check candidates for any type of cheating devices. This is in addition to having the candidates turn their pockets inside out.

- ◆ The performance of all candidates is monitored and may be analyzed to detect fraud. Candidates who violate security measures will not have their exams scores validated by ASIS.
- ◆ If you offer or receive help during the exam, you will be escorted from the testing center and reported to the PCB. Your exam will not be scored, exam fees will not be refunded, and you will be prohibited from taking the exam again.
- ◆ All exam materials, including all questions and all forms of the exam, are copyrighted and the property of ASIS. Any distribution of these materials through reproduction or oral or written communication is strictly prohibited and punishable by law.

Sound Distractions Alternatives

Candidates can bring their own small earplugs to the center with them. You must present the ear plugs to the test center proctors for examination before entering the testing room. Note that candidates may not bring their own large headphone-style noise reducers without a special accommodation.

Candidates may opt to use the noise-reducing headphones available at Prometric sites. These are

large “airport” style headphones and may be uncomfortable when worn for a long period. There are no small earplug-type noise reducers available at Prometric centers.

Eating, drinking, and smoking are not permitted during the exam. If you bring a jacket or sweater, you will be required to wear it at all times in the testing room. Visitors are not allowed in the test center, and child care is not provided.

What to Bring and Not Bring

For test security reasons, all personal items such as purses, book bags, cell phones, etc., must be placed in a locker during the exam, so please limit what you bring to the testing center.

Jewelry outside of wedding and engagement rings is prohibited and all hair accessories are subject to inspection. Please refrain from using ornate clips, combs, barrettes, headbands, and other hair accessories as you may be prohibited from wearing them into the testing room and asked to store them in your locker. Violation of security protocol may result in confiscation of prohibited devices and filing a report with local authorities.

During the Exam

Once you have completed the check-in process, you will be assigned to a testing station. You will be provided with an onscreen calculator, two erasable note boards, and dry erase markers.

- ◆ No scratch paper, dictionaries, books, notes, or other personal aids are permitted in the testing area.
- ◆ To use the restroom, candidates must notify the test center administrator (TCA); however, if you take a break, the time clock on the exam is not stopped.
- ◆ No breaks are scheduled.
- ◆ No conversation about the test is permitted with the TCA or other test takers.

A 15-minute onscreen tutorial will orient you to the features of the computer testing environment. When you have completed the tutorial, you will start the exam.

Test Taking Tips

- ◆ Relax! Reducing physical stress will help you be more alert.
- ◆ Find the right work pace. Don’t rush or go too slowly. Find a pace that is comfortable.
- ◆ Follow the directions and work carefully.

- ◆ Read all the options for each question before marking the answer.
- ◆ Skip difficult questions. You can mark questions to come back to later. If you’re still not sure, make an informed guess.
- ◆ Both unanswered questions and wrong answers are counted as wrong responses. Your score is based on the total number of correct responses.
- ◆ Keep an eye on the exam timer (on your screen). If you do not submit your exam before your time is over, the exam will automatically shut off when the time runs out.

Exam Results

Once you submit your exam, you will be directed to answer a short survey before you receive your score. These *preliminary* results will be emailed to the email address you provided to Prometric (allow up to five hours to receive this email). Your official score will be sent to you approximately three weeks after you take the exam.

You can also call Prometric’s customer services at +1.800.853.6769 to have your score report email resent.

End-of-Exam Survey

After you submit your exam and **before you receive your preliminary results**, you will be asked to complete a short survey. This is your opportunity to tell both ASIS and Prometric about your testing experience. Your comments will have no bearing on your exam score. ASIS uses the results of this survey to enhance our certification procedures.

Weather Emergencies

If severe weather, natural disaster, or other such incidents make a testing center inaccessible or unsafe, the exam may be rescheduled or cancelled (at no cost to the candidate). To check on your testing center, please check the Prometric site closure website at <https://www.prometric.com/en-us/pages/siteclosure.aspx>

HOW ARE THE EXAMS STRUCTURED?

