



CERTIFIED SECURITY PROJECT MANAGER

Candidate Handbook & Study Guide



Updated August 2022

CSPM Handbook & Study Guide

Introduction	1
The Role of the Security Project Manager	2
Why Become Certified?	2
Section I – Certification Process	3
Eligibility Requirements	3
Application and Payment	4
Special Testing Accommodations	4
Certification Fees	4
Scheduling the Exam	5
Canceling or Rescheduling the Exam	5
On the Day of the Exam	6
Exam Security	7
What to Expect After the Exam	8
Score Reporting	8
Appeals	8
Retaking the Exam	9
Certificates and Record Keeping	9
Section II – How the Certification Examination Is Developed	10
Job Task Analysis	10
Exam Specifications	10
Item Development	10
Cut Score Study	10
Section III – Preparing for the Exam	11
Exam Content	11
Suggested References	11
Sample Test Items	13
Section IV – Maintaining the Credential	15
Certification Maintenance Fees	15
Recertification	15
Compliance	16
Appendix I – Exam Specifications	17
Appendix II – Certification Agreement	22
Appendix III – Code of Ethics	24

Introduction

Thank you for your interest in the Certified Security Project Manager (CSPM®) credential from the Security Industry Association (SIA). CSPM certification is a fundamental step for security project managers eager to sharpen their professional edge.

The CSPM credential is the only project management credential specific to the security industry. Security project managers will find that holding the CSPM credential affords them greater opportunities for employment, career advancement and professional credibility. CSPMs enjoy enhanced confidence in job delivery and a sense of personal accomplishment as a result of their mastery of security industry concepts.

The CSPM credential provides assurance to employers that, through certification and recertification, each credential holder is committed to quality and has demonstrated competence in six security industry domains, making their services more likely to satisfy their employer's needs than their noncertified peers.

The security industry demands project managers who can navigate challenging situations, changing technologies and complex issues all within the framework of clients' and employers' expectations, including budgetary constraints. CSPMs employ a unique body of knowledge and skills to meet these challenges and in so doing demonstrate the value of their particular expertise. In addition to the mastery of security industry concepts that they display at the time of initial certification, CSPMs show their commitment to learning new skills through recertification activities, thereby increasing their value to clients and employers alike.

The CSPM certification program is based on a rigorous examination. All applicants must successfully complete the exam to become certified. Eligibility requirements for the exam are based on project management work experience, with academic achievements being allowable substitutions for a portion of the required work experience.

The certification program uses credentialing industry best practices for the development of a content-valid, legally defensible assessment. The examination measures individuals' potential for competence in relation to a standard set by industry experts. The method used to design the examination are outlined in Section II of this document.

This candidate information brochure is a guide to the certification process and a tool for identifying topic areas that require additional self-directed study. It is not intended to be the sole resource used in preparation efforts. Applicants should seek out additional training or study to augment their knowledge in areas identified as weaknesses.

If you have questions about this guide or any other part of the Certified Security Project Manager program, please email Katie Greatti, associate director of learning and development at the SIA, at kgreatti@securityindustry.org.

The Role of the Security Project Manager

A Certified Security Project Manager (CSPM) is a professional experienced in the management of security projects which typically entail installing and integrating various components of a security system into a physical building structure. To become certified, an applicant must meet eligibility requirements and take and pass the certification exam. When the exam is successfully completed, the candidate becomes certified for a three-year period, subject to annual certification maintenance fees. A security project manager's central activities involve:

- Leading the project team
- Understanding the entire scope of work
- Communicating and working with the project stakeholders
- Anticipating and resolving problems
- Maintaining control over the costs, schedule and quality of the project
- Assuming responsibility for the entire project life cycle
- Working with salespersons to accurately define the customer's security needs
- Ensuring the compliance of the project with all applicable codes

Why Become Certified?

There are many benefits of CSPM certification:

- **Advancement:** Increased career opportunities, with the potential for increased salary
- **Recognition & Respect:** Formal acknowledgement of your specialized knowledge and professional expertise
- **Professional Identity:** The privilege to promote yourself as a CSPM and holder of the only project management credential for the security industry
- **Esteem:** Enhanced credibility with employers and colleagues
- **Growth:** Proclaim your commitment to excellence through continuing education and professional development
- **Pride:** Self-esteem and pride in your job skills

Section I – Certification

IMPORTANT NOTES:

- SIA has employed a professional testing company, Meazure Learning, to assist in the performance of various examination development and administration functions.
- Email is the primary mode of communication between SIA and certification candidates.

Eligibility Requirements

To be eligible for the CSPM exam, a candidate must have completed a minimum of 6,000 hours (about three years) of hands-on project management experience. **A minimum of 3,000 of these hours must be direct security project management experience.**

Formal education from an accredited* institution may substitute for some of the required experience as follows:

- A candidate with a two-year associate's degree in a **security-related discipline** may substitute the degree for 500 hours of the required experience;

OR

- A candidate with a four-year bachelor's degree in **engineering, architecture or security** may substitute the degree for 2,000 hours of the required experience;

OR

- A candidate with a four-year bachelor's degree in another field of study may substitute the degree for 1,000 hours of the required experience;

AND

- A candidate who also has a master's degree may substitute it for an additional 500 hours of the required experience.

