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 version of the ASIS Recertification Guide was updated on 20 February 2024 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**.

## THE SAFETY ACT DESIGNATION

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

## 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 displayed on your certificate, on your ASIS online profile, and can also be found on your Credly Account.**

## Recertification Renewal Cycle

The recertification term (also called "certification cycle") is the three-year cycle between passing the CPP®, PCI®, PSP®, or APP® examination, and the deadline for submitting sufficient continuing education credits and payment to recertify. For example, if you passed the exam on 15 April 2022, your recertification application is due on 30 April 2025.

## Lapsed Certifications

All certificants have three months 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 have been completed in your three-year certification cycle. You cannot use the three-month grace period to accumulate additional CPEs.**

## 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.

## ASIS Certificates

All certificates related to the CPP, PCI, PSP, and/or APP designations are the sole property of ASIS International. ASIS reserves the right to request that those with a suspended and revoked

certification return their certificate to ASIS. The formerly certified individual must immediately cease using the ASIS International designations and remove them from all printed, electronic, or other forms of communications.

### 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 and Certificate

Once you have earned your ASIS certification, you will receive an email from Credly (https://info.credly.com) with instructions on downloading your digital badge and certificate. ASIS certificates are now downloadable in pdf format through your digital badge. Digital badges are portable, verifiable, and deter unauthorized reproductions of the CPP, PCI, PSP, and APP designations.

Your digital badge will be connected to the email address you submit to ASIS at the time of your application. If you are using a company email address and change companies, be sure to update your email address in your Credly account BEFORE you no longer have access to the original email address. If you need assistance after changing companies, please contact the ASIS Certification Team for assistance.

## 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 be completed during your three-year certification cycle and 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 or company-specific training.** CPEs may be earned in the following categories:

- Membership (Max. 24 CPEs)
- Education
- Instructor (Max. 30 CPEs)
- Author
- Volunteer (Max. 30 CPEs)
- 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.

# Online Recertification Review and Application Process

All recertification CPEs and related documents must be stored and submitted using your online ASIS portal. The portal allows you to load your CPEs as you earn them; however, ASIS staff will not review your submitted CPEs until you have submitted your recertification application. **Your activities will show as "pending" until you have submitted your application.** View instructions for uploading credits and submitting your application.

Although ASIS cannot pre-approve your CPEs, our staff is happy to help you decide if an activity counts for CPE credit. Please just 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.

## Your Application Review

**Your recertification is not complete when you submit your recertification application.** ASIS will review your application (please allow 2-3 weeks for review to be completed). When we've completed the review, you will receive an email notification from ASIS that your application has been approved or we need additional information before your recertification can be approved. If you need to submit more information, that will be explained in the email. **Please contact ASIS if you have not received an email after three weeks have passed since your application has been submitted.**

## 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 cannot be carried to your new certification cycle.**

**Please note that during your first and second year of your 3-year certification cycle, you can use the portal to store, track, and review your CPEs as you can accumulate them.**

## ASIS Membership Advantages

You do not have to be an ASIS member to recertify your designation but there are plenty of recertification advantages if you are! Membership alone will earn you four CPEs per year for a total of 12 CPEs during your three-year cycle. ASIS Chapter and Council Leadership roles, volunteer work at ASIS, members-only webinars, and more will help you reach your recertification goals and member discounts will apply.

## ASIS-Sponsored CPE Credits

ASIS will upload most of your ASIS-related CPEs into your online account. Those CPEs include ASIS membership, ASIS volunteer leadership, the Global Security Exchange (GSX), online courses, and our live and on-demand webinars (free for ASIS members). For some ASIS activities, you will need to self-report your participation with a letter or certificate of completion (such as special

volunteer work) 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. For ASIS webinars, your participation will upload no more than 48 hours after the webinar.**

### ASIS 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 allows you to report CPEs from your profile page in the "My Certifications" quick link. View instructions for uploading your CPEs and submitting your application.

### 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.

At least one document **must** be loaded for each self-reported CPE and the system allows up to three uploads for each entry.