All ASIS certification exams are multiple choice. You will be provided four possible answers, only one of which will be correct. Following are the number of exam items (questions) per exam and the maximum time you are permitted to complete and submit the exam:

- ◆ CPP – 200 “live” (scoreable) and 25 pre-test (unscored) items. 4 hours.
- ◆ PSP – 125 “live” (scoreable) and 15 pre-test (unscored) items. 2.5 hours.
- ◆ PCI – 125 “live” (scoreable) and 15 pre-test (unscored) items. 2.5 hours.
- ◆ APP – 100 “live” (scoreable) and 25 pre-test 2 hours

There will be a timer on your computer screen showing how much time you have left. Please make sure that you have answered all the items. Any unanswered items will be marked incorrect.

Scoring the Exam

All ASIS exams use the “**scaled score**” method to determine the passing point of each exam question. Before a question is presented on the exam, it is pre-tested. This allows Prometric’s psychometricians to weigh the performance of each question and its level of difficulty.

Individual questions are given a weighted/scaled score based on level of difficulty. A scaled score is a transformed raw exam score (the number of exam questions answered correctly). To interpret any exam score, a uniform frame of reference is required. Scaled scores provide that frame of reference based on the standard adopted by ASIS regarding the level of knowledge necessary to pass the exams without regard to the specific exam version taken.

This explains why each exam may have a different number of questions per domain area. **A scaled score of at least 650 is required to pass the exam.** A scaled score is neither the number of questions you answered correctly nor the percentage of questions you answered correctly.

The passing score was established via a systematic procedure (standard setting study) that employed the judgment of a representative group of ASIS-certified professionals with the assistance of exam development experts from Prometric. This group of subject matter experts recommended a standard to ASIS for what a minimally competent security professional needs to know about the tested content to obtain a passing score. Each **ITEM** on the computer-based test is electronically scored based on how the item performed during pre-test. Because of this method, it is virtually impossible for your exam score to be incorrect; therefore, **exams taken by computer-based testing are not eligible for a hand score.**

STUDYING FOR THE EXAM

ASIS certification exams are experience-based. Therefore, the more hands-on experience you have related to the body of knowledge, the more successful you’ll be on the exam. Everybody has a different studying preference: some like to study by themselves and others prefer a group study approach. ASIS does not require any one method of studying but we do offer the following recommendations:

Start with the body of knowledge. Read each domain carefully and make an honest assessment of your own experience. This will help you decide where you need to concentrate your studying efforts.

- ◆ [ASIS Self-Assessment for CPP, PCI, or PSP Exams](#)
- ◆ ASIS also offers [Reference Sets](#) for each certification. Our item writers and reviewers use these same materials to reference the correct answers on our exams.*
- ◆ ASIS offers many study opportunities for each exam. Visit our [Education](#) section of the asisonline.org website for more information.*
- ◆ Many [ASIS Chapters](#) offer study groups.

*ASIS does not guarantee success on the exams because you study using ASIS preparatory materials.

Exam Preparation Resources

ASIS offers a number of resources to help you study for your board certification. Candidates are encouraged to refer to the following reference material as they are preparing for the CPP, PCI, PSP, or APP examination. After carefully reviewing the domains of study and identifying individual learning needs, candidates may use additional references and study opportunities as necessary.

CERTIFIED PROTECTION PROFESSIONAL

The *Protection of Assets* (POA) and set of ASIS standards and guidelines comprise the CPP reference material. Each is available for individual purchase or as the set depicted below. Also available on Kindle.

•Protection of Assets

POA Print

POA Online

POA Combination Print and Online

•Standards and Guidelines

Standards and Guidelines Print
Standards and Guidelines Download

PROFESSIONAL CERTIFIED INVESTIGATOR

Two publications now comprise the PCI reference materials. [The Professional Investigator's Manual](#) is available in hardcover, softcover or E-book version. The Investigations Standard also is a recommended reference. ASIS members may download one free copy of the standard; nonmembers may purchase a [download](#).

