



International Management Research
and Technology Consortium – LLC - USA

CCSMP CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL



www.imrtc.org



consortium@imrtc.org

Bridging The Gap Between
Academia and The Industry
Worldwide!

JOIN NOW



CONTENTS

INTRODUCTION.....	2
ABOUT CCSMP	2
CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL (CCSMP).....	2
AUDIENCE	2
THE CREDENTIALS	2
PRE-REQUISITE:	2
PROFESSIONAL BENEFITS OF PROGRAM	2
PROGRAM STRUCTURE	2
PROGRESSION OF THE PROGRAM	2
AWARDING OF PROFESSIONAL CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL	2
COURSE CONTENTS	2
DOMAINS AND TASKS	2
KNOWLEDGE AREAS	2
ASSESSMENT OF PROGRAM (ONLINE/PHYSICAL)	2
EVALUATION AND GRADING	2
CCSMP ELIGIBILITY REQUIREMENTS	2
REGISTRATION AND PAYMENT PROCESS	2
REGISTRATION PROCESS	2
IMRTC EXAMINATION SYSTEM	2
PARTNER INSTITUTE INTERNAL EXAMINATION SYSTEM	2
IMRTC ONLINE EXAM SYSTEM	2
FEE STRUCTURE	2
TERMS & CONDITIONS RELATED TO EXAMINATION AND CERTIFICATION	2
PROCESS OF CERTIFICATION	2
EXAM CONTENT PERCENTAGE	2
CONTACT DETAILS	Error! Bookmark not defined.

JOIN NOW

Published by

International Management Research and Technology Consortium

IMRTC

Principal Office: P. O. Box 409, 9300 Conroy Windermere, Windermere, FL-34786, USA,

All rights reserved. "imrtc", the imrtc logo, "IMRTC", the CCSMP logo, CCSMP, CCSMP logo
"IMRTC", "and the IMRTC USA are registered marks of IMRTC, LLC.

The IMRTC is a trademark of the IMRTC, LLC.



JOIN NOW

CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL (CCSMP)

INTRODUCTION

There is a global demand for an industry with highly competent Cyber Security Management Professionals. The perspective of cyber security is approaching the organizations very differently, where to improve the cyber security of the organization. IMRTC recognizing the need and in consultation with senior executives and professionals & approved trainers has come up with a comprehensive certification program.

In this respect, IMRTC domain Experts designed a comprehensive training certification, which can provide facilitation to the professionals and also provide the structure to maintain and manage the Cyber Security Management System in the organization. Therefore, with the consultation of senior executives and professionals, and trainers have come up with a comprehensive certification program. **CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL (CCSMP)**

ABOUT CCSMP

CCSMP prepares a Cyber Security Management generalist who will be able to help the organizations maintain the efficiency level as well as to improve the organizational cyber security by giving the inputs to the strategic level. The framework and process will help to grow the organization.

The Certified Cyber Security Management Professional covers all the aspects of Cyber Security Management by using versatile International standards and frameworks and prepares the candidate for real-time cybersecurity engagements as well as practices and purposes. The certification assists and prepares you for the best standards.

The certification ensures that the individuals are fully aware of and follow the Professional Code of Conduct, and will be equipped with the cyber security knowledge and understanding of global standards. Understand business process development & re-engineering requirements, Business & Artificial Intelligence with Data Analysis, Information security systems and electronic equipment integration with information systems, change management systems, portfolio and project management, financial budgeting for Internal Auditing, Global Cyber Security Management and service management through technology and more content is available for learning and development. The program follows a systematic learning format with standards and guidelines, audio-visual aids, and case studies with real-time applications.



JOIN NOW

CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL (CCSMP)



AUDIENCE

People who are involved in cyber or information security or like to develop their career in the field of cyber security management may join this program. The program is available for whom, who have completed 12th grades accredited study program from any discipline from any Board or University.

THE CREDENTIALS

The candidates who are looking to have appropriate knowledge and understanding of cyber security with the requirements of global industry will earn the Certification of Cyber Security management from IMRTC. The program also a self-develop project base on any case study which can be provided by accredited any partner training institute or trainer of IMRTC of 40 Professional Training Hours (PTH).

The program also requires a self-developed project on any case study provided by an accredited training institute or trainer. The project must be in soft form and submitted to our concerned training partners or chapters for assessment. After approval, the candidate can sit in the final examination of IMRTC.