**The academic institution must be accredited by one of the six regional accreditation bodies recognized and listed by the U.S. Department of Education and the Council for Higher Education Accreditation.*

I have a ...	2-year associate's degree in a security- related discipline	4-year bachelor's degree in engineering, architecture or security	4-year bachelor's degree in another field of study	master's degree and a bachelor's degree in engineering, architecture or security	master's degree with a bachelor's degree in another field of study
I need this many hours of work experience*	5,500	4,000	5,000	3,500	4,500

**A minimum of 3,000 of these hours must be direct security project management experience.*

All applications are subject to audit whereby applicants are required to provide supporting documentation verifying the required hours of experience and education.

Application and Payment

Please carefully review the eligibility requirements above **PRIOR TO** submitting the application and nonrefundable application fee.

Candidates must complete the [online](#) application and pay the nonrefundable application fee. Once approved, candidates can pay the nonrefundable application fee.

All applications are subject to audit whereby applicants provide supporting documentation verifying the required hours of experience and education.

Each applicant will be notified of their eligibility status via email within two weeks of application.

PLEASE NOTE: By signing the Application Form, applicants attest that they have read and will abide by the Certification Agreement (Appendix I) and the Code of Professional Ethics (Appendix II). Failure to conform to either may result in disciplinary actions up to and including revocation of the credential should it be earned.

Special Testing Accommodations

SIA complies with the Americans with Disabilities Act (ADA) and is dedicated to ensuring that no eligible individual is deprived of the opportunity to take the exam due to a disability as defined under the ADA, as long as the disability is not one which would render the individual incapable of performing the duties of a certified position. **A candidate who requires special testing accommodations must make a written request for the specific type of accommodation needed at the time of application.** Each request must include documentation of a formally diagnosed, ADA-recognized disability from a qualified professional who has provided evaluation or treatment to the applicant.

Certification Fees

Application Fee	\$325
Exam Fee (due when scheduling testing appointment) for U.S. and Canada	\$75
Exam Fee outside of U.S. and Canada	\$100
Exam Rescheduling Fee (due if rescheduling less than 72 hours prior to appointment)	\$50
Annual Certification Maintenance Fee (due in each of the three years of the certification cycle)	\$40
Late/Expired Fee (due if annual certification maintenance fee is past due or if CSPM fails to recertify by the date the current certification expires)	\$25

Scheduling the Exam

Candidates schedule their exams through Meazure Learning. For help with this process, contact Katie Greatti at kgreatti@securityindustry.org or 301-804-4741.

The CSPM exam is administered at more than 900 Meazure Learning computer-based testing facilities throughout the world. Meazure Learning provides candidates with the convenience of taking the exam at a center closer to home, which saves travel time and money. In addition, candidates are provided with their preliminary scores immediately following the exam.

When you establish eligibility and your application is approved, you will receive an “authorization to test” via email; this message will contain login credentials for the Meazure Learning appointment website. Through this site, candidates schedule their appointments to take the exam and pay the \$75 U.S. and Canada testing fee. The fee to test outside of the U.S. and Canada is \$100. Available dates and times vary by testing location.

After receiving the “authorization to test,” an eligible candidate must take the exam within one year. After 12 months, this period expires, and the individual must reapply as a new applicant and pay the application fee again.

Canceling or Rescheduling the Exam

An exam appointment can be rescheduled without penalty up to 72 hours in advance of the scheduled appointment. Candidates can reschedule their exams online through the Meazure Learning website. If a candidate reschedules the exam less than four business days in advance, a \$50 rescheduling fee will be assessed.

Those who fail to appear for a test without giving prior notice will forfeit the entire exam fee unless they can document extenuating circumstances such as a death in the family, serious illness or military duty. In such circumstances, the candidate should contact SIA as soon as possible and provide an explanation of the situation in writing.

Every attempt will be made to administer all exams as scheduled; however, in the event of hazardous weather or any other unforeseen emergencies occurring on the day of a scheduled exam, Meazure Learning will determine whether circumstances require the cancellation of the exam at a particular location. In the event of a Meazure Learning cancellation, candidates will be given as much notice as possible and will not be penalized by Meazure Learning. In such instances, SIA will contact candidates for rescheduling.

On the Day of the Exam

Each candidate should report to the exam center on the day of the exam as instructed in their appointment confirmation letter and plan to arrive at least 15 minutes prior to the appointment time. **Each candidate must bring a government-issued photo ID with signature (e.g., driver's license or passport). The name on the ID must exactly match the name submitted on the application, or the candidate will be denied admission. A second form of ID may be requested at the testing center. A credit or debit card matching the name on your government-issued ID is acceptable.**

Candidates should bring as few personal belongings as possible to the testing center. Most items will not be permitted in the testing room. Some exam sites have secure locations for the storage of personal items, but this is not guaranteed at each location. SIA and Measure Learning are not responsible for any items brought to the testing center.

Items that are NOT permitted include, but are not limited to, the following:

- Books or other reference materials, including all types of dictionaries
- Papers of any kind, except as provided by the proctor
- Electronic devices of any kind, including:
 - o Telephones and signaling devices, such as cell phones, tablet computers and laptops
 - o Alarms or recording/playback devices
- Photographic or image capturing or copying devices
- Food or beverages, including water

Candidates wishing to use the restroom or water fountain should indicate this to the proctor. At any given time, only one candidate will be allowed to leave the testing room. The exam clock continues to run during any breaks taken.

