PROFESSIONAL CERTIFIED INVESTIGATOR (PCI®)

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

Earning a PCI provides objective evidence of an advanced level of investigative knowledge and skills, including, not limited to, validating your ability to collect information through the effective use of surveillance, interviews, and interrogations.

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

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

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.

PCI Eligibility Requirements

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

WORK EXPERIENCE

Without higher education degree:
Five (5) years of investigations experience (or four years if you already hold an APP), including at least two years in case management*

With a higher education degree:

Master's Degree or international equivalent from an accredited institution of higher education and have three (3) years of investigations experience, including at least two years in case management*
OR
Bachelor's Degree or international equivalent from an accredited institution of higher education and have four (4) years of investigations experience (or three years if you already hold an APP), including at least two years in case management*

*Case Management is defined as the coordination and direction of an investigation using various disciplines and resources, the finding of which would be assessed to establish the facts/findings of the investigation as a whole, the management process of investigation.

PCI Exam Contents

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

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

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