After passing the certification examination the candidates can use this credential CCSMP– Certified Cyber Security Management Professional after their names.

PRE-REQUISITE:

- 12 Years Education or equivalent or Baccalaureate, Associate's degree, or the global equivalent diploma is required to join this session.
- 14 Years Education people have not required any professional experience
- One year Professional Experience is required to opt this program

A grayscale image of a city skyline, featuring several tall buildings and skyscrapers, serves as the background for the bottom section of the page.

JOIN NOW

CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL (CCSMP)



PROFESSIONAL BENEFITS OF PROGRAM

For Individuals

- Career advancement into Cyber Security roles.
- Improved understanding of how to align cyber security principles according to International standards with business goals.
- Recognition as a certified expert in Cyber Security Management.
- Using of technologies in Cyber Security with the business methodologies
- Developing skills of Cyber Security, Governance, Compliances, Risks and Gap Analysis, & International Principles, Standards, Frameworks and Guidelines,

For Organizations

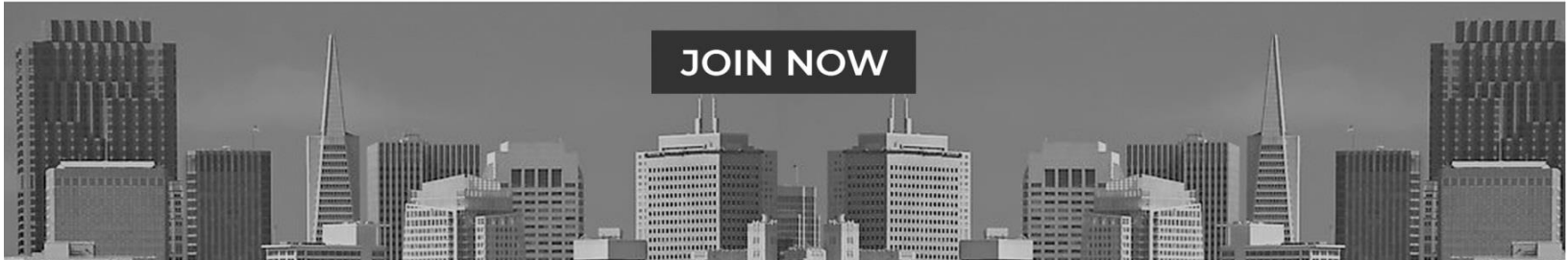
- Assurance of certified professionals with industry-recognized skills.
- Strengthened your strategy with cyber security capabilities.
- Enhanced ability to adopt and integrate with latest methodologies of emerging technologies effectively.

A grayscale image of a city skyline, featuring several tall buildings and skyscrapers, including the Transamerica Pyramid. The image is used as a background for the 'JOIN NOW' button.

JOIN NOW

PROGRAM STRUCTURE

Total Domains	8
Lectures	Lectures can be delivered through partners and trainers
Accredited Trainers	Can Deliver the lectures
One Credit Hour	10 Learning Hours
Total Credits Required	4 Credit Hours
Registration Process	Register through our partners / Trainer
Assessment	Online / Paper based
Passing Criteria	70 percent



PROGRESSION OF THE PROGRAM

Total Credentials	=	4 Credit Hours
One Credit Hour	=	10 Learning hours
Final Assessment	=	Online or physical assessment shall be taken by the IMRTC Examination Department

AWARDING OF PROFESSIONAL CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL

After getting 70 percent marks from the examination, the candidate will be awarded the Certified Cyber Security Management Professional from IMRTC USA.



JOIN NOW

COURSE CONTENTS

Certified Cyber Security Management Professional cover theory, process, and International practices for Cyber Security Management, Governance, Risk and Compliances.

Domain 1: Introduction to Cybersecurity Management

Domain 2: Cybersecurity Governance and Compliance

Domain 3: Risk Management and Assessment

Domain 4: Information Security Frameworks

Domain 5: Incident Response and Business Continuity Planning

Domain 6: Security Architecture and Design

Domain 7: Cyber Threat Intelligence

Domain 8: Cybersecurity Program Leadership

A grayscale image of a city skyline, featuring several prominent skyscrapers, including the Transamerica Pyramid. The image serves as a background for the 'JOIN NOW' button.

JOIN NOW

DOMAINS AND TASKS

In this document, you will find an updated structure for the IMRTC Standard Examination Content. Based on Experience Consultants and stakeholders, we have devised and simplified the format so that the IMRTC Examination System can be easier to understand and interpret.

