

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](mailto:certification@asisonline.org)

PHONE: +1 703.519.6200

WEBSITE: [asisonline.org](http://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 US-based 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
Is ASIS membership required?.....	7
Which Certification is Right for You? .....	7
Eligibility Requirements for all Applicants .....	8
Eligibility Requirement Changes in 2023 .....	8
APP Board Certification in Security Fundamentals .....	9
APP Eligibility Requirements.....	9
APP Impact on Eligibility Requirements for Other ASIS Certifications.....	9
APP Body of Knowledge.....	10
CPP Board Certification in Security Management.....	15
CPP Eligibility Requirements.....	15
CPP Body of Knowledge .....	15
PCI Board Certification in Investigations.....	21
PCI Eligibility Requirements.....	21
PCI Body of Knowledge .....	21
PSP Board Certification in Physical Security .....	24
PSP Eligibility Requirements.....	24
PSP Body of Knowledge.....	24
Taking Remote Proctored Exams .....	28
Applying for the Exams .....	28
Application Documents You'll Need .....	28
Deadline Reminders.....	28
Application Fees .....	28
Fees for the CPP, PCI, and PSP:.....	28
Fees for the APP:.....	28
Refunds.....	29
Retesting.....	29
Retest fees for the CPP, PCI, and PSP:.....	29
Retest fees for the APP: .....	29
Approval Notification from ASIS.....	29

Appealing a Decision .....	29
Scheduling Your Exam .....	30
Making Your Exam Appointment.....	30
Testing Accommodations for Candidates with Disabilities and Other Special Considerations.....	31
Extension Policies.....	31
Cancellation Policy .....	31
“No Shows” .....	31
On Exam Day .....	32
Check-in at a Prometric Testing Center.....	32
What to Bring and Not Bring to Testing Center.....	32
Check-in for Remote Proctored Exams .....	32
Check-in ID Requirements.....	33
During the Exam.....	33
Exam Results.....	34
Weather Emergencies.....	34
How Are the Exams Structured? .....	34
Scoring the Exam .....	34
Studying for the Exam .....	35
Exam Preparation Resources.....	35
Free Study Tools.....	36
I Passed the Exam, Now What? .....	36
Recertification.....	36
ASIS Application and Certificant Policies .....	36
Statement of Impartiality.....	36
ASIS Certification Code of Professional Responsibility .....	37
Attestation of Continued Eligibility for Certification.....	37
Revocation of Certification .....	38
Lifetime Designation .....	38
Release of Candidate and Certificant Information.....	39
ASIS Certificates .....	39
Third-Party Intervention .....	39
Filing a Complaint .....	39
About Our Testing Partner .....	40

## 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 20 February 2024 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 remain 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 ANSI National Accreditation Board (ANAB) against the International Organization for Standardization (ISO) 17024.



## 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.

## 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, exam content (body of knowledge), and exam development. All PCB directors are CPP, PCI, PSP, and/or APP certified.

Directors of the PCB manage the certification programs by ensuring 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 Global Board of Directors. Directors 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, and 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 the individual 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 remain 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 105 countries proudly maintain their ASIS board certifications.

## Is ASIS membership required?

Membership to ASIS is not required, however, members enjoy many advantages, including discounts on all certification-related products and services including exam fees, prep materials, study groups, and more! And, once you get certified, ASIS members continue to receive discounts for their required continuing education credits. Before applying to take an ASIS certification exam, become a member first. Right away, you'll see the benefits!

## Which Certification 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 or more years of compensated security experience.

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 needs.

## 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 must:**

- ◆ Have been employed full-time in a security-related role. Current employment is not required.
- ◆ Up to one year of internship experience can be counted towards this requirement, provided it is directly relevant to the certification and full-time (internships can be unpaid for CPP, PCI, and PSP).
- ◆ 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. 37).
- ◆ Agree to abide by the policies of the ASIS Certification programs as described in this handbook and the ASIS Recertification Guide.

## ELIGIBILITY REQUIREMENT CHANGES IN 2023

(Updated 20 Feb 2024) In 2023, the PCB voted to reduce the eligibility requirements for the APP certification program. These changes were made after a thorough review of the intended audience for the APP, candidate data, and APP certification trends. After the analysis, the PCB voted to change the experience requirement for the APP to require 1 or more years of compensated security experience, no higher education, effective November 1, 2023.

ELIGIBILITY REQUIREMENTS				
	APP*	PSP	PCI	CPP
No Higher Education	1 year	5 (4) years	5 (4) years	7 (6) years
Bachelor's Degree	1 year	4 (3) years	4 (3) years	6 (5) years
Master's Degree	1 year	3 (3) years	3 (3) years	5 (4) years
Responsible Charge/Case Mgt	0 years	0 years	2 years	3 years
<b>Notes:</b> Numbers in parentheses indicate requirements for those holding the APP. * APP requires 1 year of compensated experience.				

# Associate Protection Professional

## APP BOARD CERTIFICATION IN SECURITY FUNDAMENTALS

ASIS International launched the Associate Protection Professional (APP) certification program in 2019, as 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 or more years of compensated security experience\*. The exam will measure the professional’s knowledge of security fundamentals, business operations, risk management, and response management. (Updated 20 Feb 2024)

### APP Eligibility Requirements

Security Experience*	Education
One year	No higher education degree

\*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 Impact on Eligibility Requirements for Other ASIS Certifications

The chart below shows how the eligibility requirements for the other ASIS certifications are altered for those holding the APP designation.

