



GLOBAL SKILLS X-CHANGE



Candidate Handbook

2026

(v26.06.09)

Table of Contents

INTRODUCTION	3
ABOUT GLOBAL SKILLS X-CHANGE (GSX)	3
ABOUT CERTIFIED MISSION CRITICAL OPERATOR (CMCO).....	3
BENEFITS	4
ELIGIBILITY REQUIREMENTS.....	5
NON-DISCRIMINATION POLICY	5
HOW TO REGISTER.....	5
EXAM FEES	6
EXAM ACCOMMODATIONS	6
CANDIDATE AGREEMENT	7
NO-SHOW POLICY.....	7
EXAM ENVIRONMENT	7
SCORING THE EXAM	8
RETESTING.....	8
CREDENTIAL USAGE GUIDELINES	9
CODE OF ETHICS	11
APPEALS POLICY	12
REPORTING SUSPECTED VIOLATIONS.....	13
CONTACT INFORMATION	14
APPENDIX A: EXAM BLUEPRINT	15
APPENDIX B: HOW TO REGISTER FOR THE CMCO EXAM.....	27
APPENDIX C: APPEALS FORM	31
APPENDIX D: REPORTING SUSPECTED VIOLATION.....	32

Introduction

About Global Skills X-Change (GSX)

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 changes.

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 Operator (CMCO)

The CMCO 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 data center systems. The CMCO program defines and establishes the standard for knowledge and skills required for anyone operating in a data center environment. Obtaining the CMCO certification confirms achievement and helps data center operators establish professional credibility against an industry standard.

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

- 1.0 Mission Critical Infrastructure
- 2.0 Safety, Security, and Emergency Response
- 3.0 Critical Productions Space
- 4.0 Facility and System Documentation
- 5.0 Networking and Communications

- 6.0 Real-Time Information Management
- 7.0 Operations and Procedures

The full CMCO exam blueprint can be found in [Appendix A](#).

Benefits

Benefits for obtaining the CMCO 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 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 Requirements

The CMCO certification is open to any individual; however, it is recommended that an individual have one (1) year of formal training or hands-on experience.

Non-Discrimination Policy

The CMCO program does not discriminate based on 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 CMCO program complies with all applicable jurisdictional laws and regulations related to protection against discrimination in access to CMCO. Additionally, CMCO 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 CMCO have the option to purchase the exam only, or a bundle to include the exam and the CMCO refresher course that assists candidates in preparing for the exam. The exam and refresher course can be purchased at <https://www.mccerts.com/store>. Payment of an exam and/or the CMCO refresher course will be collected on the [mccerts.com](https://www.mccerts.com) certification store website. GSX offers bundled packages that can include the exam, the refresher course, and an exam retake. Other bundle packages are listed on the website. Upon submitting payment, candidates will receive a link to the CMCO refresher course and instructions on how to register via the certification management system, Credicycle. Candidates will follow the instructions in ([Appendix B](#)) to register for the CMCO 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 CMCO 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 CMCO exam before the CMCO 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 CMCO exam. Details of how to register for the CMCO exam and access the CMCO refresher course will be emailed to the candidate. The exam fee is required for each attempt of the CMCO 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 CMCO 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 CMCO 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 and ensure all proper documentation is in-place at least 30 days before the exam date. Candidates must provide verification of the disability and a statement of the specific type of assistance needed to the MC Certs PMO. Requests must be sent to the MC Certs PMO mccerts@gsxcorp.com.

NOTE: 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.

Any 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 CMCO 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 CMCO exam, unless they submit a request with an explanation as to why they were unable to make their scheduled sessions to mccerts@gsexcorp.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 a candidate is 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 CMCO 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 CMCO exam, the score is based on a scale ranging from 100 to 800 with a passing threshold of 555.

Retesting

A candidate who does not pass the CMCO 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 CMCO exam, whether the candidate passes or fails. There is a one-day waiting period, defined as 24 hours after the first attempt exam started, before 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 CMCO exam and a CMCO 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 CMCO exam.

Credential Usage Guidelines

Who Can Use the CMCO Credential?

Certificants are authorized to use the designation “CMCO” or “Certified Mission Critical Operator” once they have received their CMCO 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 Operator Certification. Certificants can use the designation and/or the URL to their BadgeCert page as long as their certification is active. “CMCO” and “Certified Mission Critical Operator” 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, CMCO
- Jill A. Smith, Certified Mission Critical Operator

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 CMCO 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 CMCO certification are authorized users and follow the guidelines and defined herein. By using any of the CMCO 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 CMCO certification. Candidates will receive access to their CMCO digital badge three to five (3-5) business days after meeting the CMCO 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., CMCO);
- 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 CMCO program requirements.

GSX maintains a registry of all certificants who have been conferred the CMCO certification. Confirmation of an individual's CMCO 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 – “CMCO” or “Certified Mission Critical Operator” 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 their credential(s) on business cards, resumes, and signatures.

