

PROFESSIONAL CERTIFIED INVESTIGATOR (PCI®)

The Professional Certified Investigator (PCI) credential provides demonstrable proof of knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings.

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

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 approximately 140 multiple-choice questions: 125 “live,” scoreable questions and up to 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: CASE MANAGEMENT (35%)

Task 1: Analyze case for applicable ethical conflicts.

Knowledge of:

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

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

Knowledge of:

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

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

Knowledge of:

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

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

Knowledge of:

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

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

Knowledge of:

1. Internal review (e.g., management, legal, human resources)
2. External review (e.g., regulatory bodies, accreditation agency)

3. Liaison resources
4. Root cause analysis and process improvement techniques

DOMAIN TWO: INVESTIGATIVE TECHNIQUES AND PROCEDURES (50%)

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

Knowledge of:

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

Task 2: Conduct interviews of individuals to obtain relevant information.

Knowledge of:

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

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

Knowledge of:

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

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

Knowledge of:

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

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

Knowledge of:

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

Task 6: Use special investigative techniques to obtain relevant information.

Knowledge of:

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

DOMAIN THREE: CASE PRESENTATION (15%)

Task 1: Prepare report to substantiate investigative findings.

Knowledge of:

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

Task 2: Prepare and present testimony

Knowledge of:

1. Types of testimony
2. Preparation for testimony