Candidate Handbook 2026

(v26.06.09)

Table of Contents

Introduction

About Global Skills X-Change

Overview
Global Skills X-Change (GSX) is a veteran-owned small business founded in 2003 with more than 20 years supporting workforce, learning, and credentialing initiatives across public and private sectors. Our mission is focused on strengthening workforce and organizational resiliency through credentialing, assessment, and data-informed solutions.

GSX specializes in supporting complex, multi-stakeholder initiatives that seek to professionalize workforces, establish defensible standards, and improve access to education and career advancement. Our work helps organizations address challenges driven by changes in technology, regulation, policy, and professional practice. GSX's core expertise is the application of functional competency models to support workforce management, educational alignment, credentialing, certification, and talent programs that respond to evolving industry needs and support systemic change.

OUR VISION
GSX empowers organizations to future-proof their workforces and improve performance in dynamic environments.

OUR MISSION
We enable organizations to create agile workforces and optimize mission performance.

About Certified Mission Critical Professional (CMCP)

The CMCP certification is a vendor-neutral, industry-developed and maintained, and globally trusted program that serves as the starting point for professionals who operate, secure, and maintain mission critical infrastructure and systems. The CMCP program defines and establishes the standard for knowledge and skills required for anyone operating in a mission critical environment. Obtaining the CMCP certification confirms achievement and helps mission critical professionals establish credibility against an industry standard.

The CMCP exam measures acceptable performance across seven (7) domains:

1.0 Core Mission Critical Concepts
2.0 Risk Management
3.0 Safety, Physical Security, and Cybersecurity
4.0 Change Management
5.0 Operations

6.0 Business Continuity
7.0 Mission Critical System Design

The full CMCP exam blueprint can be found in Appendix A.

Benefits

Benefits of obtaining the CMCP certification include:

For Individuals

- Measures the candidate's understanding and ability to apply the concepts and principles of mission critical operator tasks.
- Promotes professional development which will enhance the candidate's expertise in the mission critical operator field.
- Increases the number of employment opportunities available to the candidate across the mission critical field.
- Provides the candidate with a sense of pride and professional accomplishment.
- Demonstrates the candidate's commitment to the profession.

For Employers

- Provides a reference point for determining which individuals possess the appropriate understanding and ability to apply the facts, concepts, and principles of mission critical functions.
- Promotes the improved synchronization and alignment of individual capabilities with the mission critical profession.
- Serves as an easy identifier for competent professionals within the mission critical discipline.

For the Profession

- Defines standards and drives accountability for all mission critical professionals.
- Documents the mission critical operator essential body of knowledge (EBK) as the professional standard.
- Ensures all mission critical operator professionals have met the established standard through a formal standardized evaluation.
- Establishes an entry point for individuals wishing to pursue a career in the field.

Eligibility Requirement

The CMCP certification is open to any individual seeking to obtain the Mission Critical Professional Certification. However, it is strongly recommended that candidates have a minimum of the following:

- Two-year associate's degree (with coursework in an information technology or operations technology related field, such as engineering), including a minimum of six (6) months (two [2] quarters) of related co-op experience or an equivalent apprenticeship of at least six (6) months; OR
- Two (2) years of related work experience in a field such as information technology, operational technology, engineering, cybersecurity, military, or other mission critical fields; OR
- Any combination of the two totaling two years of experience or education, with a minimum of six (6) months hands on experience.

Non-Discrimination Policy

The CMCP Program does not discriminate on the basis of race, color, national origin, sex (including pregnancy or childbirth), religion, age, disability (physical or mental), sexual orientation, marital status, parental status, political affiliation, genetic information, or retaliate for participating in protected activities. The CMCP Program complies with all applicable jurisdictional laws and regulations related to protection against discrimination in access to CMCP. Additionally, CMCP procedures ensure that all applicants and candidates are treated in an equitable and consistent manner throughout the entire certification process. The eligibility requirements, exam instrument content, exam environment, scoring method, maintenance process, and recertification process provide for a fair, impartial, and bias-free certification program.

How to Register

Individuals interested in obtaining the CMCP certification have the option to purchase the exam only, or a bundle including the exam and the primer e-book. The exam and primer e-book can be purchased at https://www.mccerts.com/store. Payment of an exam and/or the CMCP primer e-book will be collected on the certification store website. GSX offers bundled packages that can include an exam, the primer e-book, and an exam retake. Other bundle packages are listed on the website. Within three (3) business days, an email will be sent with the CMCP primer e-book code and instructions on how to register via the certification management system, Credicycle. Candidates will follow the instructions in (Appendix B) to register for the CMCP exam.

Registration is completed online at https://gsx.assess.com. Candidates will create an account and complete a short application questionnaire. In addition, candidates will be required to

review and electronically sign an agreement regarding the security and confidentiality of the CMCP exam content. Submitted applications will be reviewed and approved by the Mission Critical Certification Program Management Office (MC Certs PMO). Candidates will receive an automated email from Credicycle once their application has been approved.