CPP	With Master’s Degree	With Bachelor’s Degree	No Degree
Current Experience Requirements	5 years	6 years	7 years
With an APP	4 years	5 years	6 years
PCI	With Master’s Degree	With Bachelor’s Degree	No Degree
Current Experience Requirements	3 years	4 years	5 years
With an APP	3 years	3 years	4 years
PSP	With Master’s Degree	With Bachelor’s Degree	No Degree
Current Experience Requirements	3 years	4 years	5 years
With an APP	3 years	3 years	4 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 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. The candidate will select one answer from the four choices offered. In total, there are 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
2. Local, national, and international public/private partnerships
3. Methods for creating effective working relationships

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

#### Knowledge of

1. The nature of verbal and 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:

**Seven (7) years of security experience\*** (or six years if you already hold an APP), at least three (3) years of which shall have been in responsible charge\*\* of a security function.

##### With a higher education degree:

**Master's Degree or international equivalent** from an accredited institution of higher education and have **five (5) years of security experience\*** (or four years if you already hold an APP), at least three (3) years of which shall have been in responsible charge\*\* of a security function.

#### OR

**Bachelor's Degree or international equivalent** from an accredited institution of higher education and **have six (6) years of security experience\*** (or five years if you already hold an APP), 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 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 means that the applicant has the authority to make independent decisions and take independent actions to determine operational methodology and manage execution of a security related project or process. This definition does not require the individual to supervise others and generally excludes such positions as patrol officer or the equivalent.

### CPP Body of Knowledge

To be awarded the CPP designation, a candidate must pass a comprehensive examination consisting of approximately 225 multiple-choice questions. The candidate will select one answer from the four choices offered. In total, there are 200 "live," scoreable questions and 25 pre-test questions. Knowledge in seven major areas (domains) is tested.

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

## DOMAIN ONE

### Security Principles and Practices (22%)

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

#### Knowledge of

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

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

#### Knowledge of

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

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

#### Knowledge of

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

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

#### Knowledge of

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

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

#### Knowledge of

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

## DOMAIN TWO

### Business Principles and Practices (15%)

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

#### Knowledge of

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

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

#### Knowledge of

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

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

#### Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

## DOMAIN THREE

### Investigations (9%)

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

Knowledge of

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

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

Knowledge of

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

**TASK 3: Manage or conduct surveillance processes.**

Knowledge of

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

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

Knowledge of

1. Financial and fraud related crimes
2. Intellectual property and espionage crimes



3. Crimes against property (e.g., arson, vandalism, theft, sabotage)
4. Cybercrimes (e.g., distributed denial of service (DDoS), phishing, ransomware)
5. Crimes against persons (e.g., workplace violence, human trafficking, harassment)

**TASK 5: Manage or conduct investigative interviews.**

Knowledge of

1. Interview and interrogation techniques
2. Techniques for detecting deception
3. Non-verbal communication and cultural considerations
4. Rights of interviewees
5. Required components of written statements
6. Legal considerations pertaining to managing investigative interviews

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

Knowledge of

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

## DOMAIN FOUR

### Personnel Security (11% )

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

## DOMAIN FIVE

### Physical Security (16%)

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

Knowledge of

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

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

*Knowledge of*

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

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

*Knowledge of*

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

## DOMAIN SIX

### Information Security (14%)

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

*Knowledge of*

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

8. Integration of facility and system plans, drawings, and schematics

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

*Knowledge of*

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

**TASK 3: Implement and manage an integrated information security program**

*Knowledge of*

1. Information security including confidentiality, integrity, and availability
2. Information security systems methodology
3. Authentication techniques (e.g., multi-factor, biometrics)
4. Continuous evaluation and improvement programs
5. Ethical hacking and penetration testing techniques and practices
6. Encryption and data masking techniques (e.g., cryptography)
7. Systems integration techniques (e.g., interoperability, licensing, networking)
8. Cost-benefit analysis methodology
9. Project management techniques
10. Budget review process (e.g., system development lifecycle)
11. Vendor evaluation and selection process
12. Final acceptance and testing procedures
13. Protection technology and forensic investigations

14. Training and awareness programs to mitigate threats and vulnerabilities (e.g., phishing, social engineering, ransomware, insider threats)

## DOMAIN SEVEN

### Crisis Management (13%)

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

Knowledge of

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

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

Knowledge of

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

**TASK 3: Respond to and manage an incident.**

Knowledge of

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

**TASK 4: Manage incident recovery and resumption of operations.**

Knowledge of

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

---

# Professional Certified Investigator

---

## PCI BOARD CERTIFICATION IN INVESTIGATIONS

The Professional Certified Investigator (PCI®) credential provides demonstrable proof of knowledge and experience in professional responsibility, investigative techniques and procedures, and case presentation.

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:

#### Without higher education degree:

**Five (5) years of investigations experience** (or four years if you already hold an APP), including at least two years in case management\*

#### With a higher education degree:

**Master's Degree or international equivalent** from an accredited institution of higher education and have **three (3) years of investigations experience**, including at least two years in case management\*

**OR**

**Bachelor's Degree or international equivalent** from an accredited institution of higher education and **have four (4) years of investigations experience** (or three years if you already hold an APP), including at least two years in case management\*

\*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.

**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, and Workplace Violence

### PCI Body of Knowledge

To be awarded the PCI designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions. The candidate will select one answer from the four choices offered. In total, there are 125 "live," scoreable questions and 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.

In 2022/2023, ASIS conducted a job analysis study to ensure the PCI Body of Knowledge still represents the knowledge and skills needed to be a successful investigator. Exam questions regarding the new information will start to appear on the exam in early 2024. (Updated 20 Feb 2024)

The updated Body of Knowledge follows. To review the approved changes, see the [PCI Test Specifications \(2023 JA Updates\)](#) document.

