PREFERRED CPE PROVIDER PROGRAM GUIDE

ASIS International
1625 Prince Street
Alexandria, VA 22314-2882
Main +1 703.519.6200
www.asisonline.org

TABLE OF CONTENTS

INTRODUCTION

The ASIS International Preferred CPE Provider Program provides ***organizations*** the opportunity to provide pre-approved recertification continuing professional education (CPE) credits for their security- or business management-related continuing education offerings. With Preferred CPE Provider status, ASIS-approved activities can be easily identified by those searching for continuing education toward their recertification.

The ASIS Preferred CPE Provider Program offers two options for those that provide educational programs:

1. **ASIS Annual Preferred CPE Provider** – for organizations that offer multiple educational activities a year.
2. **One-Time ASIS Preferred CPE Provider Event** – for organizations that only offer one educational activity a year. (A one-time event includes a course, one-day event, or one multi-day event.)

Becoming a Preferred CPE Provider will:

- help increase attendance at your courses and seminars.
- allow you to market your activities on the ASIS website (for Annual Preferred CPE Providers only).
- bring peace of mind to your attendees by removing the guesswork over which activities meet recertification requirements.

ASIS International certifications serve as a visible acknowledgment of a mastery of core security principles and skills essential to the best practice of security management. A continued commitment to lifelong learning is a critical component of ASIS's certification program, and designations must be recertified through continuing education activities every three years.

ASIS certification designations include Certified Protection Professional (CPP®), Professional Certified Investigator (PCI®), Physical Security Professional (PSP®), and Associate Protection Professional (APP).

This guide is designed to facilitate the process of applying to become an ASIS International Preferred CPE Provider and to provide continued guidance throughout your participation in the program. This guide is periodically updated as the program is refined and is enforced accordingly.

We look forward to partnering with you!

ASIS International Preferred CPE Provider Team
+1 703.519.6200
preferredprovider@asisonline.org

REQUIREMENTS FOR SUCCESSFUL PARTICIPATION

- The ASIS Preferred CPE Provider Program has been established for ***organizations*** that provide recertification continuing professional education (CPE) credits.

- The subject matter and learning objectives of your continuing education offerings **must** relate to security or business management, as defined by the Body of Knowledge (Appendix B) for each designation. (NOTE: It will be the responsibility of the organization to identify which of their classes are eligible for credit.)

- The organization must provide the resources, facilities, and administrative support to effectively deliver your Preferred CPE Provider programming.

- The organization must provide a participant evaluation process and solicit feedback to ensure continuous improvement in program content and quality.

- Continuing education offerings cannot be a part of a certificant's job duties, company-specific training, or a product endorsement session.

ACTIONS TO BE TAKEN ON BEHALF OF A SUBMITTING ORGANIZATION:

- Submit a completed application (Appendix A), course details (could be examples of last year's courses or sample courses), and the appropriate fee(s).

- Identify a dedicated primary administrative contact for your organization. This primary contact is responsible for fielding questions about courses, whether they are received directly or they are forwarded from ASIS International. Any changes in contact information **must** be reported within 30 days so timely communications won't be missed.

- Become educated on the appropriate certification's Body of Knowledge to ensure that course offerings will be accepted for CPE credit. (See Appendix B)

- Clearly advertise which courses meet the criteria for CPE credits and adhere to the Preferred CPE Provider Program logo usage guidelines provided upon being approved.

- Provide participants with a certificate of attendance (sample in Appendix C) or a letter from host organization confirming participation.

- Provide the URL that goes **directly** to the provider's course offerings page (not the organization's home page) that includes the Preferred CPE Provider logo prominently featured at each pre-approved activity.

- Maintain a list of attendees, the program description, date, number of CPE credits, and presenters. This information should be kept for four years, because exam applicants may include education taken within a three-year certification cycle.

- Renew annually by completing an application to maintain Preferred CPE Provider status.

KEY BENEFITS TO PROVIDER

- Join with a select group of organizations authorized to offer CPEs pre-approved by ASIS Internationals.
- Build recognition for your organization with your listing in a Directory of Preferred CPE Providers on the ASIS International Preferred CPE Provider Program website (for Annual Preferred Providers only).
- Expand the reach of your organization to attract more certified security professionals to your educational offerings.
- Elevate your commitment to providing continuing education for professional development and recertification activities.
- Stand out as an ASIS International Preferred CPE Provider by using the program logo on marketing materials.
- Gain increased exposure via ASIS marketing and brand recognition.
- Receive appropriate tools, resources, and support to ensure your participants can easily and properly receive CPE credit for participation.

APPLICATION PROCESS

Apply by completing the application and paying the appropriate fee.

- Applications will be accepted on a rolling basis throughout the calendar year. Once approved, the Preferred CPE Provider status will be one year, starting on the day your application is approved.

- Provider-approved status expires in one year at month's end. For example, if an application is approved on 1 March 2019, the provider status would expire on 31 March 2020.

- Applications must be submitted in English.

- All course/activity submissions for approval must be submitted **eight weeks prior** to the event date.

- Once applications are reviewed and approved or denied, the organization's primary administrative contact will be notified by email.

    - A provider whose application is approved will be advised of specific ASIS International Preferred CPE Provider Program information, including but not limited to the start and end dates of the one-year Preferred CPE Provider status period and the Preferred CPE Provider logo for use on your website at the course descriptions, marketing materials, certificates of attendance, and letters of participation.

    - A provider whose application is denied will be advised of the reason for the denial and of any opportunity for appeal.

- Once approval is granted, the organization's listing in the Preferred CPE Provider Directory (for Annual Preferred CPE Providers only) will link **directly** to its course offerings page (not the website home page) using the URL submitted on the application. Each pre-approved activity must prominently feature the Preferred CPE Provider logo.

- Provider renewal reminders will be emailed directly to the primary administrative contact 90, 60, and 30 days before the expiration date.

PROVIDER FEES

Fee Type	Amount
Annual Fee – Corporations	$950 (includes $100 nonrefundable application processing fee)
Annual Fee – Non-Profits	$450 (includes $100 nonrefundable application processing fee)
One-Time Event Fee (A one-time event includes a course, one-day event, or one multi-day event.)	$250 (includes $100 nonrefundable application processing fee)
Rush Fee (For urgent requests for approval that are submitted ***LESS THAN*** **eight weeks prior** to the event date.)	$350 (annual and one-time event) (This is in addition to regular fees noted above.)

- ASIS International reserves the right to alter these and other Preferred CPE Provider Program requirements without notice.

- If an application is denied, the annual fee will be refunded, minus the application processing fee.

CONTINUING EDUCATION OFFERINGS

All course offerings will be reviewed during the initial application process after receipt of the submitted Course Submission Form(s) and fee. Please allow up to four weeks for this review. Once approved, ASIS will monitor the use of the Preferred CPE Provider Program to ensure it is being used correctly.

To qualify for CPEs, the organization's continuing education offerings must demonstrate current subject matter and learning objectives that relate to security or business management, as defined by the Body of Knowledge for each designation (Appendix B).

Acceptable methods of course delivery include:

- Seminars or conferences
- Webinars (live or archived)
- Chapter meetings (educational portion only)
- Web-based and other self-study courses
- Higher-level academic courses

NOT ELIGIBLE to Receive CPE Credit
Offerings provided by a single individual, not an organization
Product or service pitches or endorsements
Offerings that are part of a certificant's job duties or company-related training
Offerings that are less than 30 minutes in length

AUDIT PROCESS

- All course offerings will be reviewed during the initial application process.
- In subsequent renewing years, provider offerings will be subject to random audits performed to ensure program quality, integrity, and compliance.

DENIAL AND REVOCATION

- A provider whose application is denied will be advised of the reason for the denial and of any opportunity for appeal and resubmission. Appeals will be considered within 30 days of notification of an adverse decision, with day one as the date of the organization's notification email. Appeals must be sent by email to preferredprovider@asisonline.org and include the action being requested, as well as any new or additional information for consideration. ASIS will consider the appeal and reply within 30 days of receipt. All appeals decisions are final.
- ASIS reserves the right to revoke a Preferred CPE Provider's approval status if it is determined that the provider is in violation of one or more of the terms of agreement. A provider may appeal the revocation of an education program or the ability to claim provider status to ASIS International within 30 days of notification. Appeals must be sent by email to preferredprovider@asisonline.org and include the action being requested, as well as any new or additional information for consideration. ASIS will consider the appeal and reply within 30 days of receipt. All appeals decisions are final.
- If a provider's status is revoked, it must immediately remove the ASIS International Preferred CPE Provider logo from all education offerings and cease using it on any marketing materials, certificates of attendance, or letters of participation. If the provider is an annual provider, it will be removed from the Directory of Preferred CPE Providers.
- If a provider's status is revoked, it is not eligible to submit a Preferred CPE Provider application for 12 months following notice of revocation of approval status.
- It is expected that all providers conduct their business and operations in a legal, ethical, and professional manner. ASIS International reserves the right to revoke a provider's status should it determine that a provider has violated any of these principles, without refund of annual fee.
- Any disputes or legal proceedings should be governed under the Commonwealth of Virginia.

RENEWING AS A PROVIDER

- The Preferred CPE Provider designation is valid for one year.
- At 90, 60, and 30 days before the expiration date, renewal reminders will be emailed directly to your primary administrative contact. (ASIS is not responsible for organizations not receiving this email.

Ultimately it is the responsibility of the Preferred CPE Provider to meet all deadlines.) Make sure to "whitelist" any emails from @asisonline.org.

- It is the primary administrative contact's responsibility to submit a completed application within 30 days prior to the expiration date.

PREFERRED CPE PROVIDER PROGRAM

APPENDIX A: APPLICATION

PROVIDER TERMS OF AGREEMENT

I'm applying as a(n):

☐ Annual Preferred CPE Provider

☐ One-Time Preferred CPE Provider Event

☐ Check here if this is a rush request

☐ Renewing as a Preferred CPE Provider

This agreement is between ASIS International and _____ ("Preferred CPE Provider organization's name") regarding the Provider's participation in the ASIS International Preferred CPE Provider Program. This agreement goes into effect when signed by the provider and approved by ASIS International. In submitting this Preferred CPE Provider Program application, our organization fully understands that it is an application only and does not guarantee Preferred CPE Provider status.

The Provider agrees to the following:

- The ASIS Preferred CPE Provider Program has been established for ***organizations*** that provide recertification continuing professional education (CPE) credits.

- The subject matter and learning objectives of continuing education offerings must relate to security or business management, as defined by the Body of Knowledge for each designation.

- The organization must provide the resources, facilities, and administrative support to effectively deliver your Preferred CPE Provider programming.

- The organization must have a participant evaluation process in place and solicit feedback to ensure continuous improvement in program content and quality.

- Continuing education offerings cannot be a part of a certificant's job duties, company-specific training, or a product endorsement session.

ACTIONS TO BE TAKEN ON BEHALF OF A SUBMITTING ORGANIZATION:

- Submit a completed application, course details (could be examples of last year's courses or sample courses), and the appropriate fee(s).

- Identify a dedicated primary administrative contact for your organization. This primary contact is responsible for fielding questions about courses, whether they are received directly or they are

forwarded from ASIS International. Any changes in contact information **must** be reported within 30 days so timely communications won't be missed.

- Become educated on the appropriate certification's Body of Knowledge to ensure course offerings will be accepted for CPE credit. (See Appendix B)

- Clearly advertise to the general public which courses meet the criteria for CPE credits and adhere to the Preferred CPE Provider Program logo usage guidelines provided upon being approved. For multi session events, all approved courses must be marked on programs and other marketing materials. If the Preferred CPE Provider logo cannot be placed directly on the course description, the organization must clearly show which sessions are available for credit. For instance, a key can be placed in the program that says:

    - ✓ Denotes sessions that have been approved through ASIS Preferred CPE Provider Program and are pre-approved for recertification credit. Candidates will need to provide proof of attendance when self-reporting this activity.

- Provide participants with a certificate of attendance or a letter from the organization confirming participation.

- Provide ASIS with the URL that links **directly** to the course offerings page (not the organization's home page) that includes the Preferred CPE Provider logo prominently featured at each pre-approved activity.

- Maintain a list of attendees, the program description, date, number of CPE credits, and presenters. This information will be kept for four years, because exam applicants may include education taken within a three-year certification cycle.

The Provider understands:

- Preferred CPE Provider status is an annual process and every organization must complete an application yearly to renew provider status. Provider renewal reminders will be emailed directly to the primary administrative contact 90, 60, and 30 days before the expiration date.

- ASIS International reserves the right to revoke a Preferred CPE Provider's approval status if the provider is in violation of one or more terms of agreement.

- If a provider's status is revoked, it is not eligible to submit a Preferred CPE Provider application for 12 months following notice of revocation of approval status. A provider may appeal the revocation of an education program or the ability to claim provider status to ASIS International.

- If a provider's status is revoked, it must immediately remove the ASIS International Preferred CPE Provider logo from all education offerings and cease using it on any marketing materials, certificates of attendance, or letters of participation. If the provider is an annual provider, it will be removed from the Directory of Preferred CPE Providers.

- It is expected that all providers conduct their business and operations in a legal, ethical, and professional manner. ASIS International reserves the right to revoke a provider's status should it determine that a provider has violated any of these principles, without refund of annual fee.

- Any disputes or legal proceedings should be governed under the Commonwealth of Virginia.

First and Last Name (please PRINT) _____

Title _____ Organization _____

Signature _____ Date Signed _____

CONTACT INFORMATION

Please complete all sections. If necessary, attach required supporting documentation in PDF, Excel, or Word document. Be sure to save this form to your desktop prior to filling out.

PROVIDER CONTACT INFORMATION

Organization Name _____

Address _____

City, State, Country, Zip/Postal Code _____

Website _____ Phone Number _____

PRIMARY ADMINISTRATIVE CONTACT

When necessary, be sure to update this information with ASIS International within 30 days.

Contact Name _____

Contact Email _____

Contact Phone Number _____

URL (**Must** link **directly** to educational offerings, not the organization's home page.)

_____

PLEASE ANSWER THE FOLLOWING

1. Indicate on which of the following document(s) the ASIS International Preferred CPE Provider logo will be displayed (check all that apply):

   ☐ Website course description page
   ☐ Marketing materials
   ☐ Certificate of attendance
   ☐ Letter of attendance
   ☐ Other _____

2. Approximately how many different security or business management continuing education activities do you anticipate conducting during the upcoming calendar year?

   Number of programs _____

3. Are your organization's continuing education programs approved by another entity?

   ☐ Yes ☐ No

   If yes, please list the entity _____

ACTIVITY/COURSE SUBMISSION FORM

FOR ANNUAL PREFERRED CPE PROVIDER PROGRAM ONLY

On a separate sheet, please provide details of upcoming events or a sample of previous educational offerings if current details are not yet finalized.

FOR ONE-TIME PREFERRED CPE PROVIDER EVENT ONLY

Please provide details of the event on the submission form below.

Incomplete forms may be rejected or denied approval. If additional space is needed, please submit the documentation in PDF, Excel, or Word document. Be sure to save this form to your desktop prior to filling out.

SESSION TOPIC AND CONTENT

Course title _____

Brief course description (50 words or more) _____
_____
_____
_____

COURSE DELIVERY METHOD:

☐ Seminar or conference
☐ Webinar (live or archived)
☐ Chapter meeting (educational portion only)
☐ Web-based and other self-study courses
☐ Higher-level academic courses

BODY OF KNOWLEDGE

Per the approved certification's Body of Knowledge (Appendix B), list all applicable domains for this course.

_____
_____
_____

CRITERIA FOR CONTINUING PROFESSIONAL EDUCATION (CPE) CREDITS

Those recertifying may claim the direct amount of time spent in an educational activity. ASIS accepts whole and partial hours but all sessions must be at least 30 minutes in length. For instance, a 90-minute session would be reported as 1.5 clock hours. Time for meals, breaks, social gatherings, planning sessions, business meetings, and similar activities are not included.

Number of credits expected to be awarded _____
(ASIS International reserves the right to revise this number.)

LEARNING OBJECTIVES

State at least three clearly relevant learning objectives or industry-related purposes for the program. A learning objective completes the phrase, "At the end of the program, the learner will be able to…"

1. _____

2. _____

3. _____

FEEDBACK

Describe the process used by your organization to monitor and provide feedback for the facilitators and program. Provide a sample.

_____
_____
_____

CHECKLIST

Below please find a checklist to make sure you have completed and are submitting all that is requested to apply to the ASIS International Preferred CPE Provider Program.

Your completed application and all required documents must be included in one PDF before uploading online.

ALL COMPLETED APPLICATIONS SHOULD INCLUDE:

☐ Signed Provider Terms of Agreement

☐ Completed Contact Information, including URL where courses are listed

☐ Completed Activity/Course Submission Form (for one-time Preferred CPE Providers only).

For Annual Preferred CPE Providers, provide details of your upcoming events on a separate sheet or a sample of your previous educational offerings if current details are not yet finalized.

☐ Online Submission of Appropriate Fee:

- Annual Preferred CPE Provider (Corporations) fee:
  $950 (includes $100 nonrefundable application fee)
- Annual Preferred CPE Provider (Non-Profits) fee:
  $450 (includes $100 nonrefundable application fee)
- One-time Preferred CPE Provider Event (online course, event, activity, etc.):
  $250 (includes $100 nonrefundable application fee)
- Rush fee:
  $350 (for activities that are being held less than eight weeks from submission)

If you have any questions, please contact the ASIS Preferred CPE Provider Program Team at +1.703.519.6200 or preferredprovider@asisonline.org.

ASIS International
1625 Prince Street
Alexandria, VA 22314-2882
Main +1.703.519.6200
www.asisonline.org

PREFERRED CPE PROVIDER PROGRAM

APPENDIX B: BODY OF KNOWLEDGE AND DOMAINS

Associate Protection Professional (APP) Body of Knowledge

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

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-hazards 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-hazards 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) Body of Knowledge

DOMAIN ONE

Security Principles and Practices (21%)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Roles and responsibilities of external organization and agencies
2. Methods for creating effective working relationships

3. Techniques and protocols of liaison
4. Local and national public/private partnerships

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

Knowledge of

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

DOMAIN TWO

Business Principles and Practices (13%)

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

Knowledge of

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

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

Knowledge of

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 programs, education, and training)

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

Knowledge of

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

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

Knowledge of

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

Task 6: Provide advice and assistance to management and others in developing performance requirements and contractual terms for security vendors/suppliers

Knowledge of

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

DOMAIN THREE

Investigations (10%)

Task 1: Identify, develop, implement, and manage investigative functions

Knowledge of

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

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

Knowledge of

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

Task 3: Manage or conduct surveillance processes

Knowledge of

1. Surveillance techniques
2. Technology/equipment and personnel to conduct surveillance
3. Laws pertaining to managing surveillance processes

Task 4: Manage and conduct investigations requiring specialized tools, techniques, and resources

Knowledge of

1. Techniques, tools, and resources related to:
    - financial and fraud related crimes
    - intellectual property and industrial espionage crimes
    - arson and property crimes
    - cybercrimes

Task 5: Manage or conduct investigative interviews

Knowledge of

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

Task 6: Provide coordination, assistance, and evidence such as documentation and testimony to support legal counsel in actual or potential criminal and/or civil proceedings

Knowledge of

1. Statutes, regulations and case law governing or affecting the security industry and the protection of people, property, and information
2. Criminal law and procedures
3. Civil law and procedures

4. Employment law (e.g., wrongful termination, discrimination and harassment)

DOMAIN FOUR

Personnel Security (12%)

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

Knowledge of

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

Task 2: Develop, implement, manage, and evaluate policies, procedures, programs, and methods to protect individuals in the workplace against human threats (e.g., harassment, violence)

Knowledge of

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

Task 3: Develop, implement, and manage executive protection programs

Knowledge of

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

DOMAIN FIVE

Physical Security (25%)

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

Knowledge of

1. Security protection equipment and personnel
2. Survey techniques

3. Building plans, drawings, and schematics
4. Risk assessment techniques
5. Gap analysis

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

Knowledge of

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

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

Knowledge of

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

DOMAIN SIX

Information Security (9%)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Elements of information asset protection including confidentiality, integrity, availability, authentication, accountability, and auditability of sensitive information and associated information technology resources, assets and investigations
2. Information security theory and systems methodology
3. Multi-factor authentication techniques
4. Threats and vulnerabilities assessment and mitigation
5. Ethical hacking and penetration testing techniques and practices
6. Encryption and data masking techniques
7. Systems integration techniques
8. Cost-benefit analysis methodology
9. Project management techniques
10. Budget development process
11. Vendor evaluation and selection process
12. Final acceptance and testing procedures, information systems, assessment, and security program documentation
13. Protection technology, investigations, and procedures
14. Training and awareness methodologies and procedures

DOMAIN SEVEN

Crisis Management (10%)

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

Knowledge of

1. Threats by type, likelihood of occurrence, and consequences
2. “All hazards” approach to assessing threats
3. Cost-benefit analysis

4. Mitigation strategies
5. Risk management and business impact analysis methodology
6. Business Continuity standards (e.g., ISO 22301)

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

Knowledge of

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

Task 3: Respond to and manage an incident

Knowledge of

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

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

Knowledge of

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

Professional Certified Investigator (PCI) Body of Knowledge

DOMAIN ONE

Case Management (35%)

Task 1: Analyze case for applicable ethical conflicts

Knowledge of

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

Task 2: Analyze and assess case elements, strategies and risks

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

Task 5: Identify, evaluate and implement investigative process improvement opportunities

Knowledge of

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

DOMAIN TWO

Investigative Techniques and Procedures (50%)

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

Knowledge of

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

Task 2: Conduct interviews of individuals to obtain relevant information

Knowledge of

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

Task 3: Collect and preserve potential evidentiary materials for assessment and analysis

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

Task 6: Use special investigative techniques to obtain relevant information

Knowledge of

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

DOMAIN THREE

Case Presentation (15%)

Task 1: Prepare report to substantiate investigative findings

Knowledge of

1. Critical elements and format of an investigative report
2. Investigative terminology
3. Logical sequencing of information

Task 2: Prepare and present testimony.

Knowledge of

1. Types of testimony
2. Preparation for testimony

Physical Security Professional (PSP) Body of Knowledge

DOMAIN ONE

Physical Security Assessment (34%)

Task 1: Develop a physical security assessment plan

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

DOMAIN TWO

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

Task 1: Establish security program performance requirements

Knowledge of

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

Task 2: Determine appropriate physical security measures

Knowledge of

1. Structural security measures (e.g., barriers, lighting, locks, blast migration, ballistic protection)
2. Crime prevention through environmental design (CPTED) concepts
3. Electronic security systems (e.g., access control, video surveillance, intrusion detection)
4. Security staffing (e.g., officers, technicians, management)
5. Personnel, package, and vehicle screening
6. Emergency notification systems
7. Principles of data storage and management
8. Principles of network infrastructure and network security
9. Security audio communications (e.g., radio, telephone, intercom, IP audio)
10. Systems monitoring and display (control centers/consoles)
11. Systems redundancy alternative power sources (e.g., battery, UPS, generators, surge protection)
12. Signal and data transmission methods
13. Considerations regarding Personally Identifiable Information (physical/logical/biometric)
14. Visitor management systems and circulation control

Task 3: Design physical system and prepare construction and procurement documentation

Knowledge of

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

DOMAIN THREE

Implementation of Physical Security Measures (32%)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Maintenance inspection techniques
2. Test and acceptance criteria
3. Warranty types
4. Ongoing maintenance, inspections, and upgrade
5. Ongoing training requirements
6. Systems disposal and replacement processes

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

Knowledge of

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

PREFERRED CPE PROVIDER PROGRAM

APPENDIX C: GENERAL RESOURCES

ASIS International Recertification Guide

Sample Certificate of Attendance