PHYSICAL SECURITY PROFESSIONAL

The publications listed below comprise the PSP reference material. Available as a hardcover or softcover set. Each title is available for individual purchase.

- Physical Security Principles ([hardcover](#), [softcover](#))
- Implementing Physical Protection Systems: A Practical Guide, 2nd Ed ([softcover](#))
- ASIS Business Continuity Guideline: A Practical Approach ([PDF](#) or [print](#))*
- ASIS Facilities Physical Security Measures Guideline ([PDF](#) or [print](#))*

*The two guidelines **Business Continuity Guideline and Facilities Physical Security Measures Guideline are not included in this package** (item #2300) and must be purchased separately. ASIS members are entitled to one free download (PDF) of each guideline.

ASSOCIATE PROTECTION PROFESSIONAL

The publications listed below comprise the recommended APP reference materials, which include five Standards and three volumes from the ASIS Protection of Assets. ASIS offers the following individually or in bundles.

Five Standards

1. Security Management Standard: Physical Asset Protection
2. Security and Resilience in Organizations and their Supply Chains - Requirements with Guidance
3. Investigations
4. Workplace Violence Prevention and Intervention Standard
5. Risk Assessment

Protection of Assets Volumes

1. Protection of Assets: Security Management

2. Protection of Assets: Crisis Management
3. Protect of Assets: Information Security

ASIS offers three pricing bundles for the APP:

1. APP Standards Bundle
2. Security and Crisis Management and Information Bundle for the APP Certification
3. APP Complete Reference Set

Please search for these items in the [ASIS Store](#).

CERTIFICATION REVIEWS

ASIS offers both in-person and online review courses to help you prepare for your exam. Many ASIS Chapters also offer study groups. Contact the ASIS Chapter in your area for more information.

Neither the Professional Certification Board nor ASIS Certification staff have any involvement in the ASIS review courses. Review course instructors have no access to actual exam questions.

Free Study Tools

The Practice Exams contain items that once appeared on the actual certification exams but are now retired. Use these practice exams to familiarize yourself with how exam items will appear on the current exam(s). Note: Because these questions no longer appear on the exam, they may no longer be accurate. These are intended only to know how exam questions will be formulated.

[CPP Practice Exam](#)

[PCI Practice Exam](#)

[PSP Practice Exam](#)

I PASSED THE EXAM, NOW WHAT?

Upon successful completion of the examination, you will receive a certificate bearing your name, certification cycle begin and end date, and certification number.

Also, you will receive an email from ProExam Vault (ASIS' digital credentialing partner) with the subject line "ASIS has issued you a digital badge." The message will provide an invitation and instructions to claim your digital badge(s). Please allow two to four weeks to receive your certificate and digital credential.

Wear your new designation proudly! Add it to your email signatures, business cards, and social media accounts!

Recertification

All those who hold an ASIS certification must **recertify every three years** by earning Continuing Professional Education credits. Recertification tells your colleagues, peers, and employer that you committed to staying current in the security profession. For more information on recertification requirements, please download the [Recertification Guide](#).

ASIS APPLICATION AND CERTIFICANT POLICIES

Statement of Impartiality

The ASIS Professional Certification Board (PCB) and certification staff understand the importance of impartiality and conflicts in the management of certification activities. When undertaking dealings with members and nonmembers, all involved in the certification process will maintain a high level of ethical conduct and avoid conflicts of interest in connection with the performance of their duties.

There shall be an avoidance of any actions and/or commitments that might create the appearance of:

- ◆ Using positions for personal gain
- ◆ Giving improper preferential treatment
- ◆ Impeding efficiency
- ◆ Losing independence or impartiality
- ◆ Adversely affecting the confidence of ASIS constituents in the integrity of certification operations.