## DOMAIN ONE

### Professional Responsibility (28%)

**TASK 1: Analyze case for applicable ethical conflicts.**

Knowledge of:

1. Nature/types/categories of ethical issues related to cases (e.g., attorney-client, conflict of interest, fiduciary, potential for dual role bias/discrimination, specific area competency)
2. The role of applicable laws, regulations, codes, and organizational policies/administrative guidelines in conducting investigations

**TASK 2: Assess case elements, strategies, and risks.**

Knowledge of:

1. Case categories (e.g., civil, cyber, criminal, internal, financial, workplace violence)
2. Qualitative and quantitative analytical methods and tools
3. Strategic/operational analysis
4. Criminal intelligence analysis
5. Risk identification and impact
6. Stakeholder identification

**TASK 3: Determine investigative goals and develop strategy.**

Knowledge of:

1. Initial projected case type (e.g., administrative, criminal)
2. Cost-benefit analysis
3. Procedural options
4. Case flow / investigative plan
5. Investigative methods

**TASK 4: Determine and manage investigative resources.**

Knowledge of:

1. Resource requirements (e.g., equipment, internal and external liaisons, personnel)
2. Resource allocations (e.g., budget, time)
3. Case management practices (e.g., chain of custody procedures, documentation requirements, case closure)

**TASK 5: Identify, evaluate, and implement investigative process improvements.**

Knowledge of:

1. Process improvement techniques (e.g., gap analysis, project management techniques)
2. Internal review (e.g., human resources, internal liaisons, legal, management)
3. External review (e.g., accreditation agency, external liaisons, regulatory bodies)
4. Investigative resources (e.g., administrative records, Open-Source Intelligence (OSINT))
5. Investigative tools (e.g., case management software, data collection software, digital forensic software)

## DOMAIN TWO

### Investigative Techniques and Procedures (52%)

**TASK 1: Conduct surveillance by physical, behavioral, and electronic means.**

Knowledge of:

1. Surveillance authorization and restrictions (e.g., legal considerations, types of surveillance)
2. Surveillance tools (e.g., analytics, equipment, metadata, software, system logs)
3. Pre-surveillance activities (e.g., advance assessment, logistics, planning, resources)
4. Procedures for documenting surveillance activities (e.g., case management solutions, privacy concerns, secure storage)

**TASK 2: Conduct interviews of individuals.**

Knowledge of:

1. Interview types (e.g., subject, witness, person of interest)
2. Interview techniques
3. Special considerations (e.g., environment, interview subject's mental health, translator, in-person vs. remote)
4. Indicators of deception (e.g., evasiveness, non-verbal communication, word choice)
5. Subject statement documentation (e.g., audio, video, written)
6. Representation considerations (e.g., juvenile advocacy, legal counsel, union representation)

**TASK 3: Collect and preserve evidence.**

Knowledge of:

1. Sources of evidence (e.g., biological, digital, physical)
2. Methods/procedures for collection of various types of evidence
3. Methods/procedures for preservation of various types of evidence (e.g., biological, computer operations, digital media)
4. Chain of custody considerations and requirements (e.g., physical, digital, biological)

**TASK 4: Conduct research by physical, digital, and electronic means.**

Knowledge of:

1. Methods of research using physical, information technology, and operational technology resources
2. Information sources (e.g., databases, digital media, government, open source, proprietary)
3. Methods of analysis of research results
4. Research documentation (e.g., findings)

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

Knowledge of:

1. External information sources
2. Liaison development and maintenance
3. Liaison techniques (e.g., formal, informal)
4. Techniques for using and synthesizing external information (e.g., documented vs. undocumented, protecting sources and sensitivities, redacting)

**TASK 6: Use investigative techniques.**

Knowledge of:

1. Legal, administrative, and organizational considerations
2. Concepts, principles, and methods of video/audio recordings
3. Concepts, principles, and methods of forensic analysis (e.g., biological, digital, physical)
4. Concepts, principles, and methods of undercover investigations
5. Concepts, principles, and methods of threat and risk assessments
6. Concepts, principles, and methods of applying IT/OT technologies
7. Use of confidential sources

## DOMAIN THREE

### Case Presentation (20%)

**TASK 1: Prepare report to substantiate investigative findings.**

Knowledge of:

1. Critical elements and format of an investigative report (e.g., audience/legal considerations, addressing privacy and confidentiality, types of report)
2. Investigative terminology
3. Logical sequencing of information

**TASK 2: Prepare and present testimony.**

Knowledge of:

1. Types of testimony (e.g., administrative hearings, criminal and civil proceedings, depositions)
2. Preparation for testimony (e.g., pre-trial rehearsal)
3. Testimony best practices

---

# Physical Security Professional

---

## PSP BOARD CERTIFICATION IN PHYSICAL SECURITY

The Physical Security Professional (PSP®) credential provides demonstrable proof of knowledge and experience in physical security assessment; application, design, and integration of physical security systems; and implementation of physical 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:

#### **Without higher education degree:**

**Five (5) years of physical security experience\*** (or four years if you already hold an APP)

#### **With a higher education degree:**

**Master's Degree or international equivalent\*** from an accredited institution of higher education and have **three (3) years of physical security experience**

**OR**

**Bachelor's Degree or international equivalent\*** from an accredited institution of higher education and **have four (4) years of physical security experience** (or three years if you already hold an APP)

\*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.

### PSP Body of Knowledge

To be awarded the PSP designation, a candidate must pass a comprehensive examination consisting of approximately 140 multiple-choice questions. The candidate will select one answer from the four choices offered. In total, there are 125 "live," scoreable questions and 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.

