



Professional Accreditation Program

Accredited Security Professional (ASP)

Program Administration and Guidelines

Copyright©2000 by The Canadian Society for Industrial Security, Inc. (CSIS, Inc.)

All rights reserved. No part of this publication may be produced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, now known or to be invented, without permission from the publisher.

License and Certain Restrictions: You are granted a limited non-exclusive license to use a copy of the enclosed Program.

It is prohibited to give copies to another person. You may copy the printed material, and the documentation is protected by Canadian and other copyright laws and international treaties. You may not modify, adapt, translate, rent, sublicense, assign, loan, resell for profit, distribute, or network the program or create derivative works based upon the related documentation and materials, or any part thereof. You may not transfer to a third party, or sell the program to a third party.

3rd edition published in 2000 by CSIS, Inc.

P.O. Box 57006, Jackson Station,

2 King Street West,

Hamilton ON

L8P 4W9

Toll free: 1-800-461-7748

Local: (905) 853-6523

Fax: (905) 972-0404

E-mail: inquiries@csis-scsi.org

TABLE OF CONTENTS

Forward	3
Chapter 1	Program Administration4
	Professional Accreditation Board4
	Program outline and requirements4
	Application to the program4
	Fee4
	Withdrawal from the program.....5
	Revocation of ASP status for cause5
	Appeal procedures.....5
	Recognition process5
	Responsibilities of the Accredited Security Professional5
Chapter 2	Competencies6
	Guide to preparing competency statements6
	List of competencies7
Chapter 3	The Verification Process25
	Introduction.....25
	Verification team.....25
	Protocol25
	Proprietary or sensitive information.....26
	Procedure26
Chapter 4	Study Paper27
	Requirement27
Annex A – Application Information and Form	27

Forward

Professional competence is a personal achievement. It is distinct from, but essential to, the skill and knowledge that make up a discipline or profession. The modern security discipline consists of nine principal competencies each comprising skill and knowledge, ability, experience and performance. In all professions the establishment, maintenance and evolution of fundamental competencies gives stability to the discipline and confidence to its practitioners and to their clients. These characteristics of a profession are key to an accreditation program.

CHAPTER 1

PROGRAM ADMINISTRATION

Professional Accreditation Board

The Professional Accreditation Board (PAB) is responsible to the Board of Directors for the administration of the Accredited Security Professional (ASP) program. The PAB rules on the acceptability or unacceptability of candidates. The PAB consists of a chairperson and one member.

Program outline and requirements

The ASP program requires a candidate to formally apply for admission into the program. Once accepted into the program the candidate is required to prepare and submit detailed competency statements based on the ASP competencies criteria, and to prepare and submit a study paper. Finally, the candidate is required to undergo an on-site workplace verification of the material submitted to the PAB.

A potential applicant must have a specialist (or superior) level of competency in any five of the nine competencies listed below. There is a further requirement to have a standard level of working knowledge in the remaining four competencies. Security practitioners who believe they meet this standard are eligible for, and encouraged to, apply for entry into the ASP program. The nine professional security competencies are:

Administration/Physical security/Human resource security/Information and asset security
Legal aspects of security /Investigation/Emergency planning/Employee relations/
Information technology security

Application to the program

The potential candidate is required to submit an application (Annex A) to the PAB through the Head Office of CSIS, Inc. seeking permission to enter the ASP program. The application should be accompanied by a curriculum vita. The application will be examined to determine if the basic requirements exist to be successful in the program. For example, the application will be scrutinized for evidence of extensive experience in supervision and training and management of security programs represented by the competencies, together with confirmation that the candidate is a security practitioner.

Should these prerequisites not exist; the person will be notified with the reasons for non-acceptance. The response may also include recommendations for additional training and experience to encourage a subsequent application for entry to the ASP program.

Fee

The fee for entry into the ASP program is \$595 which includes the Harmonized Sales Tax (HST).