The domain and task are well-defined on the following pages:

Domain: Defined as the high-level knowledge area that is essential to the practice of CCSMP – Certified Cyber Security Management Professional.

Tasks: The underlying responsibilities of the Cyber Security Management within each domain area.

CCSMP examination will include all tasks for a domain and will adhere to the percentage of coverage at the domain level as outlined in the further pages.

**JOIN NOW**

KNOWLEDGE AREAS

DOMAIN 1: INTRODUCTION TO CYBERSECURITY MANAGEMENT	
Task 1	<p>Understanding of Cyber Security Fundamentals</p> <p>Understanding of Standards, Governance Risk and Compliance</p> <p>Understanding of Frameworks</p> <p>Importance of cybersecurity in modern organizations</p>
Task 2	<p>Major duties in cyber security fields</p> <p>Role of a cybersecurity manager</p>
Task 3	<p>Overview of cybersecurity frameworks (ISO 27001, NIST, COBIT)</p>



JOIN NOW

KNOWLEDGE AREAS

Domain 2: : CYBERSECURITY GOVERNANCE AND COMPLIANCE	
Task 1	Understanding of Cyber Security Governance Structure Understanding of Cyber Security Governance Methodologies Development of Policies and Procedures of Cyber Security
Task 2	Building effective cybersecurity policies and procedures Implementation techniques of policies and procedure
Task 3	Risk Assessment Risk Analysis Gap Analysis Comparative Statement Statement of Applicability
Task 4	Understanding of International Cyber Security Standards Understanding of International Cyber Security Frameworks Legal and regulatory requirements (GDPR, HIPAA, PCI DSS, etc.)
Task 5	Requirement of Compliance Understanding the importance of compliances Implementing a compliance program Universal Methodologies of Compliance Management System



JOIN NOW

KNOWLEDGE AREAS

DOMAIN 3: RISK MANAGEMENT AND ASSESSMENT

Task 1	<p>Understanding of Risk , Threats and Vulnerability</p> <p>Understanding of Risk Management</p> <p>Identifying and analyzing cyber threats</p>
Task 2	<p>Gap Analysis Techniques and Cyber Security Measures</p> <p>Risk Assessment Techniques in respect of Cyber Security</p> <p>Risk mitigation strategies for Cyber Security</p>
Task 3	<p>Developing a risk management plan for Cyber Security</p> <p>Identification, assessment and treatment plan for Cyber Security</p> <p>Business Continuity Plan for Cyber Security</p>

JOIN NOW

KNOWLEDGE AREAS

DOMAIN 4: INFORMATION SECURITY FRAMEWORKS

Task 1	<p>Understanding of Cyber Security Frameworks</p> <p>Assessment of the organizations & find the best fitted frameworks</p> <p>Comparing frameworks: selecting the best fit for your organization</p>
Task 2	<p>Understanding of the Standards ISO 27001</p> <p>Deep dive into ISO 27001</p> <p>Understanding the Family of ISO 27000 Families</p> <p>Understanding and implementation techniques of ISO 27001 and their Controls</p> <p>Development of the statement of Applicability</p>
Task 3	<p>Understanding of NIST Cyber Security Framework</p> <p>Implementing techniques of NIST Cybersecurity Framework (CSF)</p>

JOIN NOW

KNOWLEDGE AREAS

DOMAIN 5: INCIDENT RESPONSE AND BUSINESS CONTINUITY PLANNING

Task 1	<p>Knowing about the critical function in the organization</p> <p>Make a complete schematic diagram with processes, control and objectives</p> <p>Design a complete incident response plans for each incident</p>
Task 2	<p>Knowing about the critical areas subject to cyber threats, which could be sabotage the major impact to organization</p> <p>Develop a complete disaster recovery plan</p> <p>Devise the a damage assessment format and emergency response plan</p>
Task 3	<p>Understanding the business functions and its criticality</p> <p>Develop a Test plan for any incident</p> <p>Develop a test plan for any disaster management</p> <p>Testing and maintaining business continuity strategies</p>