In 2022, ASIS conducted a job analysis study to ensure the PSP Body of Knowledge still represents the knowledge and skills needed to be a successful physical security manager. Only minor changes were made and noted below in **green** (these minor changes were made by the subject matter experts for better clarity). Exam questions regarding these updates started to appear on the exam in late 2023.

## DOMAIN ONE

### Physical Security Assessment (34%)

#### Task 1: Develop a physical security assessment plan.

##### Knowledge of:

1. Key area or critical asset identification
2. Risk assessment models and considerations (e.g., inside-outward, outside-inward, site-specific risk assessment, functional approach)
3. Qualitative and quantitative assessment methods
4. Types of resources & guidelines needed for the assessment (e.g., stakeholders, budget, equipment, policies, standards)

#### Task 2: Identify assets to determine their value, critically, and loss impact.

##### Knowledge of:

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

#### Task 3: Assess the nature of the threats and hazards so that the risk can be determined.

##### Knowledge of:

1. The nature, types, severity, and likelihood of threats and hazards (e.g., natural disasters, cyber, criminal events, terrorism, socio-political, cultural)
2. Operating environment (e.g., geography, socioeconomic environment, criminal activity, existing security countermeasures, security risk level)
3. Potential impact of external organizations (e.g., competitors, organizations in immediate proximity) on facility's security program
4. Other internal and external factors (e.g., legal, loss of reputation, economic, supply chain) and their impact on the facility's security program

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

##### Knowledge of:

1. Relevant data and methods for collection (e.g., security survey, interviews, incident reports, crime statistics, personnel issues,

issues experienced by other similar organizations)

2. Effectiveness of current security technologies/equipment, personnel, and procedures
3. Interpretation of building plans, drawings, and schematics
4. Applicable standards/regulations/codes and where to find them
5. Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security

#### Task 5: Perform a risk analysis to develop countermeasures.

##### Knowledge of:

1. Risk analysis strategies and methods
2. Risk management principles
3. Analysis and interpretation of collected data
4. Threat/hazard and vulnerability identification
5. Loss event profile analyses (e.g., consequences)
6. Appropriate countermeasures related to specific risks
7. Cost benefit analysis (e.g., return on investment (ROI), total cost of ownership)
8. Legal and regulatory considerations related to various countermeasures/security applications (e.g., video surveillance, privacy issues, personally identifiable information, life safety)

## DOMAIN TWO

### Application, Design, and Integration of Physical Security Systems [35%]

#### Task 1: Establish security program performance requirements.

##### Knowledge of:

1. Design constraints (e.g., regulations, budget, materials, system compatibility)
2. Incorporation of risk analysis results in design
3. Relevant security terminology (e.g., punch list, field test)
4. Relevant security concepts (e.g., CPTED, defense-in-depth, the 4 Ds- deter, detect, delay, deny)
5. Applicable codes, standards, and guidelines
6. Operational requirements (e.g., policies, procedures, staffing)



7. Functional requirements (e.g., system capabilities, features, fault tolerance)
8. Performance requirements (e.g., technical capability, systems design capacities)
9. Success metrics

**Task 2: Determine appropriate physical security countermeasures.**

Knowledge of:

1. Structural security measures (e.g., barriers, lighting, locks, blast mitigation, ballistic protection)
2. Crime prevention through environmental design (CPTED)
3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)
4. Security staffing (e.g., officers, technicians, management, administration)
5. Personnel, package, and vehicle screening
6. Emergency notification systems (e.g., mass notifications, public address, two-way intercom)
7. Principles of data storage and management (e.g., cloud, on-premise, redundancy, retention, user permissions, personally identifiable information, regulatory requirements)
8. Principles of network infrastructure and physical network security (e.g., token ring, LAN/WAN, VPN, DHCP vs. static, TCP/IP)
9. Security audio communications (e.g., radio, telephone, intercom, IP audio)
10. Systems monitoring and display (e.g., control centers/consoles, central monitoring station)
11. Primary and backup power sources (e.g., grid, battery, UPS, generators, alternative/renewable)
12. Signal and data transmission methods (e.g., copper, fiber, wireless)
13. Visitor and vendor management policies

**Task 3: Design physical security systems and project documentation.**

Knowledge of:

1. Design phases (e.g., pre-design, schematic development, construction, documentation)
2. Design elements (e.g., calculations, drawings, specifications, review, technical data)
3. Construction specification standards (e.g., Construction Specifications Institute, Owner's equipment standards, American Institute of Architects (AIA) MasterSpec)
4. Systems integration

5. Project management concepts
6. Scheduling (e.g., Gantt charts, PERT charts, milestones, objectives)
7. Cost estimation and cost-benefit analysis of design options (e.g., value engineering)

## DOMAIN THREE

### Implementation of Physical Security Measures [31%]

**Task 1: Outline criteria for pre-bid meeting.**

Knowledge of:

1. Bid process (e.g., site visits, RFI, substitution requests, pre-bid meeting)
2. Bid package types (e.g., RFP, RFQ, IFB, sole source)
3. Bid package components (e.g., project timelines, costs, personnel, documentation, scope of work)
4. Criteria for evaluation of bids (e.g., cost, experience, scheduling, certification, resources)
5. Technical compliance criteria
6. Ethics in contracting

**Task 2: Develop procurement plan for goods and services.**

Knowledge of:

1. Vendor evaluation and selection (e.g., interviews, due diligence, reference checks)
2. Project management functions and processes
3. Procurement process

**Task 3: Manage implementation of goods and services.**

Knowledge of:

1. Installation and inspection techniques
2. Systems integrations
3. Commissioning
4. Installation problem resolution (e.g., punch lists)
5. Systems configuration management (e.g., as-built drawings)
6. Final acceptance testing criteria (e.g., system acceptance testing, factory acceptance testing)
7. End-user training requirements

**Task 4: 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 (e.g., establishing KPIs, performance review, improvement processes, recruiting, onboarding, progressive discipline)
3. Security personnel professional development (e.g., training, certification)
4. General, post, and special orders
5. Security personnel uniforms and equipment
6. Security awareness training and education for non-security personnel

**Task 5: Monitor and evaluate program throughout the system life cycle.**

*Knowledge of:*

1. Maintenance of systems and hardware (e.g., preventative, corrective, upgrades, calibration, service agreements)
2. Warranty types (e.g., manufacturer, installation, replacement parts, extended)
3. Ongoing system training (e.g., system upgrades, manufacturer's certification)
4. System evaluation and replacement process

## TAKING REMOTE PROCTORED EXAMS

ASIS offers remote proctored exams that you can take in the comfort of your home. The exams are the same high caliber as they have always been but now you do not have to travel to a Prometric test center to sit for the exam. When you schedule your exam, you will decide whether to take the exam at a Prometric test center or by using Prometric's ProProctor option. And while there will be no difference in the exams themselves, there are additional technical requirements you must have if you select the ProProctor exam delivery option.

**DUE TO FIREWALL SECURITIES, IT IS HIGHLY RECOMMENDED THAT YOU DO NOT TAKE A REMOTE PROCTORED EXAM ON YOUR COMPANY COMPUTER.**

Please read the [Technical Requirements and Other FAQs](#) and [Know Before You Test](#) information before deciding which testing method is best for you.

Common problems encountered during a remote proctored exam include:

- ◆ Weak internet connection or bandwidth issues.
- ◆ Camera or microphone not working.
- ◆ Proper ID not provided to proctor

If your internet bandwidth is poor and you lose internet connectivity and/or your webcam and microphone are inoperable, and you are not able to complete your exam, you will forfeit the exam fee paid and will have to pay an exam retake fee in order to test within your two-year eligibility period.

## 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 valid, 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

**All foreign-language submissions must be accompanied with an English translation.**

### 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 [certification@asisonline.org](mailto:certification@asisonline.org).

## APPLICATION FEES

ASIS exams are offered at Prometric test centers throughout the world or through Prometric's ProProctor platform, which allows you to take the exam at your home.

The ASIS Global Board of Directors has approved special fees for those individuals who live in Emerging Markets, as identified by the World Bank.

View the [list of countries](#) identified as Emerging Markets by the World Bank.

To receive the member discount, please [become a member](#) BEFORE submitting your certification application.

### Fees for the CPP, PCI, and PSP:

**ASIS members: \$550**

**Emerging Market 1: \$450**

**Emerging Market 2: \$430**

**Nonmembers: \$855**

**Emerging Market 1: \$680**

**Emerging Market 2: \$645**

### Fees for the APP:

**ASIS members: \$280**

**Emerging Market 1: \$250**

**Emerging Market 2: \$240**

**Nonmembers: \$585**

**Emerging Market 1: \$475**

## Emerging Market 2: \$455

**Note: All fees include a nonrefundable \$150.**

**ASIS study materials, which are recommended but not required, must be purchased separately.**

### Refunds

If your application is cancelled or denied for any reason, you will receive a refund of your fee minus a \$150 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.

### 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, or the eligibility period ends, may reapply by submitting a new certification application.

Candidates paying the retesting fee will receive an exam retake authorization email from ASIS after the retake eligibility is in Prometric's scheduling system.

Once the exam retake authorization email has been received, a new exam appointment can be made.

*Retest fees are nonrefundable.*

### Retest fees for the CPP, PCI, and PSP:

**ASIS members and nonmembers: \$455**

**Emerging Market 1: \$340**

**Emerging Market 2: \$315**

### Retest fees for the APP:

**ASIS members and nonmembers: \$300**

**Emerging Market 1: \$225**

**Emerging Market 2: \$210**

## APPROVAL NOTIFICATION FROM ASIS

If you are approved to take an ASIS certification exam, an authorization to test email will be emailed to you. This letter will include:

- ◆ Your eligibility ID (ASIS 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 email to take and

pass your exam before you must reapply by submitting a new certification application.

**Remember the name on your IDs must exactly match the name on your authorization to test email.**

### Appealing a Decision

An appeal procedure is available to any individual who has applied for or received an ASIS certification and wants to contest any adverse decision. This policy applies only to the procedural aspects of the credentialing process. Those areas not subject to appeal are further identified under the section heading "General Principles Relating to Appeals" at the end of this section. Any individual who does not file a written request for an appeal within the required time limit shall waive the right to appeal. Submitting an appeal will not result in any discriminatory actions against the appellant.

Throughout the certification process, individuals may appeal certain decisions made by ASIS. Examples of appeals include:

- ◆ Decisions regarding eligibility
- ◆ Eligibility time limits
- ◆ Recertification CPE interpretations
- ◆ Criminal Convictions
- ◆ Unauthorized Use

To appeal a decision regarding your certification, the following is required:

- ◆ Appeals must be submitted within 30 days of an applicant receiving notification of an adverse decision, with day one as the date of the applicant's notification email.
- ◆ A letter must be submitted explaining actions being appealed to [certification@asisonline.org](mailto:certification@asisonline.org).
  - Appeals must be addressed to the PCB Certificant Relations Committee.
  - Appeals must identify the adverse decision being appealed and state the reasons for the appeal. Any new or additional information for consideration should be included in the letter.