Withdrawal from the program

Upon being accepted into the ASP program a candidate may withdraw from the program at any time. Upon official notification of withdrawal before the verification step (see Chapter 3) four hundred and fifty dollars will be refunded. One hundred dollars will be retained to cover administrative costs. After the verification step, if a candidate is not successful in the program a refund is not made. All materials submitted by the candidate will be returned upon request.

Revocation of ASP status for cause

The Society reserves the right to withdraw ASP status from an accredited security practitioner for cause. The Society normally deems "cause" to mean a serious breach of the Society's Code of Ethics, or other unacceptable professional or personal behavior or conduct which seriously and negatively affects the purpose, objectives, mandate, operations or reputation of the Society and its members.

Appeal procedures

If the PAB does not grant accreditation, the candidate may appeal to the PAB. Should the candidate disagree with the response to the appeal a further appeal may be directed to the Board of Directors for a final decision. The Board of Directors may ask the President's Advisory Council to review the matter and make recommendations to the Board of Directors.

Recognition process

The ASP designation is for life. No further requirements exist.

The certificate of ASP status will be presented to the successful candidate at a mutually acceptable and suitable ceremony. Normally, the Society awards such certificates at the Society's annual conference. Also, the President of the Society will forward a letter of achievement to the candidate's immediate supervisor or other person if requested. In addition, media coverage or articles recognizing the award of ASP status may be placed in the Society's national publication.

Responsibilities of the Accredited Security Professional

ASP status imposes the following professional obligations:

- ◆ Encouraging other suitable security practitioners to prepare for and enter the program.
- ◆ Serving as a member of a verification team.
- ◆ Maintaining credibility in the ASP status by remaining up-to-date in professional knowledge and expertise.
- ◆ Offering personal support and encouragement to fellow colleagues in matters of professional activity and development.

CHAPTER 2

COMPETENCIES

Guide to preparing competency statements

When accepted into the program the candidate is required to submit a written “competency statement” reflecting the current levels of achievement on each of the nine competencies that are shown in this chapter. The candidate must designate five of the nine competency statements as *Major* competencies. The remaining four competencies will then be regarded as journeyman level competencies for the purposes of the ASP process. This submission is the “heart” of the ASP application and is the main document followed by the PAB and also the verification team (Chapter 3) when confirming the self-stated professional standing by the candidate during the on-site verification.

Each competency statement is to be thorough enough to show a superior level of standing and must be signed by the candidate and countersigned by the candidate’s superior or other person with some professional knowledge of the candidate’s stature in that competency. It is permissible to have several different countersignatures throughout the entire ASP competency submission document. The verification team may contact those persons who countersign the submission documents.

Each competency statement must deal with the internal components that make up each competency shown later in this chapter. The written statement must clearly show the level of experience and involvement that the candidate has achieved in each competency. Where the candidate does not have experience in a given component of a competency a suitable statement must be included showing this fact and relating it to the impact on overall submission.

The competency statement document should be typed and easy to read. Each competency statement probably will extend over several pages. Pages should be numbered and dated and there should be a table of contents for the entire submission document. The format for the pages is optional.

Competency statement documents may be submitted electronically. It should be noted that not all electronic means of document transmittal are secure.

ASP submission documents may be either official language.

List of competencies

Competency One-Administration

This competency consists of five components as follows:

1. Planning

Standard:

- a. Identifies long-range needs and problems.
- b. Establishes achievable objectives.
- c. Formulates courses of action to achieve objectives
- d. Determines necessary policies, procedures and standards.
- e. Develops a budget reflecting the work program of the organization and work schedules for accomplishment.

Evidence of performance:

- Relevant documentation
- Candidate's testimony

2. Organizing

Standard:

- a. Responds to changing conditions in the environment.
- b. Determines the needs and goals of the company.
- c. Organizes security personnel by establishing clear understanding of the activities to be performed.
- d. Delegates authority and accountability through written agreements.