Candidates will have a window of one (1) year to schedule the CMCP exam before the CMCP exam eligibility expires; if it is allowed to expire, the candidate will be required to pay the exam fee again.

Exam Fees

Exam fees are non-refundable and must be paid prior to taking the CMCP exam. Details of how to register for the CMCP exam register and access the CMCP primer e-book will be emailed to the candidate. The exam fee is required for each attempt of the CMCP exam, whether the candidate has passed, failed, or no-showed for the exam. For specific rates and bundles, please refer to the website: https://mccerts.com/store.

Discounts are available for organizations when buying CMCP exams in bulk for their employees.

For more information, please visit mccerts.com or contact us at mccerts@gsxcorp.com or (703) 662-9830.

Exam Accommodations

If a candidate requires any special accommodations to take the CMCP certification exam, they must contact the MC Certs Program Management Office (PMO) (mccerts@gsxcorp.com) to request those accommodations. The MC Certs PMO will work with testing centers to provide reasonable accommodations in compliance with the Americans with Disabilities Act (ADA).

It is the responsibility of the candidate to seek accommodations in advance of his/her exam date. Candidates must provide verification of the disability and a statement of the specific type of assistance needed to the MC Certs PMO at least 30 days prior to the desired exam date. Requests must be sent to the MC Certs PMO mccerts@gsxcorp.com. It is recommended that candidates requiring accommodations coordinate with the MC Certs PMO in advance of their registration and payment to ensure that the program is going to be able to approve and support the specific accommodation, as last-minute accommodations on the day of testing are not going to be able to be provided, even with the proper medical documentation. The ability to provide a specific accommodation is also based on the capabilities available at the testing center administering the exam for the requesting party.

The MC Certs PMO may request documentation from an appropriate healthcare or rehabilitation professional about a disability and functional limitations when the disability and need for accommodation is not obvious.

Additional fees may apply for exam accommodations; please contact the MC Certs PMO at mccerts@gsxcorp.com for more information.

Candidate Agreement

As part of the exam, candidates are required to read and agree to GSX's Candidate Agreement which states that candidates will not share exam content or any related information with anyone, at any time. The Candidate Agreement must be completed before the individual is allowed to view any exam material. Refusal to sign the candidate agreement will result in a loss of exam fees.

No-Show Policy

Candidates who cannot attend their scheduled CMCP certification exam should reschedule their exam by contacting the Assessment Systems Corporation (ASC) support team (testcenters@assess.com) at least 48 hours before the appointment time. If the candidate has not rescheduled their exam within the 48-hour window prior to the original scheduled exam, or if the candidate is a no-show for the exam, for any reason, the system will record the candidate as a "No-Show."

The candidate must make all efforts to make their scheduled exam date or reschedule their exam at least 48 hours in advance. If the individual is a no-show for two exam iterations, they will not be allowed to participate in the CMCP exam, unless they submit a request with an explanation as to why they were unable to make their scheduled sessions to mccerts@gsxcorp.com. The MC Certs PMO will review the explanation and will notify the candidate of their status to participate in the program within three to five (3-5) business days.

Exam Environment

Current testing can be accomplished either in-person at an Assessment Systems Corporation (ASC) offered test center, or via live remote proctoring with MonitorEDU. Candidates may not bring any of the following items into the exam environment:

- Smartphones/Cell phones
- Laptops
- Hand-held computers or personal electronic devices, including e-readers, tablets, and smart watches

- Calculators
- Tape recorders
- Pagers
- Notes
- Newspapers
- Books
- Bags
- Hats/Coats
- Purses/wallets

If at a physical testing center without a designated secure storage area, candidates may bring the items into the testing room, but the items must be placed in an inaccessible location within the room during the exam.

Candidates are expected to conduct themselves in a professional manner while in the exam environment. Candidates who do not conduct themselves in such a manner are subject to disciplinary action, which can include dismissal from the test center regardless of the candidate's completion of the exam.

Test center proctors and administrators are responsible for monitoring candidates during the administration of the exam and providing instructions regarding taking the exam at the outset of the testing session. Test center proctors and administrators are not allowed to help candidates read or comprehend exam questions. During the administration of the exam, candidates are not permitted to talk to anyone other than a proctor or administrator.

Scoring the Exam

The CMCP exam is electronically scored, and a single overall score is computed. Candidates must earn a score equal to or higher than the pre-determined cut-score to pass the exam. A score report is automatically generated upon completion of the exam which includes a pass/did not pass result, as well as a summary of performance in each of the seven (7) domains covered in the exam. Candidates' scores will be displayed in a graph format that shows how they performed in each area of the exam.

The post exam scores provided are scaled scores. A scaled score is the total number of correctly answered questions converted into a standardized scale. For the CMCP exam, the score is based on a scale ranging from 100 to 800 with a passing threshold of 571 or 576, depending on the version of the exam taken.