Listen carefully to the instructions given by the proctor and read all directions thoroughly. Questions concerning the content of the exam will not be answered during the exam, but a comment form is provided within the testing software. Candidates are strongly encouraged to provide feedback or report any concerns prior to leaving the testing center.

Connectivity issues are inherent with computer-based testing. Any technical difficulties that affect a candidate's performance must be reported to the proctor immediately. Reports of this nature should be made before the candidate receives the score report and also noted in the post-exam survey. Additionally, candidates must report any complications with testing to Measure Learning immediately following the exam.

Exam Security

SIA firmly believes that each candidate deserves a fair and equal opportunity to demonstrate his or her competency in the examination process. Therefore, the examination security measures are intended to prevent any unfair advantage of one candidate over another. Security measures are also in place to protect SIA's intellectual property.

All exam materials, including the entire item (question) bank and each form of the examination, are the exclusive property of SIA.

Candidates who exhibit disruptive behavior or who give/receive assistance from other examinees, testing personnel and/or anyone outside of the testing center will be required to leave the testing room immediately. Their exam will not be scored, and their actions will be reported to SIA for possible disciplinary action. A candidate who witnesses inappropriate behavior should report it to the proctor immediately.

To prevent fraud, completed exams are analyzed statistically for any suspicious response patterns.

Removal of any material from the exam room by unauthorized persons is prohibited. Copyrights for the CSPM exam are owned by SIA. Any attempt to reproduce or memorize all or part of the exam is prohibited. Any unauthorized disclosure, publication, copying, reproduction, transmission, distribution or possession of CSPM exam content or materials in any form, including memorization, may subject the individual to civil liability and/or criminal prosecution, removal of certification and/or restrictions on future access to CSPM certification examinations. **The prohibition of "unauthorized disclosure" means that you may not discuss the contents of the examination with anyone other than SIA staff.**

A proctor may dismiss a candidate from the exam site, halt an examination in progress or report a candidate to SIA for any unauthorized behavior.

SIA reserves the right to cancel any exam scores if, in SIA's judgment, there is any reason to question the score's validity. Conduct that warrants score cancellation may include, but is not limited to: consulting study aids of any type during a testing session; copying from notes or another candidate's answers during a testing session; unauthorized communication with others during a testing session; copying, photographing, transcribing or otherwise reproducing or transmitting exam materials; removing exam materials from the testing site; aiding other examinees or receiving aid from anyone else; or having improper access to CSPM content prior to the exam administration. Engaging in such misconduct may disqualify the individual from future CSPM tests and possibly from ever being certified by SIA.

What to Expect After the Examination

Score Reporting

Candidates receive preliminary exam results at the testing center following the completion of the exam. Scores are later finalized after a statistical analysis has been done. The results will only change if any irregularities are found during this analysis. Candidates will be notified if there are any changes to their results. Changes to preliminary results are extremely rare.

The CSPM exam is a criterion-referenced exam and is not designed for use as a tool for comparison of CSPMs. All credential holders are held to a specific criterion (the passing score that is defined by subject matter experts for awarding the certification); a passing score on the exam affirms that the candidate meets an established level of competence. Comparison of candidates based on their exam scores is not appropriate for this type of exam; candidates are not competing against one another, and grades are not curved.

As a result, SIA does not report to candidates their numerical scores if they are at or above the passing score. In other words, candidates who pass the exam will only receive reports that they have passed; numerical scores will not be included in the results. Candidates who are not successful, however, will receive their scaled scores and diagnostic information that may help guide future study.

The passing score is applied consistently to all test takers. You must achieve the passing score to pass the exam. There are no exceptions.

Application for the exam signifies the candidate's authorization for the testing agency to release exam results to the candidate and SIA and Measure Learning staff. Only staff with a need to know for job completion will be provided access to score information. Individual scores will not be made available to the general public; however, aggregated results may be used by staff for research, marketing, reporting and other activities deemed appropriate by SIA.

Appeals

SIA provides candidates an opportunity to provide feedback on the exam content with respect to the technical accuracy of questions and fairness in the administration of the examination via a post-completion survey.

Any appeal must be submitted in writing to the CSPM Certification Committee via SIA's office **within seven calendar days of the examination** and should include the reason for the appeal and any supporting documentation the candidate would like to provide. SIA will not consider a request for review if it is not submitted within the seven-day window.

The committee's decision will be communicated to the candidate within 30 days of receipt of the request for review. The determination of the committee shall be final.

Administration Appeals: Appeals relating to the detrimental effects of the testing environment or administration procedures on a candidate's performance will be reviewed on a case-by-case basis.

Exam Content Appeals: A candidate who has a concern about the reliability, validity and/or fairness of the exam may submit an appeal to the SIA office. If a candidate questions the accuracy of their score, SIA will review the response record and any related facts to determine if the results are correct.

Certification will not be granted based upon a successful appeal; a free or cost-reduced examination may be awarded in such instances.

Retaking the Exam

A candidate may retake the examination an unlimited number of times within the 12-month period following the authorization to test. The exam administration fee will be charged for each attempt. After this period has passed, a candidate will be required to submit a new application and pay the application fee again.

Certificates and Record Keeping

Each candidate who passes the exam will be sent a certificate with a unique certification number issued by SIA within four weeks of passing the exam. The certification is valid for three years, contingent upon the payment of annual certification maintenance fees (see additional information about maintaining the credential in Section IV).