Evidence of performance:

- Current documentation and materials in use developed by the candidate

3. Directing and leading

Standard:

- a. Develops quality and performance standards, expectations for competence and feedback procedures for guiding, supervising and evaluating employee's efforts.
- b. Creates learning opportunities for employee development in this competency.
- c. Communicates effectively when speaking and writing.

Evidence of performance:

- Testimony of candidate's peers, both within the company and the security community

4. Controlling and auditing

Standard:

- a. Administers an audit program for standards and procedures.
- b. Conducts analysis for budget control.
- c. Develops evaluation methods as feedback and as a guide for meeting goals and needs.

Evidence of performance:

- Audit reports and comparative historical data

5. Managing employees

Standard:

- a. Develops effective procedures for the recruiting, selection, orientation, training, development, promotion and discipline of the human resources of the security organization.
- b. Develops criteria for evaluation, feedback and guidance of the security organization's programs for employee management, such as a safety and accident prevention program, a training program, and a labour-management relations program.

Evidence of performance:

- Relevant documents about current policies, procedures, programs and plans.
- Testimony of personnel managers, the candidate and employees

Competency Two-Physical Security

This competency consists of four components as follows:

1. Evaluating threats to company assets

Standard:

- a. Identifies assets that need protection.
- b. Identifies potential threats to each type of asset.
- c. Evaluates risks to each asset to include statistics and crime trends.
- d. Evaluates effectiveness of police forces to protect company assets.
- e. Prepares reports on threats assessments.

Evidence of performance:

- Reports, studies and surveys prepared by the candidate.
- Candidate's testimony

2. Planning and recommending/implementing a system of physical safeguards and equipment

Standard:

- a. Identifies safeguards needed to protect company assets.
- b. Identifies equipment that would protect company assets.
- c. Evaluates effectiveness of existing safeguards and equipment.
- d. Recommends improvements for effective and efficient procedures and/or product.
- e. Works with engineers and architects to include effective and efficient security in new projects.
- f. Prepares cost/benefit analyses.

Evidence of performance:

- Documentation of reports, studies and surveys used by the candidate
- Candidate's testimony

3. Planning and organizing an access control system

Standard:

- a. Organizes a system to control access to company premises.
- b. Integrates human resources (secretaries, receptionists, guards) and technology (card-access systems, alarm systems, closed circuit television, etc.) to control access.
- c. Writes access control policies and procedures.
- d. Writes policies and procedures regarding searches of employees and visitors entering or leaving premises; gives personnel specific instructions on procedures to follow if someone is caught stealing or threatening company assets.

Evidence of performance:

- Documentation of reports, studies and surveys used by the candidate
- Candidates testimony

4. Evaluating and recommending the most recent technological equipment, systems and methodology

Standard:

- a. Selects appropriate technology and equipment to counter identified threats to company assets using personal knowledge or using contractors and consultants.
- b. Understands the functions and applications of locks and key control, alarm systems and security containers, closed circuit television, fences, doors, windows, access controls and related systems.
- c. Recommends specific makes and types of equipment.

Evidence of performance:

- Surveys, studies, recommendations or reports used or prepared by the candidate.
- Testimony of the candidate ● Attendance at security trade shows and seminars

Competency Three- Human Resource Security

This competency consists of five components as follows.

1. Planning, organizing and implementing a human resources protection program

Standard:

- a. Plans for prevention of and responses to kidnap and hostage situations, attacks, threats and misadventure.
- b. Plans and provides guidance to the corporation to minimize risk to employees.
- c. Plans and develops a security awareness program for employees.