Retesting

A candidate who does not pass the CMCP exam on their first attempt will be allowed to retest at their convenience; however, candidates must pay the exam fees in order to attempt the exam again, unless the candidate purchased a bundle package that includes a retake. The exam fees cover one attempt at the CMCP exam, whether the candidate passes or fails. There is a one-day waiting period, as defined as 24 hours after the first attempt exam was started, for starting a second attempt. If the candidate fails the exam a second time, they must wait an additional 90 days to retake the exam, as well as 90 days after each subsequent failed attempt.

If a candidate purchases the CMCP exam and a CMCP exam retake as part of a bundle at https://www.mccerts.com/store, then the candidates initial and retake attempt are covered. If the candidate did not purchase a retake bundle, the candidates must pay the exam fees again to attempt the CMCP exam.

Credential Usage Guidelines

Who Can Use the CMCP Credential?

Certificants are authorized to use the designation “CMCP” or “Certified Mission Critical Professional” once they have received their CMCP digital badge. Certificants may use this credential on business cards, resumes, and signature lines. This designation signifies that they have met the requirements for the Certified Mission Critical Professional Certification. Certificants can use the designation and/or the URL to their BadgeCert page as long as their certification is active. “CMCP” and “Certified Mission Critical Professional” are the only designations approved for use and should appear after a comma following the certificant’s name. No other designator and no other usage is approved by GSX.

Examples of correct use:

- Jill A. Smith, CMCP
- Jill A. Smith, Certified Mission Critical Professional

GSX may also revoke the use of this designation if an individual exhibits signs of misconduct, violation of its policies, or for any reason at any time.

How the CMCP certification is used reflects on their individual brands, GSX, and your organization. To protect the integrity of GSX and its brands, GSX requires that those who use the CMCP certification are authorized users and follow the guidelines and defined herein. By using any of the CMCP certification, you agree to be bound by and comply with the following guidelines.

Authorized User vs. Unauthorized User?

An “authorized user” is deemed as an individual who passed one (1) or multiple GSX certification exams (certificant), received the appropriate digital badge(s), and whose certification status is Active.
An “unauthorized user” is deemed as an individual who never took any of GSX’s certification exams or whose certification status is Inactive.

Proof of Certification

Once a candidate passes an exam, a print-ready certificate will be available in the candidate’s Credicycle account at https://gsx.assess.com. In addition, the candidate will receive a digital badge from BadgeCert to the email address on file.

Digital Badges

Digital badges will be issued to signify the CMCP certification. Candidates will receive access to their CMCP digital badge three to five (3-5) business days after meeting the CMCP exam requirements. Information on how to access and use the digital badge will be provided in an email sent to the certificant. Digital badges are tokens that appear as icons or logos on a web page or other online venue signifying accomplishments, such as a certification or mastery of a skill. GSX will maintain a record of the digital badge with certificant metadata, inclusive of:

- The issuer’s name (i.e., CMCP);
- The certificant’s name and e-mail address;
- A short description of the badge; and
- Other details, such as the issue date and the expiration date, if applicable.

Digital badges are viewable by the certificant and those to whom the certificant provides his/her unique badge URL. The badge serves as proof that the certificant met all of the CMCP program requirements.

GSX will maintain a registry of all certificants who have met the CMCP requirements. Confirmation of an individual’s CMCP status (as Active or Inactive) will be provided to interested parties upon request, but an individual’s score will not be provided.

Use of Credentials

Approved Designations – “CMCP” or “Certified Mission Critical Professional” can be used by a certificant who received a matching digital badge. No other designation nor usage is approved by GSX.

Usage – Certificants may use the credential(s) on business cards, resumes, and signatures.

Status – As long as the certification is active, certificants can use the designation(s) and/or the URL(s) to their BadgeCert page(s).

Revocation – GSX may revoke the use of any designation by written notice if an individual exhibits signs of misconduct, violation of its policies, or for any reason at any time.

Code of Ethics

The CMCP Candidate Code of Ethics Policy ("Code of Ethics") applies to those seeking affiliation with the CMCP Program. This Code of Ethics is a requirement for:

- Individuals who register for the CMCP certification,
- Individuals who obtain the CMCP certification, and
- Individuals who wish to maintain the CMCP certification.

It is a violation of the Code of Ethics for any candidate to participate in any incident of cheating, breach of security, misconduct, submission of fraudulent information, or any other behavior that could be considered compromising the integrity or confidentiality of the CMCP exam. All candidates will adhere to the following:

Candidate Code of Ethics Policy

- All information submitted to participate in the CMCP Program must have been completed by the participating candidate.
- A candidate shall abide by all the terms and conditions set forth in the CMCP Non-Disclosure Agreement (NDA).
- A candidate shall offer and provide professional services with integrity.
- A candidate shall not disclose any confidential client information without the specific consent of the client.
- A candidate will always conduct themselves in a manner which enhances the image of the profession.
- A candidate shall provide services to clients competently and maintain the necessary knowledge and skill to continue to do so in those areas in which they are certified.
- A candidate shall not solicit clients through false or misleading communications or advertisements.
- In the course of performing professional activities, a candidate shall not engage in conduct involving dishonesty, fraud, deceit or misrepresentation, or knowingly make a false or misleading statement to a client, employer, employee, professional colleague, governmental or other regulatory body or official, or any other person or entity.