Email is the primary mode of communication between SIA and CSPM credential holders and candidates. Keeping SIA informed of any changes to your contact information is a condition of your certification. Name and contact changes must be done within your candidate record. Failure to update your contact information may result in delays in receiving critical certification-related information.

Section II – How the Certification Examination Is Developed

Job Task Analysis

A job task analysis defines the current knowledge, skills and abilities that are required for competent practice in the role of a security project manager. These competencies are defined by experts in the security industry and validated through surveys and focus groups. A large number of security project managers rate each knowledge element and skill for frequency and importance as they relate to their professional roles.

Exam Specifications

The design of the exam is governed by the exam specifications (Appendix I). This document defines the content domains (major areas of focus) and subdomains (job tasks) covered on the exam and the percent of items (questions) covering each of these.

Item Development

The CSPM Certification Committee is responsible for the development of the exam. The committee is comprised of subject matter experts from different sectors of the security industry. Each member formulates several questions (items) which are then reviewed by multiple members of the committee for consensus on the suitability of the content, construction of the question and validation of the correct answer.

Each item is referenced to a published reference. The list of references used to validate exam items is included in Section III.

Cut Score Study

The CSPM Certification Committee must conduct a standard setting workshop to establish the cut (passing) score for the exam using subject matter experts who are knowledgeable and skilled in the field. Participants are asked to have in mind 100 eligible candidates and determine the number of those they would expect to answer each question correctly. Easier items have higher ratings, and the more difficult items have lower ratings. Having a majority of easy items would result in a higher cut score. Study participants are asked to read each exam question. Reviewers are then asked, “How many of 100 candidates would answer this item correctly?” Each of the items on the exam form is rated in this manner. The ratings are tabulated, and an average cut score is calculated. Individuals who meet or exceed the cut score pass, and those that do not pass are not granted the credential.

Section III – Preparing for the Exam

SIA does not endorse any specific person, product, resource or service as a means of preparing for or achieving certification. Candidates are encouraged to plan their own courses of study by reviewing the examination specifications, identifying any areas of weakness and securing the necessary resources to adequately prepare for the examination.

Exam Content

The exam is comprised of 125 items and must be completed in two hours.

To become familiar with the content areas on the exam, candidates should refer to the exam specifications (Appendix I). Candidates are encouraged to review the specifications to assess their level of knowledge in each of the content areas and identify the areas in which they believe they need additional preparation.

Suggested References

These primary references are used by the CSPM Certification Committee to validate the exam content. The secondary references may prove valuable to candidates looking to enhance their knowledge in particular topic areas.

- [Software House From Tyco Security Products](#)
- National Fire Protection Association (NFPA) 72 National Fire Alarm and Signaling Code, NFPA, 2016
- NFPA 101 Life Safety Code, NFPA
- [Design Hardware](#)
- [Understanding Lock Functions, Melanie Whalin, CSI](#)
- [United Locksmith](#)
- [IFSEC Global](#)
- Networking for Dummies, Doug Lowe
- [Alarm System Store](#)
- BICSI Telecommunications Distribution Methods Manual, 13th Edition Volumes 1 and 2
- [InfoSec Institute](#)
- Physical Security Principles, ASIS International, Michael E. Knoke, CCP, 2015
- (ISC)², CISSP Common Body of Knowledge, June 2015
- [Reolink](#)
- [Cabling Installation and Maintenance](#)
- [Project Management Knowledge](#)
- [Pelco](#)
- [Webopedia](#)
- [Multicom](#)

- Project Resource Manual (Manual of Practice) – Fifth Edition, Construction Specifications Institute (CSI)
- The Site Security Design Guide U.S. General Services Administration (GSA), Washington, D.C.: GSA, June 2007.
- Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems 2nd Edition, Thomas L. Norman
- ANSI/UL 827, Standard for Central-Station Alarm Services, 2008
- Implementing Biometric Security, 1st Edition, John Chirillo
- U.S. Geological Survey Manual, Physical Security Handbook
- Advanced Video-Based Surveillance Systems, Editors: Regazzoni, Carlo S., Fabri, Gianni, Vernazza, Gianni (Eds.)
- Electronic Access Control, Thomas L. Norman, 2012
- [Electrical Contractor Magazine, 2001](#)
- [ASHRAE BACnet](#)
- [Project Value Delivery](#)
- Business Math for Dummies 1st Edition, Mary Jane Sterling
- AIA Contract Documents, American Institute of Architects
- [Specs and Codes –The Blog, RLGA Technical Services](#)
- [Occupational Safety and Health Administration](#)

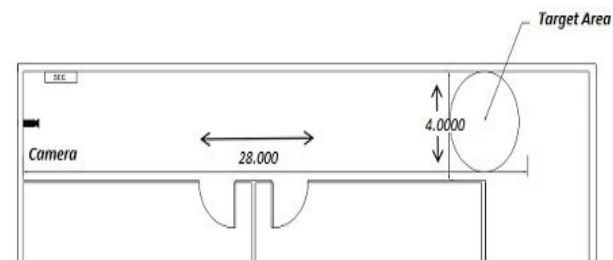
Sample Test Items

The following sample questions are intended to provide samples of the types of item formats and editorial characteristics that candidates can expect to encounter on the examination.

These items are not intended as a self-assessment instrument, nor should they be used to predict success or failure on the CSPM exam.