**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 certification cycle)
- 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 displayed 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 certification@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.**

## Extension Policies

ASIS does not grant extensions due to job demands, company budgets, employment status, personal finances, changes in marital status, changes in mailing address, and other personal or professional reasons. Extensions may be granted if there is a severe hardship such as a major medical emergency in the immediate family, a natural disaster, if on active military duty and deployed into a remote or hazardous area, or in certain circumstances, such as childbirth, adoption, or acceptance of a child in foster care. The applicant or certificant is required to provide documentation of extenuating circumstances (e.g., doctor's note or other appropriate proof of circumstance). Military personnel will need to verify their deployment status by submitting a copy of official deployment orders. This does not apply to individuals who are military contractors. Severe hardship must be documented and verifiable. ASIS certification candidates and certificants who wish to utilize an extension should contact the ASIS certification team no later than 60 days before eligibility end date or certification end date. Certificant extensions will only be considered if at time of extension application, the certificant has completed 50% or more of the required CPE credits for their current certification cycle. Recertification use case example:

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

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

## Recertification Fees

Recertification fees are outlined below. The ASIS Board has also approved special fees for those individuals who live in Emerging Markets, as identified by the World Bank. **Fees are not refundable.**

View the list of countries identified as Emerging Markets by the World Bank.

**ASIS Members: $170 (Emerging Market 1: $130; Emerging Market 2: $120)**

**Non-members: $210 (Emerging Market 1: $160; Emerging Market 2: $150)**

Recertification applications submitted during the *three-month grace period* will be subject to the recertification late fees as listed below.

**ASIS Members: $250 (Emerging Market 1: $190; Emerging Market 2: $175)**

**Non-members: $290 (Emerging Market 1: $220; Emerging Market 2: $205)**

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. Fees must be submitted in U.S. dollars and are subject to change. **Fees are not refundable.**

## 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 each designation's domains and completed within your 3-year certification cycle.

**You are required to submit supporting documentation with each CPE self-reported.** See below for acceptable documentation per credit category.

### Category 1: Membership Credit (Max. 24 CPEs)

If you are an ASIS International member, 4 CPEs will be loaded into your online account once a year (usually in July or August). 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. Membership credit for ASIS Chapter memberships is not acceptable.

**Required Documentation**

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

### Category 2: Educational Credit

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 will report 1.5 clock hours. If you attended a 45-minute session, you will report 0.75 hours. **Time for meals, breaks, social gatherings, planning sessions, business meetings, and similar activities should not be included.**

**CALCULATING CPE HOURS (EXAMPLE)**

| Educational Activity | Actual Hours |
|---|---|
| 9:00 a.m.– 5:00 p.m. | 8.00 |
| **Less:** Two 15-minute breaks | 0.50 |
| **Less:** Lunch | 1.00 |
| TOTAL | 6.50 |

Educational credit may be earned for the following activities:

- **Seminar/Conference:** Single and multiple-day programs.
- **Webinars (live or on-demand)**: Webinars must be security related and align with one of the Domains of the certification for which you are recertifying. A certificate of completion or proof of attendance **and** description of session is required.

  **Note**: ASIS allows **members free access to all webinars** – both live and on-demand (nonmember must pay a fee). ASIS-sponsored webinars will be uploaded into your ASIS online account.
- **Other security-related certifications:** If you have earned a security or business certification from another organization that maps to your certification's Body of Knowledge, you may earn up to 20 CPEs provided you earned the certification during your three-year certification cycle. CPEs may only be earned for the initial certification earned, not recertifications.
- **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 each 3-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.
- **"Best of GSX" bundles:** ASIS offers topic-specific packages of selected GSX sessions. Credits will be awarded based on bundle length.
- **Safety-Related Programs:** Attending single and multiple-day seminars and conferences may be claimed. **A total of 21 CPEs may be claimed each 3-year certification cycle for safety-related programs and/or instruction.**

**Required Documentation**

- A course description, certificate or letter of completion, and agenda that includes the hours of classroom or conference time
- A transcript showing completion of the college courses
- Badge showing "Exhibit Only" or "Exhibitor"
- For archived webinars: a screenshot of the first and last page of presentation, or letter or certificate of completion.

## Category 3: Instructor Credit (Max. 30 CPEs)

The topics of the courses must be relevant to the practice of security, business management, or safety-related programs (e.g., the domains for each certification examination).

| 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. |
| 9 | ASIS Mentor Program – **Mentors** will receive 9 CPEs per year for every active mentorship program. Each program must be at least 6 months in length. |
| 5 | ASIS Mentor Program – **Mentees** may record 5 CPEs per three-year certification cycle. Mentorship topic must align with at least one of the Domains in the certification being recertified. A letter from your mentor, explaining the purpose of the mentorship and how it aligns with the Domains is required. |
| 3 | Per participant hour, as an instructor, speaker, or panelist, at security or business management-related educational program. |

**A total of 21 CPEs may be claimed each 3-year certification cycle for safety-related programs and/or instruction.**

**Required Documentation**

- Copy of on-site program showing your role as speaker or letter from host organization attesting to your instructor role in seminar or conference **and/or**
- Course syllabus to include learning objectives, time, date, and location of course **and/or**
- Letter from chapter president affirming role of instructor **and/or**
- 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).