Evidence of performance:

- Documents relating to the program to include a bona fide record of the program's success in a related incident, if available
- The candidate's testimony

2. Planning and implementing a continuing security education program

Standard:

- a. Assesses the requirements for security awareness.
- b. Creates an awareness program.
- c. Enlists support for the program by explaining its objectives and encouraging an appreciation for its contribution

Evidence of performance:

- Documentation that the program is in place and effective
- Materials from the program ● Candidate's testimony

3. Planning, organizing, and conducting a personnel security-screening program

Standard:

- a. Designs and operates a structured system to collect relevant information, conduct appropriate background checks and make screening decisions.
- b. Applies appropriate security safeguards on the management of screening information.
- c. Investigates adverse information to determine the truth.
- d. Reports all findings that lead to denial of screening status to company executive.

Evidence of performance:

- Program documentation outlining policies and practices ● Candidate's testimony

4. Organizing and implementing a program for emergency procedures for personnel

Standard:

- a. Prepares and maintains emergency response and protective procedures.
- b. Prepares and updates procedures relating to abuse of employees in the workplace.
- c. Identifies hazards and prepares and implements procedures to deal with them.

Evidence of performance:

- Program documentation outlining policies and practices
- Candidate's testimony

5. Organizing and implementing a program for employee identification

Standard:

- a. Provides credentials for employees, agents, suppliers and/or visitors.
- b. Provides authorization documents allowing the holder selective access to the corporation's facilities, premises and processes.
- c. Plans for the control of internal movement and control of personnel.

Evidence of performance:

- Documentation that the program is in place and effective
- Candidate's testimony

Competency Four-Information and Asset Security

This competency consists of five components as follows:

1. Designing, developing and implementing a program which protects sensitive company information against loss and compromise

Standard:

Plans and organizes policies, procedures and compliance requirements for a system to protect the company's proprietary information.

Evidence of performance:

- Documentation relating to the program and evidence of its implementation
- Candidate's testimony

2. Planning and making employees aware of an information security awareness program

Standard:

- a. Maintains level of awareness commensurate with assessment of sensitivity and the perceived level of threats.
- b. Ensures the program is up-to-date and adaptable.

Evidence of performance:

- Documentation/visual aids developed by the candidate and currently in use.
- Testimony by employees exposed to the program.
- Testimony by candidate's peers within the company, and the security community if possible, who have direct knowledge of the candidate's efforts and achievements.

3. Planning and conducting audits

Standard:

- a. Provides management with an ongoing assessment of threats and risks, appropriate levels of protection and remedial action required.

Evidence of performance:

- Audit reports and other relevant documentation
- Comparative data from previous audit reports.

4. Recognizing, designing and implementing physical and electronic security countermeasures for information handling as electronic information technology is implemented and managed

Standard

- Maintains securities of information as new processing methods are introduced by applying appropriate electronic security safeguards.

Evidence of performance:

- Program documentation, revisions and installation plans.
- Candidate's testimony

5. Maintaining the security requirements required by the Industrial Security Program administered by the federal department Public Works and Government Services Canada

Standard:

- a. Fulfils the company's contractual security obligations.
Note: This may not apply if the candidate's employer is not involved in contracts with the federal government involving sensitive information.

Evidence of performance

Copies of completed or current contracts completed. Records of inspections recognizing the compliance by the company with the government security program

Competency Five-Legal Aspects of Security

This competency consists of four components as follows:

1. Developing security procedures for company employees outlining legal powers and responsibilities

Standard:

- a. Conducts basic training of security personnel on their legal powers and responsibilities.
- b. Writes procedures on legal powers and responsibilities relating to employee theft.
- c. Writes procedures on legal powers of search, seizure and arrest.
- d. Ensures these policies and procedures protect the rights of both the company and the employee.

Evidence of performance:

- Planning and delivery documents on the contents of training sessions given to security personnel.
- Procedures in place dealing with employee theft, searches, seizures and arrests
- Reports, studies, recommendations submitted by candidate.

2. Applies civil law concepts to security in a work environment

Standard:

- a. Consults with management relating to security requirements for company hiring practices.
- b. Participates in formulation of policy on discipline for dishonesty or unacceptable behavior.
- c. Evaluates an incident and decides whether sufficient evidence is available for disciplinary or criminal action.