1. A project manager's main responsibility is to:
 - A. Maintain overall security of the project site
 - B. Meet with the owner and review their changing needs
 - C. Review, document and approve changes to scope and timeline
 - D. Ensure vendors and contractors perform work to agreed scope
2. When it is necessary to obtain a clarification or interpretation of a code or standard on a particular project, the project manager should ALWAYS communicate with the:
 - A. Authority having jurisdiction
 - B. Client representative
 - C. International Codes Council representative
 - D. Local municipal code office
3. What is required to implement anti-passback in an access control system?
 - A. A closed area with one entry point
 - B. Turnstiles allowing only a single person to enter
 - C. Access locations with readers at every entry/exit point
 - D. Barriers not allowing cards to be passed back
4. An alarm is only effective if there is a:
 - A. Monitoring station
 - B. Response
 - C. Guard force
 - D. Video surveillance system
5. Which type of access credential card operates bidirectionally on an embedded processor?
 - A. Weigand card
 - B. Smart card
 - C. Barium ferrite card
 - D. Proximity card
6. On-time performance, failure rates and reliability measurements are all metrics used in:
 - A. Developing cost estimates and work breakdown schedules
 - B. Determining earned value and budgeted costs of work performed
 - C. Performing quality assurance and quality control processes
 - D. Calculating subcontractor's bonuses and incentive payments

7. Which of the following is NOT a critical aspect of the kickoff meeting?
 - A. Cost analysis
 - B. Schedule
 - C. Timeline
 - D. Meetings
8. Ways in which project managers can facilitate teamwork include all of the following, EXCEPT:
 - A. Providing timely feedback and support
 - B. Using open and consistent communication
 - C. Delegating as much responsibility as possible
 - D. Managing conflict in a constructive way
9. The project manager fails to catch a relatively small error in a vendor's cost estimate and then finds the error later in the project. What is the appropriate response?
 - A. Deduct it from the vendor's final payment
 - B. Explain the error to the client and request a budget adjustment
 - C. Independently cover the shortfall from another area of the budget
 - D. Submit the error with other change orders
10. How would a project manager determine when to schedule the installation of electric locks for a new construction project?
 - A. Review the door hardware schedule
 - B. Consult the general contractor's schedule
 - C. Review the door delivery schedule
 - D. Consult the statement of work document
11. Based on the drawing below, which is the most cost-effective lens to use for capturing video of persons entering the target area?
 - A. 2.5 mm fixed
 - B. 12 mm fixed
 - C. 2.5-12 mm zoom
 - D. 5-8 mm zoom
12. The scope of work requires the use of biometrics for verification at a card reader door. What statement would be the MOST correct?
 - A. Biometric data must be stored on a smart card
 - B. Biometric data must associate with card data
 - C. Biometric data must be stored in the reader
 - D. Biometric data is separate from the card data
13. You can minimize confusion and lost progress on a project by:
 - A. Having a meeting to discuss problems on the project
 - B. Properly documenting any changes to the scope of work
 - C. Requiring that all stakeholders attend each meeting
 - D. Ensuring the architect is aware of any and all changes



Answer Key

1:C, 2: A, 3: C, 4: B, 5: B, 6: C, 7: A, 8: C, 9: B, 10: B, 11: B, 12: B, 13: B

Section IV – Maintaining the Credential

After getting certified, a CSPM must pay annual certification maintenance fees in each of the three years of the certification cycle and recertify every three years. In addition, CSPMs are required to abide by the [Code of Professional Ethics](#). Failure to do so may result in disciplinary action up to and including revocation of the credential.

Keeping your contact information current is a condition of certification. Email is the primary mode of communication between SIA and CSPM credential holders. Name and contact information changes must be done within your candidate record. Failure to update contact information may result in delays in receiving critical certification-related information.

Certification Maintenance Fees

The annual certification maintenance fee is \$40, due in each of the three years of the certification cycle. If these fees are not paid in a timely manner, a \$25 late fee will be assessed. Recertification will not be permitted until maintenance and any late fees are paid.

Annual certification maintenance fees provide the certification program with the financial resources necessary to ensure that certification continues to meet the needs and requirements of the market and the program can continue to function on behalf of credential holders.

Recertification

To promote continuing competence, in the third year of the certification cycle, CSPMs must recertify to maintain their certification. As the security industry continues to evolve, it is vital that CSPMs stay informed of best practices and new technology in order to promote competency and consistent provision of the duties of a CSPM.

CSPMs may elect to recertify by retaking the certification exam (application and testing fees apply) or through continuing professional education (CPE). All certification maintenance fees and any accrued late fees are due prior to consideration for recertification.

To recertify through CPE credits, CSPMs must earn a minimum of 60 credits over the course of the three-year certification cycle as follows:

a) 30 Type A Credits – Direct Security Project Management Activities

Type A credits are earned by completing activities that relate directly to the security project management profession. These activities must be directly focused on the areas covered by the six domains of the CSPM examination specifications.

AND

b) 30 Type B Credits – Professional Skills Activities

Type B credits are earned by completing activities which enhance the credential holder's overall competency. These activities include professional speaking engagements and completion of management or self-improvement courses and seminars. While these may not apply directly to the field of security project management, SIA identifies these skills as important for the growth of all professional project managers.