## PCB Certificant Relations Appeal Process

- ◆ Once the written appeal has been received, the ASIS Certification Team will log the appeal in the appropriate database.
- ◆ The appeal will be evaluated by the Certification Director for compliance with ASIS appeal submission policies.
- ◆ The appeal and related materials will be forwarded to the PCB Certificant Relations Committee for a decision. The committee will make its best effort to make a decision within 90 days of receipt of the appeal. ASIS may have this decision reviewed by legal counsel prior to being sent to appellant.
- ◆ A record of the appeal decision will be recorded and logged into the appeals tracking spreadsheet and in the appellant's online record.
- ◆ Whenever possible, the appellant will receive progress reports of the process and will be notified in writing of the decision of the Certificant Relations Committee and the reasons for that decision within 30 days of the review.
- ◆ The Committee's decisions are final and may not be appealed.

## General Principles Relating to Appeals

- ◆ Appeals will be considered for hardships as outlined in the ASIS Extension Policies.
- ◆ Appeals will be considered if the appellant feels ASIS Staff made an error in the application review.
- ◆ ASIS eligibility requirements as well as the other policies of the certification program cannot be appealed.
- ◆ The passing score of the exam cannot be appealed.

## SCHEDULING YOUR EXAM

After you receive your Approval to Test email from ASIS, you will go to the [Prometric website](#) to schedule your exam.

There are two ways to take your exam. You will have the option to:

1. Take the exam in a **Prometric testing center**.  
OR
2. Take the exam through **Prometric's remote proctored ProProctor platform** using your own computer (**company-owned computers** are not recommended). If you choose to take

the exam using ProProctor, please make sure you can meet these [technical requirements](#).

ASIS exams are offered year-round. You will not be able to schedule your exam until you have been approved to take the exam and have received the authorization to test email.

## Making Your Exam Appointment

### Online scheduling

Whether you would like to test in a test center or remote, your exam appointment can be scheduled online at [prometric.com/asis](#)

You will be asked for:

- ◆ Your ASIS ID, which can be found on your authorization to test email
- ◆ 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 (Testing Center or Remote Proctored), 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. When scheduling a remote proctored exam, you will need to have this confirmation number available.

### Confirmation Email from Prometric

Once your exam appointment is confirmed, Prometric will send you an email with your exam date, time, location (test center or remote proctored), and unique 16-digit confirmation number. **Make sure to print out this letter and have with you on testing day along with two forms of identification**, one of which must be a valid, government-issued photo ID (such as a passport or driver's license, employee ID card, state ID card). Acceptable forms of secondary ID include credit card, check card, ATM card and **all must have the candidate's signature**. (Social Security cards and military IDs are not an acceptable form of identification.)

## Choosing Your Exam (English or Spanish)

The CPP, PCI, PSP, and APP 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). Those who select a Spanish-language exam will be assigned a Spanish-speaking proctor.

## 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.

## Extension Policies

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, if on active military duty and deployed into a remote or hazardous area, or in certain circumstances, such as childbirth, adoption, or acceptance of a child in foster care. The applicant or certificant is required to provide documentation of extenuating circumstances (e.g., doctor’s note or other appropriate proof of circumstance). 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. ASIS certification candidates and certificants who wish to utilize an extension should contact the ASIS certification team no later than 60 days before eligibility end date or certification end date. Certificant extensions will only be considered if at time of extension application, the certificant has completed 50% or more of the required

CPE credits for their current certification cycle.

Recertification use case example:

- Current Certification Cycle: 1 May 2021 - 31 May 2024
  - o 6-month cycle extension: 30 November 2024 to earn and report CPE
- New Certification Cycle for next cycle: 1 December 2024 – 31 December 2027

In times of crises that affect many people at one time (e.g., pandemic, national emergencies, natural disasters), extension policies may be modified in the short term. All affected by the crisis will be notified of the policy changes. (Updated 20 Feb 2024)

## Cancellation Policy

**Note: Cancellation policies apply to both test center and remote proctored exams.**

Due to frequent cancellations and short notification rescheduling, Prometric has indicated that there may be inadequate capacity. 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](https://www.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.
- ◆ 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 retest fee.

**Cancellation policies apply to both test center and remote proctored exams. Prometric makes NO exceptions to this rule.**

## “No Shows”

If you fail to cancel or reschedule your exam and you do not take the exam on the scheduled day, 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

No matter whether you are taking the exam at a testing center or taking it through remote proctoring, you will be required to follow specific check-in procedures.

### Check-in at a Prometric Testing Center

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.**

## What to Bring and Not Bring to Testing Center

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 in 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.

### Check-in for Remote Proctored Exams

Candidates testing with a remote proctored exam should make sure to allow 15 minutes to prepare your testing environment. **Due to increased security protocols, we strongly recommend NOT taking the exam on a company-owned computer.**

Check-in for remote proctored exams is a two-step process:

#### STEP ONE – Checking Your Identification

**Image Capture** – Using the ProProctor software, you will take and capture a picture of your face.

**ID Capture** – Next, you will capture a photo of your ID (see Check-in ID Requirements for acceptable ID). For those taking the exam remotely, you will only need one form of ID.