Evidence of performance:

- Company hiring standards and discipline policy
- Official investigation reports by the candidate
- Candidate's testimony

3. Directing or conducting an investigation so admissible evidence is obtained and available for prosecution authorities

Standard:

- a. Gathers and protects evidence so it is admissible at a civil or criminal trial.
- b. Evaluates for probative value real, documentary and circumstantial evidence and confessions.
- c. Briefs the police, the prosecutor or company lawyer on evidence available and its value.
- d. Gives testimony in civil or criminal proceedings.

Evidence of performance:

- Investigation reports.
- Candidate's testimony

4. Administering a contract with a security service or equipment supplier

Standard:

- a. Assesses the liability of the company as a contract guard force or service or equipment supplier.
- b. Interprets a security contract for goods and services.
- c. Determines licensing requirements for a security contractor.

Evidence of performance:

- Contract documentation.
- Candidate's testimony

Competency Six-Investigating Incidents

This competency consists of six components as follows:

1. Analyzing security conditions and circumstances

Standard:

- a. Develops or maintains statistical data and related records to identify patterns of loss, theft, damage and non-compliance.
- b. Applies basic principles of accounting and auditing to analyze financial statements and related transactions and records.
- c. Develops or maintains a reporting system for monitoring security threats to the corporation and its operating environment.
- d. Uses statistics, reports and associated information as a database on which investigative action can be reliably predicated.
- e. Categorizes security incidents as offences under the Criminal Code, provincial statutes and their regulations, municipal by-laws, standards, practices and company policies to determine the appropriate agency with jurisdiction for dealing with them.

Evidence of performance:

- Documentation of reports, statistical data, analyses, company policies and procedures on security topics
- Candidate's testimony

2. Coordinating and conducting investigations

Standard:

- a. Organizes, directs or conducts investigations effectively, having regard for the priority, purpose, legal implications and cost benefits to the company.
- b. Demonstrates a working familiarity with investigative techniques, technical, forensic and other aides to investigation, sources of information and agencies of assistance.
- c. Develops or maintains procedures for collecting, organizing, maintaining and disseminating the findings of investigations.
- d. Develops or maintains an effective working relationship with law enforcement agencies, the security community, crown attorneys and supporting units of the criminal justice system.

Evidence of performance:

- Documentation relating to investigations
- Candidate's testimony

3. Conducting interviews and obtaining statements

Standard:

- a. Develops or maintains a systematic control procedure for conducting investigations to include interviewing and taking statements, having regard for legal and ethical issues and the principles of investigation.
- b. Demonstrates knowledge of investigation in respect of legal requirements, policy compliance, employee Charter and other rights, corporate policy and case preparation.

Evidence of performance:

- Documents relating to investigations
- Candidate's testimony

4. Collecting information and evidence

Standard:

- a. Develops or maintains systematic procedures for obtaining and recording the basic information which contribute to sound investigative decisions.
- b. Develops or maintains methods and equipment and practices for identifying, collecting, protecting, preserving and transferring items of evidence for admissible presentation in a court of law.
- c. Demonstrates knowledge of sources of information including public and private agencies, archives and data banks, and of procedures for gaining access to that information.

Evidence of performance:

- Documentation outlining current practices in gathering information and evidence
- Candidate's testimony

5. Testifying before courts and other hearings

Standard:

- a. Develops or maintains guidelines for briefing witnesses which include rules relating to admissibility of evidence, expert witnesses, examination-in-chief and cross examination, conduct and deportment and court rules of procedure and protocol.
- b. Develops or maintains a program for training inexperienced personnel to give credible testimony at trial, or other hearing so their appearance and testimony is relevant and acceptable.