Credits must be submitted via the [CSPM Recertification Form](#)

Compliance

If an individual does not comply with the requirements for maintaining certification, their certification will lapse. Should a candidate with lapsed certification wish to regain the credential, they will be required to pay the application fee and successfully complete the certification exam.

In 2014 the CSPM certification program was restructured. To get certified, a candidate is no longer required to take any particular training course. Individuals who were certified prior to 2014 and did not stay in compliance by paying annual certification maintenance fees and recertifying are required to pay the application fee and take the certification exam. These individuals are not permitted to submit CPEs for recertification.

Appendix I – CSPM Examination Specifications

Description	Classification
Security Industry Specific Knowledge Fundamental	010000
Fundamental Security Project Knowledge	010000
Understand security project and security project management definitions.	010101
Read discipline construction drawings (civil, architectural, electrical, telecom and structural) that contain support infrastructure information for security systems.	010102
Identify typical terms and language used in security contracts, construction documents and other legally binding project documentation.	010103
Understand building and site infrastructure required to support the installation of physical security systems (e.g., fire-rated walls, firestopping, concrete, lighting, doors, openings, gates, continuous cable pathways, fencing and barriers).	010104
Implement safety protocols, building construction codes and CSI Masterformat specifications, specifically, divisions (28, 27 and 0871), relevant electrical codes and environmental health and safety (EHS) standards.	010105
Understand structured cabling systems requirements to support security systems (i.e., CAT5E , CAT6, RS-485 and Wiegand).	010106
Understand fundamentals of IP networking, specifically, device address schemes; level-2 network switches; and network layer, transport layer and application layer protocols.	010107
Understand integration of security systems with enterprise software applications (e.g., Active Directory, SAP, PeopleSoft and proprietary HR software).	010108
Review electronic lock permit packages before submitting to local authority having jurisdiction (AHJ) for approval.	010109
Understand the primary operations of access control systems (headend hardware, cabling systems, software applications, opening devices and credential technologies).	010110
Describe access control credentials and reader technology (e.g., smart cards, RFID, mag stripes, wireless readers, wireless locks and other identity management-related technologies).	010111
Identify common incompatibilities, pitfalls, and limitations in access control systems technology.	010112
Describe basic biometrics technology installation and operations (components, products, software applications, enrollment, limitations and quality and reliability issues).	010113
Describe primary components and basic operations of digital and analog video surveillance systems (i.e., products, software applications, hardware, IP network and storage requirements).	010114

Describe basics of security systems monitoring technology (i.e., signaling communications and encoding formats) and alarm response.	010115
Describe the basic components of security audio communications systems (i.e., products, software applications, technologies and implementation strategies).	010116
Define the basic functionality of intrusion detection systems (i.e., products, applications, components, technologies and limitations).	010117
Identify emerging security technologies and trends (e.g., drones, unmanned autonomous vehicles, PSIMs, wireless credentials, offline locks, ODSP readers, touchless openings, temperature, monitoring cameras, biometrics, AI, analytics, cloud services, IoT, machine learning and cybersecurity).	010118
Explain emergency duress concepts, solutions, applicable standards, best practices and compliance regulations.	010119
Identify common auxiliary devices and accessories connected to security systems.	010120
Specify electrical power requirements necessary to install security systems.	010121
Identify best practices, tools and techniques for conducting effective project meetings (e.g., transition meetings between sales implementation teams and between sales team customer contacts, on-site survey meetings and subcontractor reviews meetings).	010122
Relationships Between the Components of a Security Project	010200
Define applications of biometric technology to implement security identity management solutions and services.	010201
Confirm video surveillance system interface capabilities match requirements for connecting to other security systems.	010202
Interpret security systems monitoring requirements and capabilities.	010203
Confirm power requirements for equipment and devices are properly specified for a security system.	010204
Identify fire detection and alarm system (FDAS) interface requirements (i.e., fire alarm auxiliary-to-access control power supply drop-out relays) in specification and other construction documents.	010205
Understand IT network cybersecurity project management and security system requirements.	010206
Understand physical security design requirements.	010207
Understand intrusion detection design requirements.	010208
Understand building automation systems (BAS) integration requirements.	010209
Identify security operation centers (SOCs), security control centers (SCCs) and cloud-based systems command center integration requirements.	010210
Understand security audio communication system (e.g., PA system integrations and radio-over-IP) and emergency communications system (e.g., emergency call boxes and radio-over-IP) requirements.	010211

Understand mass notification system integration requirements.	010212
Coordinate door-opening hardware (e.g., locks and auto openers) with relevant disciplines (door hardware specifier, electrical contractor and architect) for doors, locks, auto-openers and lever styles, etc.	010213
Security Project Planning Basic	020000
Basic Planning Assessments	020100
Develop project management plans that identify internal and external roles, responsibilities, skill sets and training and reporting relationships for project team.	020101
Document scope of work, customer requirements, acceptance criteria and sales documents.	020102
Assess scope of work, customer requirements and sales documents.	020103
Implement project risk management processes and procedures (i.e., identify assets, conduct risk assessment and recommend and implement security measures)	020104
Develop mitigation contingency plans for risks.	020105
Create a work breakdown schedule.	020106
Analyze project activity and tasks sequences and durations.	020107
Determine potential resource constraints.	020108
Review and validate project scope of work including project budget.	020109
Plan project quality control and assurance processes and procedures.	020110
Develop project change control, configuration management, communications and assurance plans.	020111
Develop and distribute a security project schedule for review, adjustments and approval.	020112
Project Planning Roll-Out	020200
Plan, schedule and facilitate project kickoff meeting.	020201
Participate in the procurement process (e.g., proposal design, review of bids, proposals submission, contract signing)	020202
Understand the differences between the three most common methods of pro-curement (i.e., sole source, request for proposals [RFP] and invitation for bids [IFB]).	020203
Determine the type, quantity, and lead time of materials, equipment, permits and supplies needed.	020204
Define technology required to support team and project management functions.	020205
Interpret a Security "Basis of Design."	020206
Project Execution and Monitoring	030000
Execution	030100
Adopt and implement appropriate quality standards.	030101