**Checklist** – You will review the checklist on screen to ensure you are ready to launch the exam

#### STEP TWO – Meet Your Prometric Readiness Agent

**Candidate Detail Confirmation** – You will have a video chat with the agent to confirm your personal information

**360 Environmental Check** – Using your webcam, you will show the agent a 360-degree scan of your room and your workstation. You'll need a medium/large hand-held mirror so Readiness Agent can see your computer, if your computer does not have an external webcam. **NOTE: DO NOT HAVE YOUR LAPTOP HOOKED TO A DOCKING STATION.**

**Candidate Person Check** – Your Readiness Agent will ask you to stand up to do a scan of

your person. This scan will include – but is not limited to – conducting a sleeve, pocket, and glasses check. Additionally, you will be asked to turn all pockets inside out. NOTE: EMPTY YOUR POCKETS BEFORE STARTING THE CHECK-IN PROCESS.

## Check-in ID Requirements

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

**Two forms of identification are required at the test center (only one form of ID is needed for those taking the exam remotely),** one of which must be a valid, government-issued photo ID (such as a passport, driver’s license, employee ID card, state ID card). Acceptable forms of secondary ID include credit card, check card, ATM card and **all must have the candidate’s signature.** (Social Security cards and military IDs are 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 from Prometric 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, or national ID. Expired IDs and military IDs will not be accepted.

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

## Security Measures at Testing Center

Prometric testing center 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 accommodation approved in advance.

Candidates may opt to use the noise-reducing headphones available at some 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 (except water), and smoking are not permitted during the exam. If you wish to have water during your exam appointment, it must be in a clear container with a lid/cap. No labels or other decorations are permitted on the bottle. Your water bottle will be inspected as part of the check-in process. 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 childcare is not provided.

## During the Exam

Once you have completed the check-in process, you will be assigned to a testing station or a remote proctor.

### At a testing station

- ◆ You will be provided with 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) or remote proctor; however, if you take a break, the time clock on the exam is not stopped. This is considered an unscheduled break.
- ◆ No breaks are scheduled.
- ◆ No conversation about the test is permitted with the TCA, proctors, or other test takers.

**Your remote setting must meet the following requirements:**



- ◆ Testing location must be indoors (walled), well lit, free from background noise and disruptions.
- ◆ No third party may be present in the room or enter the room for the duration of the exam. If this occurs, your exam will be terminated and/or your results invalidated.
- ◆ Your workstation and surrounding area must be free of pens, paper, electronic devices, etc.
- ◆ Two tissues are permitted at the workstation but must be inspected by the Proctor prior to the start of exam.
- ◆ Review the [ProProctor User Guide \(prometric.com\)](https://www.prometric.com) for additional information.

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, *preliminary* exam results will be emailed to the email address you provided to Prometric (allow up to five hours to receive this email). Official verification of your score will be sent to you by ASIS approximately three weeks after you take the exam. You can also go to Prometric's [website](https://www.prometric.com) to retrieve your score report (you will be asked for your confirmation number and last name).

### Post-Exam Survey

When you receive your official score report from ASIS, you will be provided with a link to complete a post-administration survey about your testing experience. 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/closures>

### 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” (scored) and 25 pre-test (unscored) items. 4 hours.
- ◆ PSP – 125 “live” (scored) and 15 pre-test (unscored) items. 2.5 hours.
- ◆ PCI – 125 “live” (scored) and 15 pre-test (unscored) items. 2.5 hours.
- ◆ APP – 100 “live” (scored) and 25 pre-test (unscored) items. 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. 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 and indicate the same level of performance regardless of the specific exam version taken. A scaled score is a transformed raw exam score (the number of exam questions answered correctly) into to a consistent and standardized scale. ASIS scaled scores are based on the standard adopted by ASIS regarding the level of knowledge necessary to pass the exams. **A scaled**

**score of at least 650 is required to pass ASIS examinations.** 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) 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 the ASIS PCB 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 using a verified key or correct response option. Electronic scoring reduces scoring errors and therefore it is virtually impossible for your exam score to be incorrect. **Multiple choice exams taken by computer-based testing are therefore not eligible for a hand score.** (Updated 20 Feb 2024)

## 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, PSP, and APP 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](http://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 (costs are not included in the application fees). Candidates are encouraged to

refer to the following reference materials as they are preparing for the CPP, PCI, PSP, or APP examinations. 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 a set.

#### Protection of Assets (POA)

POA is a comprehensive reference covering a range of technical and managerial subjects providing the solutions necessary to meet the security demands of the 21st century. The POA was [updated in June 2021](#).

- [e-Book](#) (bundle)
- [Print](#) (bundle)

#### ASIS Standards & Guidelines

ASIS Standards set forth industry-recommended best practices on specific concerns inherent to the security industry and provide tools and processes for implementation. Along with the POA, these seven standards and guidelines make up the CPP reference set.

Standards:

- Senior Security Executive
- Security and Resilience in Organizations and Their Supply Chains—Requirements with Guidance\*
- Workplace Violence Prevention and Intervention
- Physical Asset Protection

Guidelines:

- General Security Risk Assessment Guideline
- Information Asset Protection Guideline
- Preemployment Background Screening Guideline

ASIS Members are entitled to free online access to each standard and guideline.

- [Free e-Book Access for ASIS Members](#)
- [Standards & Guidelines CPP softcover bundle](#)

### PROFESSIONAL CERTIFIED INVESTIGATOR

Two publications now comprise the PCI reference materials.

- [POA Investigations volume](#)
- [ASIS International's Investigations Standard](#) (free e-Book access for ASIS Members)

## PHYSICAL SECURITY PROFESSIONAL

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

- [POA Physical Security volume](#)
- [Implementing Physical Protection Systems: A Practical Guide, 3rd Ed](#)

Guidelines:

- [Business Continuity Management Guideline](#) (free e-Book access for ASIS Members)

Standards:

- [ASIS Physical Asset Protection Standard](#) (free e-Book access for ASIS Members)

## 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

- Physical Asset Protection
- Security and Resilience in Organizations and their Supply Chains - Requirements with Guidance
- Investigations
- Workplace Violence and Active Assailant – Prevention, Intervention, and Response
- Risk Assessment

### Protection of Assets Volumes ([Updated June 2021](#))

- Protection of Assets: Business Principles
- Protection of Assets: Crisis Management
- Protection of Assets: Security Management  
(Note: Replaces POA Information Security volume)

### ASIS offers three pricing bundles for the APP:

- [APP Standards Bundle](#)
- [Protection of Assets Bundle for the APP Certification](#)
- [APP Complete Reference Set](#)

For those who have an APP and are studying for the CPP, ASIS offers an [APP Transition](#) package that include the Investigations, Physical Security, and Personnel volumes of the POA. Also offered is an [APP to CPP Complete Reference Set](#).

ASIS offers other preparatory items (such as flash cards and study manuals). Please search for these items in the [ASIS Store](#).

## CERTIFICATION PREPARATION

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 begins and end date, and certification number. Please allow at least four weeks to receive your certificate.

Also, you will receive an email from Credly (ASIS' digital credentialing partner) with the subject line "You've earned a badge from ASIS International." The message will provide an invitation and instructions to claim your digital badge(s) and certificate (s). Please allow a minimum of two weeks to receive your digital credentials.

Wear your new designation proudly! Add it to your designation 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 (CPEs). 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**

(Updated 20 Feb 2024) In addition to the ASIS International Code of Ethics and Code of Conduct, all 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 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.

Per ANAB ISO 17024 Standards, if your ASIS Certification is revoked, you may be asked to return your certificate.

### **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), Associate Protection Professional (APP), Professional Certified Investigator (PCI), or Physical Security Professional (PSP) 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, as required by the ASIS Board Certification Handbook and the Board Recertification Guide. Additionally, examination candidates are not permitted to utilize another individual, company, and/or artificial intelligence (AI) during your examination administration; this includes, but is not limited to, any form of proxy tester, natural language processing, predictive analysis, generative AI, open AI, etc.

I understand that in order to maintain my certification, I must re-certify 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 an 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 only limited to, no longer being in 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 email, mailing 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.

I attest that I have completed all certification and/or recertification requirements as required by the ASIS Board Certification Handbook or the Board Recertification Guide, as appropriate. (Updated 20 Feb 2024)

## 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 may 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:

- ◆ The candidate must be a CPP, PCI, PSP, or APP in good standing (e.g., status is "current" and not "lapsed" or "expired").
- ◆ The candidate must have held the certification for twelve consecutive years.
- ◆ The candidate must be currently retired from any form of security employment/practice,

or receiving compensation from same, as defined by the applicable certification exam domain.

- ◆ The candidate must have paid the recertification fee for the current term.

Lifetime designees in good standing are subject to the same conditions of other certificants except that recertification will not be required and recertification fees will not be charged.

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 successfully pass the appropriate certification exam. Although Lifetime Certificants are automatically eligible to sit for the exam of their prior certification, without the need to submit additional supporting materials, they must submit an application. Application fees apply.

If granted a Lifetime Certification, a new certificate with the new designation will be sent. To display this new designation, the certificant will use the following: CPP – Life Certified (Retired), PCI – Life Certified (Retired), or PSP – Life Certified (Retired). One cannot use the designation without these qualifying descriptions.

Per ANSI ISO 17024 Standards, ASIS reserves the right to revoke any Lifetime Certification should it be discovered that the certificant is no longer retired. If a Lifetime Certification is revoked, the Lifetime certificate must be returned to ASIS.

**To apply for lifetime certification**, please complete and submit this [application](#) at [certification@asisonline.org](mailto:certification@asisonline.org). **There is a \$100 fee to apply.**

## 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 or ASIS is compelled to do so by law. Consent to release information must include to whom the candidate or certificant information can be released and the information that can be released. Information cannot be released if the law prohibits this release.

## ASIS CERTIFICATES

All certificates related to the CPP, PCI, PSP, and APP designations are the sole property of ASIS International. The certificate may only be displayed during the time period for which the credential is valid. Certificates remain the property of ASIS and must be returned to ASIS, if requested. The formerly certified individual should immediately cease from using the ASIS International designations and remove them from all printed, electronic, or other forms of communications.

## THIRD-PARTY INTERVENTION

The Professional Certification Board (PCB) sets the policies of the ASIS Certification Programs. There is an appropriate and required “wall” between ASIS certification activities and the ASIS Global Board, ASIS staff, and ASIS’s CEO. Only the PCB can adjudicate certification matters.

Because ASIS certification programs are accredited by ANAB to the ISO 17024 Standard, involving third parties to try to change a decision made by the PCB is against ANAB accreditation requirements and doing so jeopardizes ASIS accreditation status as an international certification body. In addition, ASIS strives to apply our policies consistently in order to be fair to all. Allowing special “rules” to some is simply not fair to the 10,000+ certificants who do follow the policies. Finally, due to confidentiality requirements, the PCB and the Certification Team can only communicate directly with the certificant; they cannot share information with third parties.

## 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 per the instructions in Section III: Process for filing a complaint. The confidentiality of both the complainer as well as the person to whom the complaint is lodged are protected by ASIS Confidentiality Agreements.

The complaint must contain 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.

Whenever possible, ASIS will make progress reports to both the person submitting the complaint and to the person to whom the complaint is lodged. Receipt of the complaint will be sent to the person submitting

the complaint 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. ASIS's complete complaint policy can be found [here](#).

## **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.