Appeals Policy

The CMCP Appeals Policy governs the process for reviewing decisions made by the MC Certs PMO about registration, eligibility, exams, or any other registration/exam-related certification issues or challenges.

Grounds for Appeal: An appeal may be filed based on all decisions relating to:

- Candidate registration protocols (that is determination of eligibility).
- Findings by the MC Certs PMO related to alleged cheating, violations of rules of conduct or law, or inaccurate application information.

Decisions Not Eligible for Appeal: Matters not described in "Grounds for Appeal" above are not within the purview of the CMCP and are not appealable to the MC Certs PMO:

- Examination results and/or criteria for obtaining a passing score on the CMCP certification exam.
- Exam content.

Appeals Process: Upon receiving a decision from the MC Certs PMO, a candidate/certificant has up to 15 business to submit an appeal. All appeals must be submitted in writing using the Appeals Request Form to the MC Certs PMO at mccerts@gsxcorp.com. Individuals submitting an appeal must provide their contact information (phone number and email address), specific grounds for appeal, and evidence in support of the appeal.

Appeals Review: The MC Certs PMO conducts a preliminary review of all appeals within five (5) business days of receipt to ensure the appeal is timely, contains all required and pertinent information, and is allowable/meets grounds for appeals. Appeals that are not allowable or are received outside the 15-business day window, will be dismissed without further consideration or review. The candidate will be notified in writing of the dismissal.

Upon receipt of a valid appeals request, the MC Certs PMO shall have 30 business days to review relevant information, request additional information, and decide. The MC Certs PMO may grant or deny the appeal request. The MC Certs PMO shall provide a written response to the individual documenting the basis for the decision.

NOTE: Appeals that require additional information will be referred to the appealing individual to provide further information before a determination on the validity of the appeal is made.

If an individual exhibits signs of misconduct or violation of its policies, such as cheating, breach of security, misconduct, submission of fraudulent information, or any other behavior that could be considered compromising the integrity or confidentiality of the CMCP exam, the MC Certs PMO will notify the individual through a written notice of violations. After a candidate has received a written notice of violations and applicable sanctions from the MC Certs PMO, they will have 30 business days to complete an appeals form for appeal pursuant to Appeals

Process. The candidate must request an Appeals form from the MC Certs PMO. The candidate is then required to complete the appeal form and include a statement describing the grounds for appeal, why the appeal should be granted, and all supporting evidence. A candidate's appeal will not be considered after such a 30-day period has expired.

Reporting Suspected Violations

The MC Certs PMO enforces policies and procedures governing disciplinary action for the CMCP Program. On disciplinary matters, the MC Certs PMO may only address the conferral and certification aspects of the violation and may include loss of the credential, being barred from participation in the program, and possible litigation (depending on the severity of the violation). Unethical or unprofessional behavior may be cause for the MC Certs PMO to deny a candidate's admission to the CMCP Program, to terminate participation at any stage throughout the conferral process, or to invalidate the result of an exam. In the case of a certificant, the individual may have their certification revoked and be barred from re-entry into the CMCP Program for a period of up to two (2) years.

Grounds for disciplinary action include, but are not limited to the following:

- **Cheating:** Cheating is the willing reference to a notebook, workbook, textbook, or other source of information not authorized by the program or exam proctor explicitly; willingly receiving aid, providing aid, or requesting aid from another candidate or certificant; obtaining or attempting to obtain copies of the exam before the administration of the exam; or any act or attempt made with the intent of violating or circumventing the stated conditions governing the administration of an exam.
- **Exam Compromise:** Exam compromise includes those actions that compromise the integrity of the CMCP certification exam, including but not limited to unauthorized possession of or access to real exam questions; copying any portion of a CMCP certification exam (this includes any portion of the exam questions or answers); or the sharing or the receipt of exam information before, during, or after the exam session that gives any tester an unfair advantage over other candidates.
- **Misrepresentation or False Statements:** Misrepresentation is a false or misleading statement or a material omission which renders other statements misleading, with intent to deceive (i.e., claiming to hold the CMCP certification when the certification has not been conferred, or claiming to hold the certification after it has expired but was not renewed in accordance with the CMCP certification exam guidelines. Falsification is the act of deliberately lying about or misrepresenting something.
- **Non-Compliance:** Refusal by the candidate or certificant to comply with their organization's Code of Ethics, standards of conduct, rules, or professional behavior. This particularly includes any violation of any part of their signed CMCP NDA.
- **Request by Company and/or Parent Organization**: If a company and/or parent organization requests a certificant's certification be revoked, the MC Certs PMO may conduct inquiries in direct coordination with the individual candidate's and/or

certificant's employer into suspected violations of the CMCP Certification Disciplinary Policy.