| 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 | 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.[1] |

**Required Documentation**

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

## Category 5: Volunteer Service (Max. 30 CPEs)

| CPEs (credits per year) | Volunteer Activities |
|---|---|
| 30 | National or international **Executive Committee** member serving on a board of directors of a chartered security-related organization or association (e.g., executive committee members of the ASIS Global Board, CSO, Foundation, PCB, and PSB). |
| 25 | **Member** of a national or international board of directors of a chartered security-related organization or association. (e.g., ASIS Global Board |

[1] 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.

| | |
|---|---|
| | Directors; Regional Board/Advisory Committee; and Directors of the ASIS CSO, Foundation, PCB, and PSB). |
| 18 | ASIS service as a Senior Regional Vice President or Community Vice President of a chartered security-related organization or association. |
| 15 | ASIS service as a Regional Vice President, Steering Committee Chair or Vice Chair, or Chapter Chair, or similar roles of a chartered security-related organization or association. |
| 12 | ASIS service as Assistant Regional Vice President, Steering Committee Member, Chapter Vice Chair, Secretary or Treasurer, GSX Host Committee Chair, or Awards Committee Chair, or similar service of a chartered security-related organization or association. |
| 9 | ASIS service as GSX Host Committee member or Awards Committee member, Chapter Committee Chair, or similar roles for an annual or other conference of a chartered security-related organization or association. |
| 4 | ASIS service as a Chapter Committee member, or equivalent service with 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 Job Analysis Panel member |
| 12 | Per occurrence, Pass Point or Standard Setting study |
| 5 | Per occurrence, evaluation of ASIS International Annual GSX Call for Presentations |
| 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 (additional information may be requested)

# Recertification by Exam

A current certificant in their third year may recertify by taking the exam (rather than submitting CPEs). To recertify by taking the exam, you must contact the certification department of your intentions. The certification team will need to terminate your current certification for you to submit an exam application. You will be required to follow all the policies regarding submitting an exam application and the appropriate fees.

Remember, if you fail the exam, ASIS cannot reinstate your previous certification status.

If you pass the exam, the start date of your three-year certification cycle will be set to the date on which you passed the exam.

# Appealing a Decision

An appeal procedure is available to any individual who has applied for or received an ASIS certification and wants to contest any adverse decision. This policy applies only to the procedural aspects of the credentialing process. Those areas not subject to appeal are further

identified under the section heading "General Principles Relating to Appeals" at the end of this section. Any individual who does not file a written request for an appeal within the required time limit shall waive the right to appeal. Submitting an appeal will not result in any discriminatory actions against the appellant.

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

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

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

- Appeals must be submitted within 30 days of an applicant receiving notification of an adverse decision, with day one as the date of the applicant's notification email.
- A letter must be submitted explaining actions being appealed to certification@asisonline.org
- Appeals must be sent by mail or email. If sent by mail, ASIS strongly suggests sending by certified or express mail so the package can be traced
- Appeal must be submitted to the PCB Certificant Relations Committee
- Appeals must identify the adverse decision being appealed and state the reasons for the appeal. Any new or additional information for consideration should be included in the letter

**Appeals should be sent to:**

PCB Certificant Relations Committee
certification@asisonline.org

## PCB Certificant Relations Appeal Process

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

## General Principles Relating to Appeals

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

## 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 including the rationale, 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 Committee's decision is final and may not be appealed.**

# Lifetime Designation

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

- The candidate must be a CPP, PCI, PSP, or APP in good standing (e.g., status is "current" and not "lapsed" or "expired").
- The candidate must have held the certification for twelve consecutive years.
- The candidate must be currently retired from any form of security employment/practice, or receiving compensation from same, as defined by the applicable certification exam domain.
- The candidate must have paid the recertification fee for the current term.

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

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

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

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

**To apply for lifetime certification**, please complete and submit this application at certification@asisonline.org. **There is a $100 fee to apply.**

## 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 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 Confidentiality 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

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 complete the respective volunteer survey.

- APP
- CPP
- PCI
- PSP

## Third-Party Intervention

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

Because ASIS certification programs are accredited by ANAB to the ISO 17024 Standard, involving third parties to try to change a decision made by the PCB is against ANAB accreditation requirements and doing so jeopardizes ASIS accreditation status as an international certification body. In addition, ASIS strives to apply our policies consistently in order to be fair to all. Allowing special "rules" to some is simply not fair to the 10,000+ certificants who do follow the policies.