JOIN NOW

KNOWLEDGE AREAS

DOMAIN 6: SECURITY ARCHITECTURE AND DESIGN

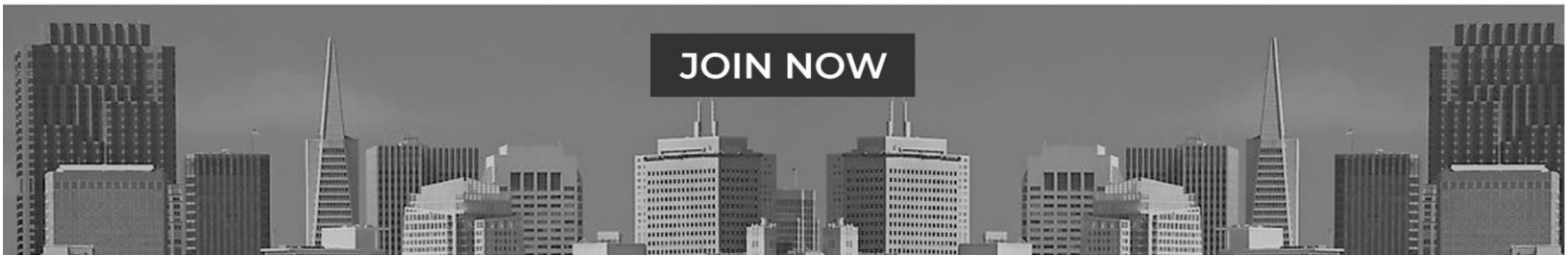
Task 1	<p>Understanding of Security Architecture and Design</p> <p>Understanding of Principles of Secure Network Design</p> <p>Use any case and develop any Security Architecture</p>
Task 2	<p>Understanding Access control management</p> <p>Access Control Models</p> <p>Identification and Authentication</p> <p>Access Control Policies and Enforcement</p> <p>Cryptographic Controls in Network Access Management</p> <p>Network Access Controls</p> <p>Cloud and Remote access Controls</p>
Task 3	<p>Zero Trust Architecture</p> <p>Overview of Zero Trust Principles</p> <p>Key Components of Zero Trust Architecture</p> <p>Network Segmentation</p> <p>Endpoint Security</p> <p>Data Security</p> <p>Security Monitoring and Analytics</p>



JOIN NOW

KNOWLEDGE AREAS

DOMAIN 7: CYBER THREAT INTELLIGENCE	
Task 1	<p>Understanding and threat Intelligence landscapes</p> <p>Intelligence Cycle in CTI</p> <p>Threat Intelligence Sources</p>
Task 2	<p>Threat Intelligence Frameworks and Standards</p> <p>Tools and Platforms for CTI</p> <p>Threat Actor Profiling</p> <p>Indicators of Compromise (IOCs)</p> <p>Threat Hunting Using CTI</p> <p>CTI for Incident Response and Mitigation</p>
Task 3	<p>Monitoring and analyzing security events</p> <p>Leveraging artificial intelligence in threat detection</p> <p>Challenges in Cyber Threat Intelligence</p>



KNOWLEDGE AREAS

DOMAIN 8: CYBERSECURITY PROGRAM LEADERSHIP

Task 1	Developing Leading team for Cyber Security Team management and training
Task 2	Communicating cybersecurity to executive leadership Reporting Formats Monitoring and Securing Methodologies Penetration Testing Report Analysis, Impact and Response Plans Vulnerability Assessment Reports and response Plans
Task 3	Budgeting for cybersecurity initiatives Meeting formats and budget approvals Convincing to higher management regarding cyber security threat and budgets requirements.



JOIN NOW

ASSESSMENT OF PROGRAM (ONLINE/PHYSICAL)

- The exam paper will be online/physical as per the choice of the candidate, but it is preferable to give the exam online.
- The exam paper will cover the above topics domain-wise.
- The Passing marks will be 70%.
- Internal Marks can be adjusted in the final marks through accredited trainers by obtaining prior permission from our Examination Department of IMRTC.
- Those candidates who cannot be able to give online tests due to online facility. So they are allowed paper-based examinations. Otherwise, the partner must arrange the center for the online exam as per the guidelines of the Examination Department
- Assessment will be done according to the domains and tasks mentioned above through our online methodology

EVALUATION AND GRADING

- The student will be examined through exams conducted by IMRTC LLC USA. Total marks for passing the CERTIFICATION/DIPLOMA will be 70 out of 100.

A grayscale image of a city skyline, featuring several tall buildings and skyscrapers, including the Transamerica Pyramid. The image serves as a background for the 'JOIN NOW' button.