The PCB and certification staff will ensure that in its dealings with constituents, they are and will remain impartial and confidential.

ASIS Certification Code of Professional Responsibility

ASIS board certified security professionals and applicants for certification must adhere to the Code of Professional Responsibility, agreeing to:

- ◆ Perform professional duties in accordance with the law and the highest moral principles. Noncompliance includes any acts or omissions amounting to unprofessional conduct and deemed prejudicial to the certification.
- ◆ Observe the precepts of truthfulness, honesty, and integrity.
- ◆ Be faithful, competent, and diligent in discharging their professional duties.

- ◆ Safeguard confidential and privileged information and exercise due care to prevent its improper disclosure.
- ◆ Not maliciously injure the professional reputation or practice of colleagues, clients, or employees.

Any act deemed prejudicial to the certification may result in denial of approval to take the certification examination or disciplinary action by the Professional Certification Board (PCB), up to and including revocation of certification. Such acts may include, but are not limited to:

- ◆ Providing false or misleading statements or information when applying to take the certification examination or to recertify.
- ◆ Any act or omission that violates the provisions of the ASIS Certification Code of Professional Responsibility.
- ◆ Any act that violates the criminal or civil laws of any jurisdiction.
- ◆ Any act that is the proper basis for suspension or revocation of a professional license.
- ◆ Any act or omission that violates the PCB Disciplinary Rules and Procedures.
- ◆ Failure to cooperate with the PCB's Board of Professional Review in performance of its duties in investigating any allegation against an applicant or current certificant.
- ◆ Making any false or misleading statements to the PCB regarding an applicant or current certificant.

Attestation of Continued Eligibility for Certification

All those applying for an ASIS exam will sign the following attestation on the application.

By my signature, I attest that the information I submit herein or in any required accompanying or subsequent documentation is true and accurate to the best of my knowledge.

I understand that persons who apply for certification as a Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), or Associate Protection Professional (APP), or persons who have been certified by ASIS International, are subject to ASIS International's eligibility requirements for certification, recertification, and to the ASIS Certification Code of Professional Responsibility.

I understand that in order to maintain my certification, I must recertify every three years by reporting a specified

number of Continuing Professional Education (CPE) credits, in accordance with ASIS policy and procedures for submitting such reports. I understand that CPE credits may be earned through education programs and courses and other activities, and that all CPEs must conform to the requirements specified in ASIS International's Recertification Guide. I further understand that from time to time ASIS International may amend its requirements, policies, and procedures to include initial certification, recertification, and the Code of Professional Responsibility.

I also understand that I may be subject to audit at any time and that ASIS International reserves the right to take action for failure to comply with the audit procedures.

While holding ASIS International certification, I agree to notify ASIS International in writing immediately if I fail to comply with any of the requirements for gaining or maintaining certification or recertification, such as, but not limited to, no longer working the profession, no longer holding Lifetime Retired status due to returning to full-time employment, failing to earn the number of CPE credits needed to maintain certification or to be recertified, or having been disciplined – including suspension, expulsion, or loss of the credential – as a result of having been found in violation of the Code of Professional Responsibility. I also agree to notify ASIS International in writing of any address or name change(s) within thirty (30) days after the change becomes effective.

If requested to do so, ASIS International may verify my certification status.

REVOCATION OF CERTIFICATION

Certifications are subject to revocation for any of the following causes:

- ◆ The certified individual shall not have been eligible to receive such certification, irrespective of whether or not the facts were known to, or could have been ascertained by, the PCB at the time of issuance of such certification; or
- ◆ The certified individual shall have made any misstatement of fact in the application for such certification or any other statement or representation, connected with the application for certification; or
- ◆ The certified individual has been found to have engaged in unethical practices or has been convicted of a felony.