Finally, due to confidentiality requirements, the PCB and the Certification Team can only communicate directly with the certificant; they cannot share information with third parties.

## Filing A Complaint

Complaints regarding the eligibility requirements, test scheduling, policies, and procedures of the ASIS certification program, certification personnel, or another certificant may be filed in writing per the instructions in Section III: Process for filing a complaint. The confidentiality of both the complainer as well as the person to whom the complaint is lodged are protected by ASIS Confidentiality Agreements.

The complaint must contain sufficient objective evidence to substantiate the complaint. All complaints will be reviewed by the Certification Director and/or members of the PCB Certificant Relations Committee.

Whenever possible, ASIS will make progress reports to both the person submitting the complaint and to the person to whom the complaint is lodged. Receipt of the complaint will be sent to the person submitting the complaint and will include actions taken by ASIS to remedy the situation. When the complaint has been resolved, the person filing the complaint will be notified with the results of the review. ASIS's complete complaint policy can be found here.

## 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.

## ASIS Certification Code of Professional Responsibility

(Updated 20 Feb 2024) In addition to the ASIS International Code of Ethics and Code of Conduct, all ASIS board certified security professionals and applicants for certification must adhere to the Code of Professional Responsibility, agreeing to:

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

- Be faithful, competent, and diligent in discharging their professional duties.
- Safeguard confidential and privileged information and exercise due care to prevent its improper disclosure.
- Not maliciously injure the professional reputation or practice of colleagues, clients, or employees.

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

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

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

## Attestation of Continued Eligibility for Certification

**All those applying for recertification of their ASIS certification will sign the following attestation on the application.**

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

I understand that persons who apply for certification as a Certified Protection Professional (CPP), Associate Protection Professional (APP), Professional Certified Investigator (PCI), or Physical Security Professional (PSP) or persons who have been certified by ASIS International, are subject to ASIS International's eligibility requirements for certification, recertification and to the ASIS Certification Code of Professional Responsibility, as required by the ASIS Board Certification Handbook and the Board Recertification Guide. Additionally, examination candidates are not permitted to utilize another individual, company, and/or artificial intelligence (AI) during your examination administration; this includes, but is not limited to, any form of proxy tester, natural language processing, predictive analysis, generative AI, open AI, etc.

I understand that in order to maintain my certification, I must re-certify every three years by reporting a specified number of Continuing Professional Education (CPE) credits, in accordance with ASIS policy and procedures for submitting such reports. I understand that CPE credits may be earned through education programs and courses and other activities, and that all CPEs must conform to the requirements specified in ASIS International's Recertification Guide. I further understand that from time-to-time ASIS International may amend its requirements. Policies, and

procedures to include: initial certification, recertification, and the Code of Professional Responsibility.

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

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

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

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

## Release of Candidate and Certificant Information

Release to third parties of confidential information of ASIS candidates and certificants is prohibited unless ASIS obtains signed permission from the candidate or certificant to do so or ASIS is compelled to do so by law. Consent to release information must include to whom the candidate or certificant information can be released and the information that can be released. Information cannot be released if the law prohibits this release.

## 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 directors are CPP, PCI, PSP, and/or APP certified.

Directors of the PCB manage the certification programs by ensuring that standards are developed and maintained, quality assurance is in place, and the exams accurately reflect the duties and responsibilities of security professionals in the areas of security management, investigations, and physical security. The PCB is a committee of the ASIS Board of Directors. Directors 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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

**TASK 5: Implement and/or coordinate an investigative program.**

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

# DOMAIN TWO

## Business Operations (22%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

1. Communication strategies, methods, and techniques
2. Techniques for quantifying productivity/metrics/key performance indicators (KPI)

3. Project management fundamentals tools and techniques
4. Principles of performance evaluations, 360 reviews, and coaching

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

# DOMAIN THREE

## Risk Management (25%)

**TASK 1: Conduct initial and ongoing risk assessment processes.**

*Knowledge of*

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

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

*Knowledge of*

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

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

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

**TASK 4: Implement and/or coordinate recommended countermeasures for new risk treatment strategies.**
*Knowledge of*

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

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

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

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

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

## DOMAIN FOUR

### Response Management (18%)

**TASK 1: Respond to and manage an incident using best practices.**
*Knowledge of*

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

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

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

**TASK 3: Conduct a post-incident review.**
*Knowledge of*

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

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

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

**TASK 8: Coordinate with emergency services during incident response.**

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

# Certified Protection Professional (CPP) Body of Knowledge

## DOMAIN ONE

### Security Principles and Practices (22%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

1. Training methodologies
2. Communication strategies, techniques, and methods
3. Awareness program objectives and program metrics