Manage project resources, team activities and performance and feedback processes.	030102
Coordinate subcontractor activities to ensure compliance with contractual requirements and provide feedback.	030103
Utilize project management methodologies to manage project performance including the work breakdown, sequencing, network-based scheduling, dependencies and critical path.	030104
Utilize budget tracking methodology to report gross revenue, net revenue, total cost, net cost, contribution margins, break-even point and return on investment.	030105
Report financial performance using inputs such as schedule of values, earned values, bills of materials, contractor's application for payment (AIA Form G702 and Form G703) and progressive payments memos.	030106
Distribute updates and reports to the project team and other stakeholders as documented in communications plans.	030107
Implement a problem management process for identifying, documenting, tracking and solving problems (including escalation criteria guidelines).	030108
Implement a change management process for identifying, documenting, tracking and implementing changes to scope, changes and costs.	030109
Test and commission systems and technologies to validate compliance with quality requirements and user acceptance criteria.	030110
Coordinate and schedule construction administration site visits.	030111
Monitoring	030200
Maintain accurate records such as project specifications, scope of work, final submissions, red line drawings, record drawings, as builds, materials, equipment and supplies.	030201
Document and ensure compliance with quality, safety protocols, codes and regulations.	030202
Oversee the change management process (i.e., changes to project scope, schedule and cost).	030203
Implement earned value management (EVM) best practices to periodically reconcile actual performance (schedule, scope and cost) versus planned performance.	030204
Assess the completion status of closeout deliverables such as project specifications, scope of work, final submissions, red line drawings, record drawings, as builds, materials, equipment, supplies and on-site activities.	030205
Log communications and distribute information according to communications plan.	030206
Escalate potential project risks and present risk mitigation strategies.	030207

Project Closing	040000
Project Closing	040100
Confirm project deliverables and acceptance criteria were completed.	040101
Prepare closeout submission package for final distribution, review and acceptance (e.g., commissioning documents, O&M manuals and record drawings).	040102
Confirm procurement tasks were completed and documented.	040103
Validate and reconcile outstanding tasks for financial closure.	040104
Submit final warranty certificates to the end user or owner.	040105
Complete end of project turnover training for security system users and owners.	040106
Coordinate installation team-to-service team handover meeting with owners of installed security systems.	040107
Incorporate maintenance and service requirements in service level agreements (SLAs).	040108
Perform financial, administrative and contractual closure.	040109
Management Skills	050000
Management Skills	050100
Implement best practices for performance management, coaching and developing project teams.	050101
Implement time management principles.	050102
Demonstrate effective verbal and written communication skills.	050103
Implement effective conflict management strategies.	050104
Manage projects within the project management triangle of constraints (i.e., project scope, project schedule and project budget).	050105
Embody the SIA Code of Ethics and adhere to it in all situations.	050106

Appendix II – Certification Agreement

When an applicant signs the CSPM application form, they are legally attesting to the fact that they have read and will abide by the Certification Agreement below.

I certify that all information contained in my application to the Security Industry Association (SIA) for the Certified Security Project Manager (CSPM) examination is true and accurate to the best of my knowledge. Further, I agree to notify SIA promptly of any change in name, address or contact information or in the event of any occurrence bearing upon my eligibility for certification, including but not limited to any criminal conviction or disciplinary action by a licensing board or professional organization.

I hereby authorize SIA and its officers, directors, employees and agents (“the above-designated parties”) to review my application, contact employers and/or references listed on my application and determine my eligibility for examination and certification. I agree to cooperate promptly and fully in this review, including submitting any documents or information deemed necessary to confirm the information in my application. I authorize the above-designated parties to communicate any and all information relating to my application, examination or certification status and review thereof, including but not limited to the pendency or outcome of disciplinary proceedings, to state and federal authorities, employers and others.

I have read and understood SIA’s instructions and policies related to the application and examination process and agree to abide by the terms. If any statement made on my application or hereafter supplied to SIA is false or inaccurate, or if I violate any other rules or regulations of SIA, I acknowledge and agree that the penalties for doing so include denial of certification or suspension, revocation or placement of limitations upon my certification (if already granted). I agree to indemnify and hold harmless the above-designated parties for any action taken pursuant to the rules and standards of SIA with regard to this application, the CSPM examinations I take and/or my certification, except claims based upon gross negligence or lack of good faith by SIA.