Evidence of performance:

- Documentation of program guidelines for coaching and preparing personnel in providing evidence
- Candidate's testimony

6. Writing reports and correspondence

Standard:

Develops or maintains reporting systems that records essential information, transmits investigative findings, provides for security of information, and provides a permanent record of all investigative activity and evidence obtained.

Evidence of performance:

- Documentation to include sample reports written and supervised
- Candidate's testimony

Competency Seven-Planning for Emergencies

This competency consists of three components as follows:

1. Developing and managing a corporate or facility security program to deal with routine corporate and workplace emergencies

Standard:

- a. Identifies response needs by analyzing data, considering probabilities, impacts and developing priorities.
- b. Develops measures to prevent, reduce, detect and respond to incidents and evaluates outcomes.
- c. Integrates an emergency security program with other corporate emergency services.
- d. Obtains management approval for plans.
- e. Implements the emergency response program.

Evidence of performance:

- Documentation relevant to the security program
- Candidate's testimony

2. Managing the security aspects of a corporate disaster response program

Standard:

- a. Represents the security function on corporate management's emergency planning and response teams.
- b. Develops emergency security support services.
- c. Liaises and integrates services with other corporate emergency support services.
- d. Implements security aspects of the plan.
- e. Evaluates outcomes.

Evidence of performance:

- Documentation relating to the program
- Candidate's testimony

3. Managing security aspects of a corporate program to deal with community-wide disasters

Standard

- a. Represents the corporation with local emergency measures organizations.
- b. Represents the security function on corporate management's emergency planning and response teams.
- c. Develops and integrates security emergency operations with other corporate emergency programs.
- d. Evaluate outcomes.

Evidence of performance:

- Documentation relevant to the program
- Candidate's testimony

Competency Eight- Employee Relations

1. Conducting or directing an investigation into an employee in a manner that protects both the employee rights and company assets

Standard:

- a. Has a working knowledge of federal and provincial laws that define the rights and obligations of labor and management.
- b. Protects the rights of an employee under investigation.
- c. Assesses evidence gathered in preparation for labor arbitration or wrongful dismissal suits.
- d. Instructs counsel in preparation for labor arbitration or wrongful dismissal suits.

Evidence of performance:

- Documentation relating investigations
- Candidate's testimony

2. Preparing a program for security during a labour strike or corporate lockout of workers

Standard:

- a.. Provides a security program at a facility during a strike or lockout in a manner that protects the rights of employees and protects company assets.

Evidence of performance:

- Documented procedures outlining instructions to employees or security staff during a strike or lockout
- Candidate's testimony

3. Preparing a case for presentation to a labour arbitration hearing

Standard:

Gathers evidence on behalf of the employer and prepares it for admission at a labour arbitration hearing.

Evidence of performance:

- Documentation relating to a case prepared or directed by the applicant.
- Candidate's testimony.

4. Preparing a health and safety program for a work site

Standard:

Prepares and implements a program developed for the health and safety of employees.

Evidence of performance:

- Documentation relevant to a health and safety program
- Evidence of corporate personnel having direct knowledge of the program
- Candidate's testimony

Competency Nine-Information Technology Security

This competency consists of seven components:

1. Planning, organizing, implementing and conducting an Information Technology Security (ITS) program

Standard:

- a. Provides ITS safeguards to protect all facets of information that is proprietary to the organization or entrusted to it.
- b. Ensures that the program is comprehensive as required by corporate needs.
- c. Provides essential components of the ITS program to include control and implementation of passwords, user identification, information classification, documentation, access, maintenance, operational services, telecommunications, copiers, shredders, dial-up access and encryption.
- d. Prepares, using necessary assistance, design specifications for new or expanded computer facilities.
- e. Acts as facility ITS coordinator responsible for local implementation of ITS policies and procedures.
- f. Provides internal advice on the practicality of applying or modifying ITS measures considered generic to industry.