4. Elements of a security awareness program (e.g., roles and responsibilities, physical risk, communication risk, privacy)

# DOMAIN TWO

## Business Principles and Practices (15%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

# DOMAIN THREE

## Investigations (9%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

1. Financial and fraud related crimes
2. Intellectual property and espionage crimes
3. Crimes against property (e.g., arson, vandalism, theft, sabotage)
4. Cybercrimes (e.g., distributed denial of service (DDoS), phishing, ransomware)
5. Crimes against persons (e.g., workplace violence, human trafficking, harassment)

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

*Knowledge of*

1. Interview and interrogation techniques
2. Techniques for detecting deception

3. Non-verbal communication and cultural considerations
4. Rights of interviewees
5. Required components of written statements
6. Legal considerations pertaining to managing investigative interviews

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

*Knowledge of*

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

# DOMAIN FOUR

## Personnel Security (11%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

## DOMAIN FIVE

### Physical Security (16%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

## DOMAIN SIX

### Information Security (14%)

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

*Knowledge of*

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

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

*Knowledge of*

1. Principles of information security management
2. Information security theory and terminology

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

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

*Knowledge of*

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

# DOMAIN SEVEN

## Crisis Management (13%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

# Professional Certified Investigator (PCI) Body of Knowledge

In 2022/2023, ASIS conducted a job analysis study to ensure the PCI Body of Knowledge still represents the knowledge and skills needed to be a successful professional investigator. Changes were made and the updated body of knowledge is presented below. Exam questions regarding these updates will start to appear on the exam in early 2024.

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

## DOMAIN ONE

### Professional Responsibility (28%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

1. Resource requirements (e.g., equipment, internal and external liaisons, personnel)

2. Resource allocations (e.g., budget, time)
3. Case management practices (e.g., chain of custody procedures, documentation requirements, case closure)

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

*Knowledge of*

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

# DOMAIN TWO

## Investigative Techniques & Procedures (52%)

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

1. Methods of research using physical, information technology, and operational technology resources

2. Information sources (e.g., databases, digital media, government, open source, proprietary)
3. Methods of analysis of research results
4. Research documentation (e.g., findings)

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

*Knowledge of*

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

**TASK 6: Use investigative techniques.**

*Knowledge of*

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

# DOMAIN THREE

## Case Presentation (20%)

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

*Knowledge of*

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

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

*Knowledge of*

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

# Physical Security Professional (PSP) Body of Knowledge

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

## DOMAIN ONE

### Physical Security Assessment (34%)

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

*Knowledge of*

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

**Task 2: Identify assets to determine their value, 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 for various types of assets and business operations

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

*Knowledge of*

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

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

*Knowledge of*

1. Relevant data and methods for collection (e.g., security survey, interviews, incident reports, crime statistics, personnel issues, issues experienced by other similar organizations)
2. Effectiveness of current security technologies/equipment, personnel, and procedures
3. Interpretation of building plans, drawings, and schematics

4. Applicable standards/regulations/codes and where to find them
5. Environmental factors and conditions (e.g., facility location, architectural barriers, lighting, entrances) that impact physical security)

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

*Knowledge of*

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

# DOMAIN TWO

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

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

*Knowledge of*

1. Design constraints (e.g., regulations, budget, materials, system compatibility)
2. Incorporation of risk analysis results in design
3. Relevant security terminology (e.g., punch list, field test)
4. Relevant security concepts (e.g., CPTED, defense-in-depth, the 4 Ds- deter, detect, delay, deny)
5. Applicable codes, standards, and guidelines
6. Operational requirements (e.g., policies, procedures, staffing)
7. Functional requirements (e.g., system capabilities, features, fault tolerance)
8. Performance requirements (e.g., technical capability, systems design capacities)
9. Success metrics

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

*Knowledge of*

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

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

*Knowledge of*

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

# DOMAIN THREE

## Implementation of Physical Security Measures [31%]

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

*Knowledge of*

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

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

*Knowledge of*

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

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

*Knowledge of*

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

**Task 4: Develop requirements for personnel involved in support of the security program.**

*Knowledge of*

1. Roles, responsibilities, and limitations of security personnel (including proprietary [in-house] and contract security staff)
2. Human resource management (e.g., establishing KPIs, performance review, improvement processes, recruiting, onboarding, progressive discipline)
1. Security personnel professional development (e.g., training, certification)
2. General, post, and special orders
3. Security personnel uniforms and equipment
4. Security awareness training and education for non-security personnel

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

*Knowledge of*

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