If another CMCP certificant, employer, exam proctor, or other person affiliated with the CMCP Program suspects another certificant or candidate has violated the policies outlined in this handbook, they should be reported to the MC Certs PMO. A Suspected Violation Report form can be found in Appendix D and should be submitted to the MC Certs PMO via email (mccerts@gsxcorp.com). The complainant's name, witnesses, and the content of the complaint will remain confidential, unless legal requirements mandate disclosure. All investigations into suspected violations will be completed within 30 business days.

Contact

For more information, please contact us at:
Email: mccerts@gsxcorp.com
Phone: +1 (703) 662-9830
Web: www.mccerts.com

Appendix A: Exam Blueprint

The table below lists the domains measured and the extent to which they are represented in the exam. The CMCP exam is based on the below domains.

Domain	% of Assessment
1.0 - Core Mission Critical Concepts	15%
2.0 - Risk Management	15%
3.0 - Safety, Physical Security, & Cybersecurity	25%
4.0 - Change Management	5%
5.0 - Operations	21%
6.0 - Business Continuity	10%
7.0 - Mission Critical System Design	9%
Total:	**100%**

1.0 Core Mission Critical Concepts

1.1 Operations technologies and concepts

- Interdependencies and interoperability among key resources such as water, cooling, power, monitoring and control systems, IT, HVAC, and telecommunications
- Availability-Integrity-Confidentiality (AIC)
- The impact of operations technology on critical infrastructure
- Resilience and redundancy
- The measurement of availability
    - The nines of uptime

1.2 Information technologies and concepts

- Confidentiality-integrity-availability (CIA)
- Networking principles
    - TCP/IP addressing Fuel type
    - Protocols
    - Open Systems Interconnection (OSI) model
    - Network topologies
- LAN, WAN, WLAN, VLAN, MAN, and VPN
- The interoperability of systems
- Emerging concepts
    - virtualization
    - cloud
    - data and analytics
    - open source
    - Industrial Internet of Things (IIoT))

1.3 IT-OT convergence and cybersecurity

- Interdependence of:

    - IT systems
    - OT systems
    - 16 DHS Critical Infrastructure Sectors
- Networking of
    - OT equipment
    - Supervisory Control and Data Acquisition (SCADA)
    - Programmable Logic Controllers (PLCs)
    - Distributed Control Systems (DCS)
    - other common OT components
- Legacy systems and gateways and their impact
- Impact of proprietary technologies
    - Industrial wireless networks
    - Laser wireless networks
- IT-OT
    - Collaboration
    - Integration
    - Cybersecurity implications

1.4 Standards and regulations

- Presidential Policy Directive 21 (PPD-21) and the 16 DHS Critical Infrastructure Sectors
- Standards organizations and their focus, including:
    - ASHRAE
    - FIPS
    - ISA
    - ISO
    - IEC
    - IEEE
    - IETF
    - NFPA
    - NIST
    - DoD
    - API
- Standards, including:
    - ISO27001
    - ISO9001
    - ISA/IEC62443
    - FIPS-140
    - NIST
    - Cybersecurity Framework
    - Common Criteria
- Regulatory bodies, including:
    - OSHA
    - EPA
    - FERC

    - NRC
    - DHS
    - DOE
    - PHMSA
    - U.S. DOT
    - NTSA
    - NERC
    - FDA
- Regulations, including:
    - Sarbanes-Oxley
    - PCI
    - HIPAA
    - NERC
    - CIP
    - CFATS
    - NRC
    - FISMA
- Fundamental concepts in:
    - Standards
    - Regulations
    - Compliance

2.0 Risk Management

2.1 Fundamentals of risk management.

- The definition of risk and how risk is measured
- Risk management resources
    - FEMA
    - ISO
    - NIST
    - DHS
- Risk management cycles and strategies
- Risk management components
    - Likelihood/probability
    - Consequence/impact
    - Threat
    - Vulnerability
    - Mitigation/countermeasures/safeguards
    - Hazards
- Quantitative and qualitative risk analysis
- Process hazards analysis (PHA)

2.2 Identification of mission critical assets

- Asset inventories and their importance
- The need for assigning criticality of assets

- Confidentiality, integrity, availability (CIA) and availability, integrity, confidentiality (AIC) and the relative priorities for each asset

2.3 Threat assessment

- Natural and man-made hazards
- Intentional threat attributes, including actors, target, target attractiveness, motivation and probability of action, and capability
- Unintentional threat attributes, including competency, training, and experience
- Sources of threat intelligence and their relative credibility