Should my application be accepted and I am allowed to sit for the CSPM examination, I understand that SIA and/or its testing agents reserve the right to refuse my admission to test if I do not have the proper photo identification or if I do not report at the appropriate time. If I am refused admission for any of these reasons or if I fail to appear at the test site as scheduled, I will not receive a refund of the examination fee and there will be no credit transferred to future examinations. I recognize that the proctor(s) at my assigned test site are required to maintain proper and secure test administration conditions (which may include direct observation or closed-circuit cameras), and I will follow their instructions. I will not attempt to communicate in

any way with other examinees or any outside parties during the examination. I will not bring any outside materials into the testing site, including reference materials, notes, photographic or communication devices or calculators. I understand that the content of the CSPM certification examination is copyrighted and is the property of SIA. Exam materials will be provided to me for the sole purpose of testing my competencies for which I seek certification, and I am prohibited from using or possessing examination content for any other purpose or at any other time. I agree not to disclose, publish, copy, reproduce, transmit or distribute exam content, in whole or in part, in any form or by any means, for any purpose without express prior written authorization from SIA. Any unauthorized possession, disclosure, publication, copying, reproduction, transmission or distribution of CSPM exam content or materials in any form is prohibited and may subject me to civil liability and/or criminal prosecution.

SIA reserves the rights to cancel any examination score if, in its professional judgment, there is any reason to question the score's validity. Candidate conduct which warrants score cancellation may include, but is not limited to: consulting study aids of any type during a testing session; copying from notes or from another examinee during a testing session; speaking or otherwise communicating with others during a testing session; copying, photographing, transcribing or otherwise reproducing test materials; removing test materials from the examination room; aiding other examinees or receiving aid from anyone else; or having improper access to CSPM examination content prior to the examination administration. Engaging in such misconduct may disqualify me from all future CSPM tests and from ever being certified by SIA. Significant score increases upon retesting may also be investigated to ensure the authenticity of results.

Should I be granted CSPM certification, I agree that SIA may release my name and the fact that I have been granted certification. I agree further that SIA may include my name and contact information in a listing of certified individuals available to the public in print and/or electronic format. I understand and agree that it will be my responsibility to maintain my status by complying with all SIA certification and recertification standards and procedures.

I understand that all notices pertaining to the examination, and to any subsequent certification I may earn, will be sent to my email address of record. CSPMs are required to keep SIA informed of updates to their contact information as a requirement of certification. Changes to contact information may be submitted through the SIA offices. In no instance will any contact information (including telephone, email or mailing address), financial information of any type or any personal information be disclosed other than verifying certification. I understand that SIA's primary method of communication with its credential holders and members is via email and that should I opt out, block SIA's email communications or fail to update my record of changes in email address, I may not receive critical information concerning my examination, certification, continued education requirements and status, recertification and related matters.

In such instances, I become solely responsible for contacting SIA to obtain such information that is critical to maintaining my certification in good standing.

I accept full responsibility for maintaining the CSPM credential through recertification, shall remain current in the field and shall continuously uphold the Code of Professional Ethics. I acknowledge that "Certified Security Project Manager" and "CSPM" are registered trademarks of SIA and that I am authorized to use these designations only so long as the certification has not expired, been suspended, revoked or voluntarily relinquished or converted to the "inactive" status. I understand that violating the Code of Professional Ethics could lead to suspension or revocation of my CSPM certification. I also understand that if my certification lapses or is revoked for any reason, I will no longer be authorized to use the CSPM designation.

BY TAKING THE EXAMINATION, YOU ARE AFFIRMING BY YOUR ACTIONS THAT SIA HAS YOUR PERMISSION TO CONTACT YOU ON MATTERS RELATING TO YOUR EXAMINATION AND CERTIFICATION, AND YOU UNDERSTAND THE TERMS HEREIN THIS CERTIFICATION AGREEMENT AND YOUR INTENT TO BE BOUND BY THE TERMS AND CONDITIONS SET FORTH ABOVE.

Appendix III – Code of Ethics

In addition to satisfying the educational and experiential requirements established above, the CSPM Candidate must agree to abide by the Security Project Manager Code of Professional Ethics to earn the CSPM certification. The Security Industry Association (SIA) sets forth this Code of Professional Ethics to guide the professional and personal conduct of its certification holders. CSPM certification holders shall:

- Hold paramount the safety, health and welfare of the public
- Act for each employer or customer as faithful agents or trustees
- Maintain the highest standard of personal and professional conduct
- Support the implementation of and encourage compliance with appropriate standards and procedures for the effective management of security projects and technology, including the installation, implementation, control, monitoring and risk management of each project
- Perform duties with objectivity, due diligence and professional care, in accordance with professional standards
- Serve in the interest of stakeholders in a lawful manner while maintaining high standards of conduct and character and not discrediting the profession or SIA
- Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority – such information shall not be used for personal benefit or released to inappropriate parties
- Maintain competency in the field of security project management and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence
- Provide accurate, truthful information and representations concerning qualifications, experience and performance of work.
- Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results
- Refrain from engaging in activities for inappropriate personal gain at the expense of customers, their companies or the profession
- Be accurate and truthful in all dealings with customers and be careful not to misrepresent the quality, availability or ability of his/her services
- Support the professional education of stakeholders in enhancing their understanding of the management of security projects
- Serve all members of the public impartially, providing no special privilege or substandard service based upon age, race, national origin, color, gender or handicapping condition
- Cooperate with SIA concerning ethics violations and the collection of related information

Failure to comply with this Code of Professional Ethics can result in an investigation into a certification holder's conduct and, ultimately, in disciplinary measures.