JOIN NOW

CCSMP ELIGIBILITY REQUIREMENTS

To be eligible for the Certified Cyber Security Management Professional at any level, the candidates must have a 12-years Education or equivalent with one year experience at least. The candidate should have to submit the credentials

Educational Background	Accredited Training
12 years Education or Equivalent (Baccalaureate, Associate Degree or Global Equivalent)	40 PTH Training must be earned from any accredited trainer or any partner institute
Professional Experience	Certification/Diploma
One year Professional Experience Required	After completing all the formalities and passing the test, will get the certification

REGISTRATION AND PAYMENT PROCESS

REGISTRATION PROCESS

Registration of the program is to be completed through our registered partners and if the partners are not available in your city or country then you can download this registration form and submit the fee in our bank account directly and wait for the email or contact from our Registration or Examination Department. For further information to our examination department contact at registration@imrtc.org.



JOIN NOW

IMRTC EXAMINATION SYSTEM

CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL

PARTNER INSTITUTE INTERNAL EXAMINATION SYSTEM

The concerned partner/institute/trainer will take examinations online and submit to the International Management Research and Technology Consortium Examination Department.

IMRTC ONLINE EXAM SYSTEM

IMRTC will provide access to all partners to schedule the exams of the particular courses of any individual candidates. Therefore, according to the availability, the partner institutes will schedule the exam of individual candidates' subjects or courses/certifications.



JOIN NOW

FEES STRUCTURE

CERTIFIED CYBER SECURITY MANAGEMENT PROFESSIONAL

S. No	Description	Fees
1.	Membership Fee	USD 50
2.	Examination Fee For Members	USD 495
3.	Examination Fee For Non Members	USD 695



JOIN NOW

PROCESS OF CERTIFICATION



To get the certification, 40-Professional training hours as PTH is mandatory from any concerned professional trainer or Partner, and participants should submit their training PTH with the Examination Application Form with the attachments of required qualifications and other experience certificates/letters. The Paper is based on 100 Questions with MCQs of each semester and 70% passing marks are required to pass the exam. Further, if the Project is also included in your exam, marks will be distributed according to course & certification.

TERMS & CONDITIONS RELATED TO EXAMINATION AND CERTIFICATION

- The 40-Training-hours as PTH are valid up to one year.
- If the candidate is failed in the examination then S/he has one more chance to attempt the paper within a year, and if the candidate cannot pass, then they have to pay the examination fee and re-appear in the examination.
- If the candidate cannot pass the examination within one year and after some time S/he would like to appear in the examination then the candidate must resubmit 40 Professional Training hours as PTH again required to appear in the examination.
- The examination system is online and candidate can book the exam anytime according to his or her availability.
- Those countries, that do not have the facility of online examination facility then they can give the paper-based examination, which can be sent to authorized partner/trainers/examiners. The assessment time will be a month and we will send the results to the concerned partner.
- The candidate will get the certificate within one month and the administration will send to the concerned partners.
- To maintain the worth and eligibility in the market, the candidate must have to renew their membership on a yearly basis.

A grayscale image of a city skyline, featuring several tall skyscrapers. The image is used as a background for the 'JOIN NOW' button.

JOIN NOW

EXAM CONTENT PERCENTAGE

The table below prescribes the proportions of examination questions from each section or Knowledge Areas defined above. The exam will be based on multiple choice questions, fill in the blanks and letter writing.

CONTENT	DOMAIN WISE PERCENTAGE
DOMAIN I	10%
DOMAIN II	15%
DOMAIN III	15%
DOMAIN IV	15%
DOMAIN V	15%
DOMAIN VI	10%
DOMAIN VII	10%
DOMAIN VIII	10%



JOIN NOW

CONTACT DETAILS

ADDRESS Principal Office: P. O. Box 409, 9300 Conroy Windermere, Windermere,
FL-34786, USA,

TELEPHONE (+1) (689) 276-4636

Web <https://www.imrtc.org>

EMAIL consortium@imrtc.org

SOCIAL MEDIA ACCOUNT

Facebook <https://www.facebook.com/IMRTConsortium/>

LinkedIn <https://www.linkedin.com/company/imrtc>

YouTube https://www.youtube.com/channel/UCE_GYVI4WJMKIUXQhouA4LA

INTERNATIONAL MANAGEMENT RESEARCH AND TECHNOLOGY CONSORTIUM

USA LLC L24000411080



JOIN NOW