2.4 Vulnerability Assessment

- Systems vulnerability analysis, including system/process and architecture vulnerability identification
- Physical vulnerability analysis, including site, building, infrastructure, and asset vulnerability identification
- Cyber/IT vulnerabilities, including wired, wireless, physical, portable media and transient electronic devices, vendor, and hosts
- Physical vulnerabilities
- Penetration testing techniques, including social engineering, phishing, USB drops
- Compliance gap assessment

2.5 Risk Assessment

- Risk assessment methodologies
- Required preparatory information, including processes, plans, procedures, and drawings
- Roles and responsibilities when performing a risk
- assessment
- Identification of risks and hazards
- Risk prioritization

2.6 Risk management plans

- Risk disposition strategies (mitigate, accept, remove, or transfer)
- Risk remediation and exception
- Allocation of resources
- Impact of regulations and business operations interdependencies

3.0 Safety, Physical Security, and Cybersecurity

3.1 Occupational safety

- Standards, regulations, and guidelines, including NFPA, IEC, and OSHA
- Activation of local response resources
- The importance of lock-out/tag-out procedures
- The importance of personal protective equipment (PPE)
- The importance of safety orientation/training
- The importance of job safety analysis (JSA)/job hazards
- analysis (JHA)

- The importance of safety data sheets (SDSs)
- Fire safety
- Electrical safety
- Hazardous material identification system (HMIS)
- Hazardous area classification
- Hazardous operations (HAZOPs) (e.g., confined space, working at heights)

3.2 Public Safety

- Incident priorities (life safety, incident stabilization, and property preservation)
- Incident impact or consequences internally and externally
- The importance of communicating with safety organizations during an incident (escalation path)
- Where to find and how to use local, state, and federal public safety resources

3.3 Process/Functional safety

- The importance of safeguards and their application (e.g., safety relief devices, safety interlocks)
- Hazardous process controls
- Safety integrity levels (SILs)
- Process/functional safety standards and regulations (e.g., IEC 61511, IEC 61508, OSHA PSM)
- Process hazards analysis (PHA)

3.4 Environmental Safety

- The importance of EPA Risk Management Program (RMP) regulations
- Safe handling and disposal of materials
- Emissions, discharges, and loss of containment monitoring

3.5 Physical Security

- Access control
- Intrusion detection
- Intrusion prevention
- Incident response

3.6 Cybersecurity

- Cybersecurity risks to mission critical operations (e.g., social engineering, insider threat, targeted attacks)
- Cybersecurity Frameworks: identify, protect, detect, respond, and recover
- Standards, frameworks, and regulations relating to cybersecurity
- (ISA-62443, NERC-CIP, CFATS, NIST SP800, NIST, Cybersecurity Framework, DOD 8500, ISO 2700x, FIPS, Common Criteria, and NSA PL-x)
- Data integrity and security (at rest and in motion)
- Defense in depth

- The importance of cybersecurity hygiene, including access control, malware prevention, system hardening, and patching
- The importance of network and system monitoring, intrusion detection, and prevention

4.0 Change Management

4.1 Planning for change management in IT and OT environments

- The justification for change
- The impact of change
- Implementation window, duration (outage time), and back-out triggers
- The importance of change review and approval (stakeholders, peer)
- Testing (pre- and post-implementation)

4.2 Change management process

- Change execution, including emergency, design, process, configuration, upgrade, and workflow
- Document management (version/revision control)
- How validation and verification (V&V) applies to the document change process

5.0 Operations

5.1 Standard operating procedures (SOPs)

- The importance of SOPs
- The differences between industry standards and proprietary SOPs
- SOP version control
- Response to SOP errors or omissions
- The elements of a procedure

5.2 Troubleshooting, repair, and restoring functions

- Troubleshooting methodologies
- Separation of duties/responsibilities
- Critical versus non-critical repair procedures
- The impact of recovery point objectives (RPOs), recovery time objectives (RTOs), and service level agreements (SLAs) on troubleshooting activities
- The impact of restoration

5.3 Infrastructure monitoring, alerting, and response

- Logging and auditing
- Intrusion detection system (IDS) and intrusion prevention system (IPS) concepts
- Network and component monitoring concepts and tools (e.g., SNMP, NetFlow)
- Physical infrastructure monitoring, including power, temperature, humidity, etc.
- Uninterruptable power supply (UPS)
- Differences among events, alarms, alerts, and notifications
- Event matrix (false positives and false negatives)
- Event/alarm correlation
- Alarm management

5.4 Process control, monitoring, alerting, and response

- Setpoints and calibration
- Basic control principles, including open/closed loop control and proportional-integral-derivative (PID)
- Difference between digital and analog signaling
- Field sensors and actuators
- Fieldbus protocols, including industrial Ethernet variants
- Human-machine interfaces (HMIs) and operator interface
- terminals (OITs) and the role of the operator
- Historians
- Real-time control requirements
- Control technology (e.g., PLC, DCS, SCADA)
- Safety instrumented systems (SIS)
- Protection systems
- Differences among events, alarms, alerts, and notifications
- Event matrix (false positives and false negatives)
- Event/alarm correlation
- Alarm management
- Operations and maintenance key performance indicators (KPIs)