No certification shall be revoked unless the following procedures are followed:

- ◆ A copy of the charges against the certified individual and the information concerning the event or events from which such charges have arisen is sent by registered mail to the individual. Such notice shall state that no action will be taken against the certified individual until after a hearing unless the individual fails to request a hearing or offer a defense within 15 days.
- ◆ The certified individual is given at least 15 days to prepare a defense.
- ◆ A hearing is held on such charges, before a designated panel, at which time the person is given a full opportunity to be heard in his or her own defense, including the right to be presented by counsel, the right to cross-examine witnesses appearing, and to examine documents material to said charges. Accommodation support will be provided to eligible individuals.
- ◆ The panel shall initially determine whether or not the individual's certification should be revoked. The initial determination of the panel, including all evidence submitted at the hearing, shall be reviewed. Upon review, the PCB may affirm, reverse, modify, or remand the original determination of the panel.
- ◆ If the initial determination of the panel is to revoke the certification of the individual, and if a majority of the PCB, in official session, affirm the panel's determination that the individual is not eligible for continued certification, then a notice will be issued. If your certification is revoked, you will be asked to return your certificate and cease using the designation.

LIFETIME DESIGNATION

CPPs, PCIs, or PSPs may be considered for Lifetime Designation, if the individual meets the following criteria:

- ◆ Be a CPP, PCI, or PSP in good standing
- ◆ Have maintained a single certification for twelve consecutive years preceding the date of application
- ◆ Be currently retired ("retired" is defined as complete cessation from any security-related employment or practice or representation of any such employment or practice) and have no legal, financial, or business interest with any form of security-related employment or practice, as defined by the applicable certification exam domain

- ◆ Have paid the recertification fee for the current term

If a lifetime certificant returns to professional practice after the end of the last term of their regular certification, they must submit a recertification application demonstrating the successful completion of sixty (60) CPEs within the previous three-year period, or they must retake and pass the appropriate certification exam. Lifetime certificants are automatically eligible to sit for the exam of their prior certification, without the need to submit additional supporting materials but are required to pay the application fees.

If you are granted a Lifetime Certification, you will receive a new certificate with your new designation. To display this new designation, you will use the following: CPP – Life Certified (Retired), PSP – Life Certified (Retired), or PCI – Life Certified (Retired). You cannot use the designation without these qualifying descriptions.

[Applications](#) for lifetime designations may be obtained on the ASIS website.

RELEASE OF CANDIDATE AND CERTIFICANT INFORMATION

Release to third parties of confidential information of ASIS candidates and certificants is prohibited unless ASIS obtains signed permission from the candidate or certificant to do so. Consent to release information must include to whom the candidate or certificant information can be released and the information that can be released.

ASIS CERTIFICATES

All certificates related to the CPP, PCI, PSP, and APP designations are the sole property of ASIS International. Suspended and revoked certificates must be returned to ASIS International Certification Directors within 15 days of notice of suspension and/or revocation. The formerly certified individual should immediately cease from using the ASIS International designations and removed them from all printed, electronic or other forms of communications.

FILING A COMPLAINT

Complaints regarding the eligibility requirements, test scheduling, policies and procedures of the ASIS certification program, certification personnel, or another certificant may be filed in writing to the Certification Director within 90 days of the incident's occurrence. Please submit your complaint in writing and mail or email to certification@asisonline.org.

Please provide sufficient objective evidence to substantiate the complaint. All complaints will be reviewed by the

Certification Director and/or members of the PCB Certificant Relations Committee. Receipt of your complaint will be sent to you and will include actions taken by ASIS to remedy the situation. When the complaint has been resolved, the person filing the complaint will be notified with the results of the review.

ABOUT OUR TESTING PARTNER

Prometric is an independent testing company currently under contract with ASIS to administer the ASIS certification exams. Experts at Prometric work closely with ASIS and the Professional Certification Board (PCB) to develop exams that accurately evaluate a candidate's knowledge of the security profession. Prometric scores the exam, sends the results to ASIS, and stores exam records. ASIS staff and the PCB oversee Prometric's activities to ensure that all aspects of the exam process meet certification standards.