Evidence of performance:

- Documentation relating to contracts with an ITS consulting firm and records of measures taken to comply with corporate policy
- If applicable, unclassified correspondence relevant to the Industrial Security Program assuring federal clearance of ITS facilities for federal contract use
- Documentation relevant to the program and records, operational logs and correspondence describing the various program elements
- Candidate's testimony

2. Planning, organizing and implementing Information Technology Security (ITS) policies and procedures

Standard:

Manages easily understood policies, procedures and documentation that provide a mandate and instructions to protect the organization's information technology resources.

Evidence of performance:

- Documentation relating to ITS policies and procedures
- Evidence that ITS personnel can authoritatively comment on the adequacy and control of ITS systems, programs, data processing and user documentation
- Candidate's testimony

3. Planning, implementing and conducting Information Technology Security (ITS) security awareness and education program

Standard:

- a. Plans and implements an awareness program covering all aspects of the Corporate ITS program

Evidence of performance:

- Documentation that the program is in effect
- Articles or material from the program
- Evidence from ITS personnel who can reasonably comment on the program's effectiveness
- Candidate's testimony

4. Planning and organizing a security self-assessment program to be implemented by Information Technology Security (ITS) security supervisors at dispersed corporate facilities

Standard:

Distributes ITS monitoring responsibility to each major organizational entity that uses information technology in order to identify and improve upon its own deficiencies.

Evidence of performance:

- Documentation relevant to the program
- Records showing the appointment of ITS supervisors and checklists specific to the sub-organizations completed by the ITS supervisors.
- Correspondence indicating action taken to correct deficiencies
- Candidate's testimony

5. Planning and implementing an Information Technology Security (ITS) physical security program

Standard:

- a. Provides security safeguard equipment to protect the data processing installation against unauthorized access, fire, water damage, electrical failure and power irregularities and temperature and humidity.
- b. Provides security safeguards, devices and procedures that minimize or eliminate exposure of personal computers to theft of the machine or its information.

Evidence of performance

- Presence of systems or equipment
- Records of logged access by authorized contractors and visitors.
- Operator's testimony that contractors, visitors, and maintenance staff are supervised within the center
- Candidate's testimony

6. Assisting in the planning and implementing Information Technology Security (ITS) for information technology operations

Standard:

- a. Works with information technology operators to achieve optimum recovery from system failures, maintenance of system monitoring, investigation of security violations and breaches of security, control of equipment vendors and secure storage, inventory control and erasure of electronic data from electronic media.

Evidence of performance

- Documentation relevant to security briefing/training provided and security and operating procedures
- Operator's testimony on system monitoring and ability to recover from failures
- Records of investigation into violations and breaches
- Maintenance agreements.
- Use of an appropriate tape storage area
- Presence of labels on media containers (tapes and disks) showing security classification
- Candidate's testimony.

7. Planning, organizing and implementing a contingency and business recovery program

Standard:

- a. Provides a detailed contingency plan for data processing operations that ensures resumption of business in the event of major equipment failure or destruction of the computer operations center,
- b. In consultation with others plans a business system that provides for regular computer media back-ups off-site and that assures access protection according to the classification of the media's content.
- c. Reduces the organization's overall financial costs attributable to security risks.

Evidence of performance

- Documentation of the plan
- Written verification of the plan's successful implementation in a test, or after an actual incident
- Records showing that the plan is reviewed and tested on a regular cycle.
- Documentation of methods of financial risk control and/or insurance policies
- Candidate's testimony

CHAPTER 3

THE VERIFICATION PROCESS

Introduction

A team of not less than two security practitioners who hold Accredited Security Professional (ASP) designation will be tasked to perform a verification visit(s) to the work or other site of the candidate. During this visit the team will examine a suitable random sampling of the competency statements submitted by the candidate and compare each such statement with available acceptable evidence of performance. Verification of the candidate's competency statements provides assurance that the Accredited Security Professional (ASP) status has been achieved and confirms the credibility and suitability of the candidate for ASP status.