Status – As long as their certifications are 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 CMCO Candidate Code of Ethics Policy (“Code of Ethics”) applies to those seeking affiliation with the CMCO Program. This Code of Ethics is a requirement for:

- Individuals who register for the CMCO certification
- Individuals who obtain the CMCO certification
- Individuals who wish to maintain the CMCO 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 to the integrity or confidentiality of the CMCO exam. All candidates will adhere to the following:

Candidate Code of Ethics Policy

- All information submitted to participate in the CMCO Program must have been completed by the participating candidate.
- A candidate shall abide by all the terms and conditions set forth in the CMCO 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 CMCO 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 CMCO and are not appealable to the MC Certs PMO:

- Examination results and/or criteria for obtaining a passing score on the CMCO 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 CMCO 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 CMCO 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 CMCO 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 CMCO 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 CMCO certification exam, including but not limited to unauthorized possession of or access to real exam questions; copying any portion of a CMCO 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 CMCO 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 CMCO 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 CMCO 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 CMCO Certification Disciplinary Policy.

If another CMCO certificant, employer, exam proctor, or other person affiliated with the CMCO 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 Information

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 CMCO exam is based on these objectives:

Domain	% of Assessment
1.0 - Mission Critical Infrastructure	21%
2.0 - Safety, Security, and Emergency Response	14%
3.0 - Critical Production Space	14%
4.0 - Facility and System Documentation	12%
5.0 - Networking and Communications	5%
6.0 - Real-Time Information Management	17%
7.0 - Operations and Procedures	17%
Total:	100%

1.0 Mission Critical Infrastructure

1.1 Compare and contrast various types of HVAC systems.

- Refrigerant-based cooling system
 - Air cooled chiller
 - Water cooled chiller
 - Direct Expansion (DX)
 - Pump refrigerant
- Water-based cooling system
 - Pumping systems
 - Primary/secondary
 - Variable primary
 - Cooling tower
 - Heat exchanger
 - Thermal storage
- Alternative technologies
 - Thermal wheel cooling
 - Free-air cooling
 - Air side economization
 - Geo-thermal cooling
 - Evaporative cooling
- 100 percent (%) fresh air technology
 - Exhaust methodology
- Fan systems
- Air handling unit
 - Dedicated outdoor air handling unit
 - Rooftop unit
- Terminal devices

- Fan Powered Terminal Units
- Variable Air Volume

1.2 Summarize various power source technologies.

- Utility
 - Multiple source / multiple feed
 - Low vs. medium voltage systems
 - Switching / fail over
- Generator
 - Standby vs. continuous vs. prime ratings
 - Fuel type
 - Fuel oil
 - Natural gas
 - Automatic transfer switch
 - Paralleling switchgear
- Uninterruptible Power Supply (UPS)
 - Double conversion
 - Line interactive
 - Delta conversion
 - Rotary UPS
 - Diesel Rotary UPS
 - Flywheel
 - Load bus synchronization
- Battery
 - Lithium
 - Lead Acid
 - Flooded wet-cell
 - Valve Regulated Lead Acid (VRLA)
 - Nickel Cadmium (NiCad)
- Alternative power sources
 - Fuel cells
 - Solar panels
 - Wind
 - Co-generation
 - Super capacitor

1.3 Compare and contrast various power distribution concepts and equipment.

- Level of redundancy
 - N
 - N+1
 - 2N
 - 2(N+1)
- Dual cord
- Close transition vs. open transition vs. soft loading
 - Static transfer switch
 - Automatic transfer switch
 - Breaker pairs
 - Soft loading closed transition switch
- Tier level/Topology
 - Tier I (Basic)
 - Tier II (Redundancy)
 - Tier III (Concurrent maintainability)
 - Tier IV (Fault tolerance)
- Electrical protection
 - Grounding
 - Over current
 - Protective relays
 - Surge protection / Transient Voltage Surge Suppressor (TVSS)
 - Lightning protection
 - Arc flash protection
 - Zone selective interlock

1.4 Identify basic plumbing concepts and the relationship to core mechanical systems.

- Water treatment
 - Blow down
- Humidification
- Water source
 - Municipal
 - Water storage
 - Reclamation
 - Well
- Floor drains
 - Trap primers
- Make up water
- Water pumps / pressurization
- Natural gas piping
- Backflow preventer
- Filtration

1.5 Explain life safety system elements, their purposes and impact on normal operations.

- Fire detection
 - Fire alarm
 - High sensitivity smoke detection
 - Smoke and heat detection
 - Flame/flash detection
 - Fire alarm control panel
 - Beam detector
 - Laser
- Fire suppression
 - Sprinklers
 - Wet pipe
 - Drypipe
 - Mist
 - Fog
 - Pre-action
 - Double interlock
 - Single interlock
 - Clean agent
 - Fire extinguishers and types
 - Foam system
- Fire-rated construction
 - Walls
 - Doors
 - Dampers
 - Shutters
 - Penetrations
- Fire pump system
 - Jockey pumps
 - Primary pumps
 - Secondary pumps
 - Transfer switch/controls
- Emergency lighting
- Emergency receptacle identification
- Emergency Power Off (EPO)

2.0 Safety, Security, and Emergency Response

2.1 Given a scenario, implement proper safety techniques in a mission critical environment.

- Personal Protective Equipment (PPE)
- Lock out/Tag out
- Barrier/boundaries
- Machine guarding
- