ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS INTERNATIONAL
BOARD RECERTIFICATION

asisonline.org/certification/recertification

CPP® Certified Protection Professional
Board Certified in Security Management

PCI® Professional Certified Investigator
Board Certified, ASIS International

PSP® Physical Security Professional
Board Certified, ASIS International

APP Associate Protection Professional
Board Certified in Security Management Fundamentals

ASIS INTERNATIONAL CONTACT INFORMATION

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

EMAIL: certification@asisonline.org

PHONE: +1 703.519.6200

WEBSITE: *asisonline.org*

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

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

This Guide includes the policies and procedures related to the recertification of your ASIS designation(s). It is your responsibility to be aware of the processes and procedures explained in this Guide, and to meet all required deadlines. This updated version of the ASIS Recertification Guide was released on December 1, 2018 and supersedes all previous versions.

IMPORTANT: ASIS CONTACTS YOU MAINLY VIA EMAIL. IF YOUR INFORMATION CHANGES, PLEASE BE SURE TO UPDATE YOUR ASIS ONLINE RECORDS AS SOON AS POSSIBLE.

Contents

ASIS International Certification Program

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

By earning a CPP®, PCI®, PSP®, or APP your employer, clients, and colleagues recognize that you have the knowledge and skills to be a successful security professional. Earning an ASIS certification is a milestone accomplishment that will help you reach your career goals. Once certified, you are required to recertify your designation through continuing education activities **every three years**.

Why Recertify?

Recertifying your ASIS designation every three years demonstrates that you have made a commitment to stay informed about the current practices and emerging trends in the security industry.

When Do I Recertify?

Your designation must be recertified every three years. Your end date is printed on your certificate and can also be found on your online profile.

Recertification Renewal Cycle

In 2018, ASIS announced updates to the recertification renewal cycle. Those who passed the certification exam prior to 2018 will need to recertify their designation on 31 December every three years. For example, if you passed the exam on 30 April 2017, your recertification application is due on 31 December 2020.

Those who pass the exam in 2018 and beyond will have their three-year certification cycle begin at the time of notification of passing the certification examination and end three years later at the end of the month.

For example, a certificant who achieves certification on 14 April 2018 would be due to recertify by 30 April 2021. The subsequent recertification dates would begin on 1 May 2021 and end three years later on 30 May 2024.

Lapsed Certifications – New Policy

(Effective on 1/1/2019 - Lapsed policy changes from one year to three months)
Those whose certification end date was 31 December 2017 have until 31 December 2018 to submit their recertification applications.

- If you submit your recertification CPEs between **1 January 2018 and 30 June 2018,** a total of 64 credits is required to reinstate your designation
- If you submit your recertification CPES between **1 July 2018 and 31 December 2018,** a total of 68 credits is required to reinstate your designation.

Beginning 1 January 2019, all certificants have three months (not one year) after their certification end date to recertify. During this three-month grace period, you will be permitted

to submit your application; however, **all 60 CPEs must be completed in your three-year certification cycle. You cannot use the three-month grace period to accumulate additional CPEs.** A $40 late fee will be applied in addition to the recertification fee, at the time of submission.

Expired Certification

If your recertification application is not submitted by the end of your three-month grace period, your certification will expire, and you will need to apply, take, and pass the exam to be certified again.

Promoting Your Certification

There are many ways to show your colleagues and peers that you have successfully earned your ASIS certification. We provide information on how to display your credential and how to use the ASIS board-certified logos

Digital Badges

Once you have earned your ASIS certification, you will receive an email from ProExam (https://proexamvault.com) with instructions on downloading your digital badge. Digital badges are portable, verifiable, and deter unauthorized reproductions of the CPP, PCI, PSP, and APP designations. For more information on ASIS's digital badges, click here.

Recertification Requirements

You will need to complete **60 Continuing Professional Education (CPE)** activities during your three-year certification cycle to remain certified.

All CPE activities must relate to security/business management, as defined by the body of knowledge of the relevant examination. Certificants must link each submitted activity to an exam Domain. **View the CPP, PCI, PSP, and/or APP Exam Domains.**

Recertification credits are intended for security- or business-related learning, teaching, or service that **are not part of a certificant's regular job duties.** CPEs may be earned in the following categories:

- Membership
- Education
- Instructor
- Author
- Volunteer
- Certification, Standards, and Guidelines Program
- Public Service
- Other Accomplishments

Additional information about each of these categories and the documentation you'll need to report on your recertification application is explained below.

New Recertification Review and Application Process

(Effective 1 February 2018)

In 2018, ASIS launched an updated Certification portal. The portal allows you to load your CPEs as you earn them; however, ASIS staff will no longer review your submitted CPEs until you have submitted your recertification application.

Call or email ASIS if you have any questions about your CPEs. Also, we recommend (but do not require) that you submit additional CPEs if you have them.

Recertifying Before Your End Date

Your recertification application may be submitted anytime in your third year of your certification cycle. Once your CPEs have been reviewed and approved, **your new certification cycle will start where your three-year cycle ended** (i.e., you will not get a new cycle start and end date). All CPEs must be earned during your three-year cycle. If you recertify early in your third year and any of your CPEs are not approved, you will have until the end of your three-year cycle to submit your missing CPEs.

Once your recertification application has been approved, **any CPEs earned after you've recertified but before your new cycle starts will not be carried to your new certification cycle.**

Please note that during your first and second year of your certification cycle, you can use the portal to store, track, and review your CPEs as you can accumulate them.

ASIS-Sponsored CPE Credits

(Effective 1 January 2018)

With the exception of ASIS membership, ASIS volunteer leadership, ASIS Global Access Live, and the Global Security Exchange (GSX), formerly known as the ASIS Annual Seminar, all ASIS-related activities will no longer be uploaded to your online certification account by ASIS. You will receive a certificate of completion or other documentation for all other ASIS-related activities from your ASIS leader. This documentation, which you'll upload into your account, will be guaranteed CPE credit.

For the CPEs that are loaded into your account by an ASIS staff member, please allow 4-6 weeks after the activity has ended for your CPEs to appear in your account.

Chapter/Region Events

Credits for activities at the ASIS Chapter/Region level must be self-reported in your online account. At the Chapter/Region level, there are two options to provide confirmation of CPEs earned for attending a qualifying event. Click here for more information. (Spanish version)

Uploading Your Recertification Activities

ASIS's online CPE reporting system was recently enhanced, enabling you to report CPEs from your profile page in the "My Certifications" quick link. View instructions for uploading your CPEs and submitting your application.

NOTE: The first time you login to your online account, click the "Calculate" button to total up any CPEs that we imported from the previous ASIS database (if you don't see any CPEs after you click "calculate" then your application is up to date).

Supporting Documentation

Supporting documentation for all activities is required (except CPEs loaded into your record by ASIS). All activities must align with at least one of the Domains and Knowledge and Task Statements for the designation you are recertifying. **Your documentation must include proof that you attended the session and a description of the learning objectives of the activity.** Your documentation may include a copy of a certificate/letter of completion and agenda, which includes the hours of classroom attendance completed. All supporting documentation must be in English or Spanish. Any foreign-language submissions must be accompanied with an English translation.

You are only allowed **one upload per activity** you are reporting; therefore, please make one pdf that includes all the following information.

Documents submitted must include:

- Certificant name
- Topic name
- Program sponsor name
- Course description from program sponsor (this will be used to verify that the course is aligned with the designation's Domains)
- Date of attendance or completion (Must be within the 3-year period of certification)
- Number of instructional hours awarded or agenda
- Certificate/letter of completion

(Please see **CPE Categories and Required Documentation** below for specific documentation needed for each credit category.)

Recertification Notifications/Reminders

Your designation must be recertified every three years. Your end date is printed on your certificate and can also be found on your online profile.

ASIS makes every effort to keep you informed about your recertification deadlines. Email notifications will be sent to the primary email address from your online account. **Please make sure to keep your email address current and "whitelist" all emails from asisonline.org to help keep track of recertification reminders.** Ultimately, however, you are responsible for keeping up-to-date on recertification deadlines and submitting the appropriate documentation. **Failure to receive ASIS notifications is not an acceptable reason for missing application deadlines.**

Recertification Fees

ASIS Members: $70

Non-members: $90

Fees must be submitted in U.S. dollars and are subject to change.

During the third year of your certification cycle, you may submit your recertification application at any time. You will be notified by email when your application has been reviewed.

CPE Categories and Required Documentation

Sixty (60) CPEs must be reported for every certification you hold. If you hold more than one ASIS certification, you will need to submit a recertification application for each designation. Note that in some cases, one CPE activity may be submitted for more than one designation provided the course description of the activity aligns with that designation's Domains.

With ASIS's new online application process, you will be required to submit supporting documentation with each CPE reported. See below for acceptable documentation per credit category.

Category 1: Membership Credit

If you are an ASIS International member, 4 CPEs will be loaded in to your online account once a year. You may also report membership in other security-related associations. In your three-year certification cycle, a maximum of 24 CPE credits (4 CPEs per membership per year) may be submitted for individual memberships in:

- Nonprofit professional security or security-related organization or association, and/or
- Nonprofit business management-related organization or association

Corporate memberships are not acceptable.

Required Documentation

- Receipt of paid membership dues that includes years of membership
- Letter from member organization confirming years of membership (must be on the organization's letterhead), and/or
- Copy of membership directory listing including your name and years of membership

Category 2: Educational Credit

Effective 1 July 2018, 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, if you attend a 90-minute session, you would report 1.5 clock hours. If you attended a 45-minute session, you would report 0.75 hours. **Time for meals, breaks, social gatherings, planning sessions, business meetings, and similar activities should not be included.**

CALCULATING CPE HOURS

Educational Activity	Actual Hours
9:00 a.m.– 5:00 p.m.	8
Less: Two 15-minute breaks	0.50
Less: Lunch	1
TOTAL	6.5

Educational credit may be earned for the following activities:

- **Seminar/Conference:** Single and multiple-day programs.
- **Webinars (live or archived)** purchased through ASIS (webinar subscription or single purchase) or webinars sponsored by others. Webinars must be security related and align with one of the Domains of the certification for which you are recertifying. A certificate of completion (ASIS Webinars) or proof of attendance **and** description of session is required.
- **ASIS International Chapter Meetings:** Educational programs must have a formal speaker or facilitator and relate directly to the competencies (Domains) of the applicable certifications
- **Correspondence, Web-Based, and Other Self-Study Courses:** Activities offered through an institution that requires a final examination and where the course sponsor issues a certificate of completion listing instructional hours attained.
- **Accredited College Courses:** Security management or business management-related accredited college courses may be claimed and computed at the rate of seven (7) CPE credits for each semester hour completed. This includes Internet/distance learning and/or other self-study programs that result in accredited college or university credit. **Only 21 CPEs may be claimed per each three-year certification cycle for business management courses.**
- **Exhibits-Only and Exhibitor Participation:** Three (3) CPE credits may be awarded for participation and/or attendance at each security-related exhibit.
- **Archived GSX Educational Sessions:** ASIS accepts a maximum of three (3)CPEs per year for reviewing recordings of GSX educational sessions. Proof of purchase is required, and titles of three sessions viewed must be submitted.
- **GSX Access LIVE!:** Each year, ASIS offers live screenings of selected GSX educational sessions. Those virtually attending GSX Access LIVE! events will receive CPEs.

Required Documentation

- A course description, certificate or letter of completion, and agenda that includes the hours of classroom time

- A transcript showing completion of the college courses
- Badge showing "Exhibit Only" or "Exhibitor"
- For archived webinars: a screen shot of the first and last page of presentation, or letter or certificate of completion.

Category 3: Instructor Credit[1]

The topics of the courses must be relevant to the practice of security or business management (e.g., the Domains for each certification examination). **A maximum of 30 CPEs per certification term.**

CPEs	Instructor Activity
20	Per topic, initial preparation or major modifications of course work for serving as principal instructor or speaker for a security or business management-related course at an accredited college or university
12	Chapter Certification Study Courses: Planning the entire study course including multiple meetings
9	Documented Chapter Certification Study Courses (mentoring a student through the entire study course or fulfilling a specific role in conduct of the course). Only ASIS-approved mentorship programs are allowed.
3	Per participant hour, as an instructor, speaker, or panelist at a security or business management-related educational program

Required Documentation

- Course syllabus to include learning objectives, time, date, and location of course
- Letter from chapter president affirming role of instructor
- A certificate or thank you letter from the sponsor of the program

Category 4: Author Credit

The topics must be relevant to the practice of security or business management (e.g., the Domains for each certification examination).

[1] Except as noted, CPEs cannot be accrued for instructor activities for which participation is inherently part of the participant's job and/or assigned duties. Participation must be voluntary in nature.

CPEs	Authored Articles and Publications (Unlimited)
45	Per security-related and/or business management book
9	Per security-related and/or business management article in recognized periodical
9	Per monograph, booklet, or contribution of chapter to book on security-related and/or business management topics
3	Acceptance by the ASIS Leadership and Management Practices Council for each case study submission
3	Each book review published in recognized periodical
1-2	Per translation of an article related to any security Domain that was originally and/or subsequently published in Security Management magazine or other security-related publication.[2]

Required Documentation

- Copy of the article to include name, date of publication, and author byline
- Letter from publisher (on letterhead) attesting to contribution

Category 5: Volunteer Service

CPEs (credits per year)	Volunteer Activities (a maximum of 30 CPEs per three-year certification cycle)
30	Member of an Executive Committee of a chartered security-related organization or association
25	Member of a national or international Board of Directors of a chartered security-related organization and President of the ASIS International PCB

[2] No credit will be given for paid translation of articles. One CPE awarded for articles up to 1,000 words and two CPEs awarded for articles greater than 1,000 words. A maximum of four CPEs may be awarded per year, with a maximum of 12 CPEs per three-year recertification cycle. To receive credits, certificant must submit a copy of the original article, along with a copy of the translated published article. Both copies must clearly indicate the publication and date. To receive credit for a translation, the certificant must be named in or credited with the translation. If not, certificant must submit written verification from the publisher that the certificant was responsible for the translation.

21	Member of a Certification Board, on a national level, of a chartered security-related organization or association
18	Service as a Senior Regional Vice President or Council Vice President of a chartered security-related organization or association
15	Service as a Regional Vice President, Council Chairman, or Vice Chairman, or ASIS Standards & Guidelines Commission of a chartered security-related organization or association
12	Service as a Council Member, GSX Host Committee Chairman, or Assistant Regional Vice President of a chartered security-related organization or association Service as a duly elected or appointed Chairman, Vice Chairman, Secretary or Treasurer, on the local level, of a chartered security-related organization or association
9	Service as Host Committee member for an annual or other major conference of a chartered security-related organization or association Service as a Committee Chairman, on the local level, of a chartered security-related organization or association
4	Service as a Committee member, on the local level, of a chartered security-related organization or association

Required Documentation

- Letter from organization attesting to volunteer role and dates of service.

Category 6: Certification, Standards & Guidelines Program Service

CPEs (credits per year)	Certification and ASIS Standards & Guidelines (S&G) Activities
15	Per occurrence, Item Development Group (IDG) or role delineation (job analysis) preparation
12	Per occurrence, Pass Point or Standard Setting study

5	Per occurrence, evaluation of ASIS International Annual GSX Call for Presentations or completion of a role delineation questionnaire (job analysis)
2/meeting	Per occurrence, ASIS Standards and Guidelines Technical Committee members; attendance/participation is mandatory
1/meeting	Per occurrence, ASIS Standards and Guidelines Working Group members; attendance/participation is mandatory.

Required Documentation

- Letter from organization attesting to your volunteer role and dates of service.

Category 7: Public Service

At the discretion of the PCB, activities related to security or business management fields, as described in the Domains of each examination, may be eligible for credits. Eligible activities may include those for a charitable, religious, governmental and/or community entity that is performed pro-bono. Examples are security audits of public school buildings; security plan for fundraising event or other large activity; or evaluation of emergency management for a public agency. The PCB will determine points to be awarded based on scope of activity, value to recipient, accomplishments vis-à-vis objectives, and time spent.

Required Documentation:

- Letter from the organization attesting to your public service role, dates of service, hours spent, a brief description of pro-bono service provided, and number of credits requested

Category 8: Other Accomplishments

At the discretion of the PCB, special activities related to security or business management fields as described in the Domains of each examination may be eligible for credits. The PCB will determine points to be awarded based on scope of activity and other relevant factors.

Required Documentation

- Letter to the PCB attesting to your special activity, dates of activity, and number of credits requested

Appealing a Declined Application

Appeals will be considered within 30 days of a certificant's recertification application or CPE activity denial, with day one being the date of the applicant's notification email. Please follow these instructions when filing an appeal:

- Appeals should be sent by mail or email to the Professional Certification Board (PCB) Certificant Relations Committee, address below. If sent by mail, ASIS suggests using a traceable delivery method (e.g., certified or express mail).
- Appeals must identify the adverse decision and state the reasons for the appeal. Also, any new or additional information for consideration should be submitted with the appeal.

Appeals should be sent to:

PCB Certificant Relations Committee

c/o ASIS International

1625 Prince Street

Alexandria, VA 22314

Attn: Certification Department

certification@asisonline.org

PCB Certificant Relations Committee Appeal Process

The PCB Certificant Relations Committee will evaluate and consider a properly filed appeal via teleconference or during one of its meetings.

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

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

The PCB decision is final.

Lifetime Certification (Retired)

ASIS offers lifetime certification to certificants who:

- Hold a CPP, PCI, or PSP in good standing (e.g., not lapsed or expired)
- Have maintained a single certification for 12 consecutive years preceding the date of application
- Have retired (defined as complete cessation from any security-related employment or practice or representation of any such employment or practice) and have no legal, financial, or business interest with any form of security-related employment or practice, as defined by the applicable certification exam Domain

- Have paid the recertification fee for the current term

If a lifetime certificant returns to professional practice after the end of the last term of their regular certification, they must submit a recertification application demonstrating the successful completion of sixty (60) CPEs within the previous three-year period, or they must retake and 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.

To apply for lifetime certification, please contact the Certification Department at certification@asisonline.org.

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

Per ANSI ISO 17024 Standards, ASIS reserves the right to revoke your Lifetime Certification should it be discovered that you are no longer retired. If your Lifetime Certification is revoked, you will be required to return your Lifetime certificate.

Become an ASIS Volunteer

ASIS relies on volunteers for all aspects of its certification programs (e.g. exam development, score setting, job analysis). All aspects of the CPP, PCI, PSP, and APP are created and then maintained by the dedicated professionals who provide their expertise and time to ensure our programs reflect the knowledge and skills needed to be a security management professional.

To become a volunteer, you must:

- Be ASIS-certified
- Agree to abide by the ASIS Code of Professional Responsibility
- Sign a Do Not Disclose contract
- Not participate, coordinate, host, or teach an ASIS certification review or prep class, and agree not to for at least two years after your volunteer assignment is complete
- Agree not to apply for or take an ASIS certification exam for at least two years after your volunteer assignment is complete

ASIS periodically recruits volunteers to:

- Write or review exam questions
- Sit on a job analysis study panel
- Sit on a standards-setting panel
- Lend their expertise on special projects

All those chosen to be volunteers for the ASIS certification program will receive CPEs for their involvement.

If you are interested in becoming a volunteer, please contact certification@asisonline.org

Professional Code of Conduct

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

- Perform professional duties in accordance with the law and the highest moral principles. Noncompliance includes any acts or omissions amounting to unprofessional conduct and deemed prejudicial to the certification
- Observe the precepts of truthfulness, honesty, and integrity
- Be faithful, competent, and diligent in discharging their professional duties
- Safeguard confidential and privileged information and exercise due care to prevent its improper disclosure
- Not maliciously injure the professional reputation or practice of colleagues, clients, or employees

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

- Providing false or misleading statements or information when applying to take the certification examination or to recertify
- Any act or omission that violates the provisions of the ASIS Certification Code of Professional Responsibility
- Any act that violates the criminal or civil laws of any jurisdiction
- Any act that is the proper basis for suspension or revocation of a professional license
- Any act or omission that violates the PCB Disciplinary Rules and Procedures.
- Failure to cooperate with the PCB 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 ANSI ISO 17024 Standards, if your ASIS Certification is revoked, you will be required to return your certificate.

Filing A Complaint

Complaints regarding the eligibility requirements, test scheduling, policies, and procedures of the ASIS certification program, certification personnel, or another certificant may be filed in writing to the Certification Director within 90 days of the incident's occurrence. Please submit your complaint in writing and mail or email to certification@asisonline.org. Complaints made anonymously will not be reviewed.

Please provide sufficient objective evidence to substantiate the complaint. All complaints will be reviewed by the Certification Director and/or members of the PCB Certificant Relations Committee. Receipt of your complaint will be sent to you and will include actions taken by ASIS

to remedy the situation. When the complaint has been resolved, the person filing the complaint will be notified with the results of the review.

ASIS Certificates

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

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
- Affecting adversely 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.

About 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 members are ASIS certified.

Members 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 Board of Directors. Members of the PCB are chosen through a nomination process. The board meets three times per year.

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
1. Local, national, and international public/private partnerships
2. Methods for creating effective working relationships

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

Knowledge of

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

TASK 5: Implement and/or coordinate an investigative program

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Risk mitigation techniques (e.g., technology, personnel, process, facility design, infrastructure)

2. Physical security protection equipment, technology, and personnel
3. Security survey techniques

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

Knowledge of

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

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

Knowledge of

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

DOMAIN TWO
Business Operations (22%)

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

Knowledge of

1. Data analysis techniques and cost-benefit analysis
2. Principles of business management accounting, control, and audits
3. Return on Investment (ROI) analysis
4. Fundamental business finance principles and financial reporting
5. Budget planning process
6. Required components of effective documentation (e.g., budget, balance sheet, vendor work order, contracts)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Interpersonal communications and feedback techniques
2. Relevant laws and regulations
3. Governance and compliance standards
4. Generally accepted ethical principles
5. Guidelines for individual and corporate behavior

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

Knowledge of

1. Confidential information protection techniques and methods
2. Relevant laws and regulations
3. Key concepts in the preparation of requests for proposals and bid reviews/evaluations
4. Service Level Agreements (SLA) definition, measurement and reporting
5. Contract law, indemnification, and liability insurance principles
6. Monitoring processes to ensure that organizational needs and contractual requirements are being met
7. Vendor qualification and selection process

DOMAIN THREE

Risk Management (25%)

TASK 1: Conduct initial and ongoing risk assessment processes

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

DOMAIN FOUR
Response Management (18%)

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

Knowledge of

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

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

Knowledge of

1. Recovery assistance resources

2. Mitigation opportunities during response and recovery processes

TASK 3: Conduct a post-incident review

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

TASK 8: Coordinate with emergency services during incident response

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Communication techniques and protocols of liaison

2. Communication techniques and notification protocols

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

Knowledge of

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

Certified Protection Professional (CPP) 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

6. Principles and techniques of policy/procedures development
7. Communication strategies, methods, and techniques
8. Training strategies, methods, and techniques
9. Cross-functional collaboration
10. Relevant laws and regulations

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

Knowledge of

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

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

Knowledge of

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

9. Talent management and succession planning

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

Knowledge of

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

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

Knowledge of

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

DOMAIN THREE

Investigations (10%)

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

Knowledge of

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

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

Knowledge of

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

TASK 3: Manage or conduct surveillance processes.

Knowledge of

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

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

Knowledge of

1. Financial and fraud related crimes
2. Intellectual property and industrial espionage crimes
3. Arson and property crimes
4. Cybercrimes

TASK 5: Manage or conduct investigative interviews.

Knowledge of

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

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

Knowledge of

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

DOMAIN FOUR

Personnel Security (12%)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

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

DOMAIN FIVE

Physical Security (25%)

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

Knowledge of

1. Security protection equipment and personnel
2. Survey techniques
3. Building plans, drawings, and schematics
4. Risk assessment techniques
5. Gap analysis

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

Knowledge of

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

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

Knowledge of

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

DOMAIN SIX

Information Security (9%)

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

Knowledge of

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

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

Knowledge of

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

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

Knowledge of

1. Elements of information asset protection including confidentiality, integrity, and availability, authentication, accountability, and audit ability of sensitive information; and associated information technology resources, assets, and investigations
2. Information security theory and systems methodology
3. Multi-factor authentication techniques
4. Threats and vulnerabilities assessment and mitigation
5. Ethical hacking and penetration testing techniques and practices

6. Encryption and data masking techniques
7. Systems integration techniques
8. Cost-benefit analysis methodology
9. Project management techniques
10. Budget development process
11. Vendor evaluation and selection process
12. Final acceptance and testing procedures, information systems, assessment, and security program documentation
13. Protection technology, investigations, and procedures
14. Training and awareness methodologies and procedures

DOMAIN SEVEN

Crisis Management (10%)

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

Knowledge of

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

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

Knowledge of

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

TASK 3: Respond to and manage an incident.

Knowledge of

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

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

Knowledge of

1. Resource management techniques

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

Professional Certified Investigator 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
2. report
3. Investigative terminology
4. Logical sequencing of information

TASK 2: Prepare and present testimony.

Knowledge of

1. Types of testimony
2. Preparation for testimony

Physical Security Professional 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 (punchlists)
5. Systems configuration management
6. Final acceptance testing criteria
7. End-user training requirements

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

Knowledge of

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

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

Knowledge of

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