Verification team

The Professional Accreditation Board (PAB) selects, without consultation with the candidate, two security practitioners who hold the ASP designation to perform the verification visit. The candidate is notified of the identity of the verification team members. An objection by the candidate to one or more of the team members is examined by the PAB and, if warranted, the Board of Directors. If an objection is accepted one or more alternate verification team members will be selected.

The verification team members are provided with all the documentation submitted by the candidate. They are responsible for studying the material and making a mutually acceptable visit and work plan for the verification process in consultation with the candidate.

During the visit to the work or other site the candidate is responsible to be present, host the verification team and make access available to all necessary evidence required for the team to do its work.

Protocol

The verification team will abide by the Code of Ethics of the Society. In addition they will:

- Not disclose a confidence that is unrelated to the ASP verification.
- Respect all limitations required by the management of the enterprise.
- Focus only on verifying the accuracy of the summary of the nine competencies submitted by the candidate.
- Not divulge any information provided by the candidate's supervisor.
- Not disrupt any production schedules or work practices unless approved by management of the enterprise.
- Report only to the PAB, or if approved, the Board of Directors

Proprietary or sensitive information

Should a verification team member accidentally see proprietary, government or sensitive information, it is the candidate's responsibility to manage these circumstances to minimize compromise. The verification protocol will assure the verification team, the PAB or CSIS, INC, does not further distribute the information.

All ASP program records and reports become the property of CSIS, Inc. and are protected from third party disclosure. Records and reports relating to ASP are normally retained by the Society for several years, and may be destroyed after a suitable period of retention. Requests for the return of ASP application and process records to the candidate should be made to the Board of Directors.

Procedure

It is recommended that the verification team be introduced to organization officials and the role of the team explained. At this time any questions can be answered and assurances made about the confidentiality and other protocols to be followed by the team. The verification team should be provided with working space.

The team will be guided in their work by the candidate's submission. The team will need to see copies of relevant security policy and other documents. The availability of documents is an important point in the verification process because much of the effectiveness in security management is tied to the existence of policy, procedures and practices. Key documents that are unavailable may, therefore, limit the ability of the verification team to assure existence of suitable performance and render it incapable of verifying the candidate's submission. Specific arrangements for viewing documents, areas and perhaps speaking with employees, if that is needed, can follow any suitable schedule.

The verification team's interview with the candidate's manager is a key activity that serves to reinforce the assessment of the competency of the candidate. Such interviews are not normally long, but it is important that the team have sufficient time and a suitable place to deal with the details of their mission and obtain substantive information on the professional standing of the candidate. The candidate is not present during this interview.

The verification team will not debrief the candidate before departure from the work or other site. The team will prepare a written report of their findings and make recommendations to the PAB. The report will contain a copy of the ASP competency statements and the study paper submitted by the candidate. The team will not disclose their findings or recommendations to the candidate. A summary of this information will be forwarded to the candidate by the PAB.

CHAPTER 4

STUDY PAPER

Requirement

Candidates are required to prepare a fully researched study paper on any aspect of security. The paper must be of sufficient quality and substance to permit publication in a national magazine or newsletter. The purpose of this submission is to show professional awareness of security issues and to give substance to the statements of competency and degree of professionalism. This submission also provides an opportunity for the candidate to contribute to the body of published security knowledge. Attribution of sources of information (footnotes or a chapter listing sources) is required. A bibliography must be included. The extent of the paper is optional; however, ASP study papers are expected to contain at least 3500 words.

The paper may contain charts, graphs, tables, images and any other graphic material supporting the topic being presented. The Professional Accreditation Board (PAB) might consider other forms of material, such as a video and/or audio production, if permission is obtained in advance. The document may be in any suitable binder and should, for convenience of a publisher, also be in electronic form, such as a diskette.

Copyright remains with the candidate. Opinions remain those of the author.

Annex A

Application Information and Form