5.5 Audit and maintenance

- Mitigation implementation
- Backup and patch management and upgrades
- Malware
- Physical environment maintenance
- Software and network tool maintenance
- Periodic testing
- Auditing and monitoring
- System baselines and normalization

5.6 Asset life cycle and resource management

- Life cycle phases (provisioning, commissioning, support, decommissioning, retention, or disposal)
- Obsolescence planning and forecasting
- Resource accountability
- Critical resource allocation

6.0 Business Continuity

6.1 Planning, training, testing, and approval

- The purpose and content of a business continuity plan/Continuity of Operations Plan (COOP)
- The identification of essential functions and resources (i.e., business impact analysis)
- The prioritization of essential functions and resources (i.e., order of operations)
- The importance of resilience, contingency response, and recovery
- The importance of business continuity training

- The need for testing and post-testing analysis of the business continuity plan
- Approval process

6.2 Incident response

- Implementation of the business continuity plan/Continuity of Operations Plan (COOP)
- Incident command system (ICS)
- The tiered support response structure
- Regulatory/compliance reporting requirements
- Communications requirements to and from stakeholders
- Closed-loop tracking of incidents
- The need for post-incident analysis

6.3 Disaster recovery

- Implementation of the business continuity plan/Continuity of Operations Plan (COOP)
- Roles, responsibilities, and levels of authority
- Communications
- Logistics
- Recovery objectives and order of operations based on recovery goals (i.e., RTO/RPO)
- Root cause analysis (RCA)/after action report (AAR)

6.4 Emergency management

- The phases of emergency management in the mission critical environment (i.e., prevent, protect, mitigate, respond, recover)
- Roles, responsibilities, and levels of authority (e.g., NIMS)
- Logistics
- Public safety communications

7.0 Mission Critical System Design

7.1 Process control networks

- Elements of process control networks
- Network isolation and segmentation
- Device communications

7.2 Network design

- Equipment selection
- Cabling standards
- TCP/IP and open systems interconnection (OSI) model
- Routing concepts and protocols
- Designing for redundancy
- Different network topology design options
- IP addressing
- Wired and wireless networks
- Network, host, and server operating systems
- Network software diagnostic tools

- Dataflow security, integrity, and reliability
- Remote access vs. local access design
- Logging information from critical devices
- Integration of different critical networks
- Bandwidth management

7.3 Physical infrastructure

- Electrical and mechanical support and fire suppression systems (e.g., HVAC, water, gas, compressed air)
- Controlled access and physical security
- Designing for redundancy
- Designing for catastrophic events
- Interdependence of critical infrastructure

Appendix B: How to Register for the CMCP Exam

To apply to take the CMCP exam, candidates must complete the two-step registration process as outlined on the following page.

The CMCP exam is delivered via two delivery methods: 1) in-person at a test center or 2) via remote proctoring with MonitorEDU. More information about both options are provided here. GSX uses Credicycle as the certification management system, which is where candidates will create an account and complete the online registration.

Note: Prior to completing the steps outlined on the following page, candidates will need to purchase their exam via https://www.mccerts.com/certifications. All payment is collected outside of the Credicycle system.

More information about payment, registration, and test taking can be found in the program candidate handbooks and on the GSX Credicycle FAQ page.

Application Instructions Steps

Step 1 - Create an Account with Credicycle

1. Visit https://gsx.assess.com/dashboard
2. Click “Sign-Up” in the top right-hand corner of the screen.
3. Fill out the contact information form (Name, phone number, email address, password, confirm password) and select “CMCP” from the “Select Institution” drop down menu.
4. Click “Sign up”.

Step 2 - Requesting Eligibility for CMCP Application

1. Log into Credicycle.
2. Click on click “Store”.
3. Select “Learn More” next to the CMCP delivery method you are choosing (e.g., CMCP Test Center or CMCP Virtual Proctoring via MonitorEDU).
4. Click “Request Eligibility”.
5. Complete the application.
6. Click “Send Request” once the application is complete.
7. Once you’ve submitted your eligibility request, notify the MC-Certs PMO (mccerts@gsxcorp.com) who will review and approve the application.

Once your eligibility has been approved:

- **If taking the exam at a test center**, candidates will receive a separate email from the Assessment Systems Corporation (ASC) team requesting three options of their preferred date/time/location. The ASC team will coordinate with the test centers and send a confirmation email with the appointment details.

- **If taking the exam via virtual proctoring with MonitorEDU**, candidates do not schedule an appointment to take the exam, rather they can connect to an on-demand proctor at any time they desire to take the exam. The exam day preparation instructions for MonitorEDU are provided below.

Exam Delivery Methods

The Certified Mission Critical Professional (CMCP) certification exam is offered via two different delivery methods.

Method 1 – Test Centers:

Candidates have the option to take an exam in-person at a physical test center. Prior to selecting this delivery method, candidates should review the available test centers to determine if there is one within an appropriate proximity to their location.

If taking the exam at a test center, candidates will receive a separate email from the Assessment Systems Corporation (ASC) team requesting three options of their preferred date/time/location. The ASC team will coordinate with the test centers and send a confirmation email with the appointment details.

Method 2 – Virtual Proctoring:

Candidates have the option to take an exam via virtual/remote proctoring from their home. This option is offered through MonitorEDU.

If this delivery method is preferred, candidates who select to take their exam via MonitorEDU do not schedule an appointment to take the exam, rather they can connect to an on-demand proctor at any time they desire to take the exam. The exam day preparation instructions for MonitorEDU are provided below.

CMCP MonitorEDU Preparation Instructions

Before Exam Day

- **Watch the Prep Video.**
- **Download Google Meet app** to your mobile device (free, usually pre-installed).
- **Practice mobile setup** – Phone/tablet must show you, your workspace, and computer screen. Keep the device plugged in and charging (extension cord if needed).

On Exam Day

Room Setup

- Quiet, well-lit room; no one else present.
- Only allowed materials or items on the desk (allowed per your organization).
- No headsets or extra devices may be used during your proctoring session.

Connect on Your Computer

- Go to: ascproctor.com and select your organization GSX (Global Skills X-Change)
- Review rules & tutorial video.
- Fill in your information
- Take a photo of your ID and yourself.
- Click **Open Chat → Start Chat** to receive your Google Meet code from the proctor.

Join Google Meet on Your Phone

- Open Google Meet app.
- Enter code from proctor.
- Tap **Join** and allow camera/mic access.

Just Before the Test

- Proctor will ask for a room scan using your mobile device to inspect your work area
- Position the phone to the side so the proctor can see you, your desk, and your screen.
- The proctor will give the next steps to connect webcam and screenshare.
- The proctor will ask to see and inspect any allowed materials.
- Follow proctor's instructions to launch your exam.

During the Test

- No talking unless reporting a technical issue.
- Stay in view and keep the phone connected for the entire test.
- No unauthorized materials or websites.
- No breaks allowed.

If Disconnected

- Stay calm, keep working on the exam.
- Try to refresh/rejoin Google Meet.
- If out for 5+ minutes, connect to backup chat support.

End of Exam

- Always verbally alert your proctor you have finished, show exam submission, tear notes or erase whiteboard, and complete the check-out steps with your proctor before disconnecting.

Appendix C: Reporting Suspected Violations

Certified Mission Critical Professional Appeal Request Form

Name:			
Employer:			
Work Address:			
City/State/Zip:			
Employer:		**Work Telephone #**	
Work Email:		**Employer POC:**	
Employer POC Email:		**Employer POC Phone #**	
REASON FOR APPEAL			
Date of appealable event:			
☐ **Examination Results**		☐ **Certification disciplinary matters**	
☐ **Candidate Registration/Eligibility**		☐ **Test-Taking Protocols**	
☐ **Decisions related to alleged cheating, alleged violation of professional rules of conduct, or inaccurate information on the application form**			
Explain the basis of the appeal. (Limit 1,000 words; continue writing on back of page if needed)			
Attach all pertinent documentation with the initial submission so your appeal can be properly reviewed. (Please indicate the type of documentation submitted – check all that apply.			
☐ **Score Report**		☐ **Disciplinary Violation Report**	
☐ **Medical Form**		☐ **Alleged Cheating Defense**	
☐ **Complaint Form**		☐ **Other**	
ACTION TAKEN (For MC Certs PMO Only)			
☐ **Approve the appeal**			
☐ **Reject the appeal:** ☐ **Insufficient ground for appeal** ☐ **Missed deadline for appeals submission**			
☐ **Return – Incomplete information in the appeals submission**			
Comments:			

MC Certs PMO Signature: _____ Date: _____

Appendix D: Reporting Suspected Violation

Certified Mission Critical Professional Suspected Violation Form

Subject Name:			
Subject Employer:			
Subject Work Address:			
City/State/Zip:			
Employer POC Email:		**Employer POC Phone #:**	
Reporting Official Name:		**Work Telephone #:**	
Work Email:		**Employer POC:**	
REASON FOR Violation			
Date of violation event:			
☐ **Cheating**		☐ **Misrepresentation or false statements**	
☐ **Exam compromise**		☐ **Non-compliance**	
☐ **Revocation request by the certificate's company and/or parent organization**			
Explain the basis of the violation. (Limit 1,000 words)			
ACTION TAKEN (For MC Certs PMO Only)			
☐ **Violation confirmed; revoke certification**			
☐ **Violation not confirmed**			
☐ **Return – Incomplete information in the report**			
Comments:			

MC Certs PMO Signature: _____ Date: _____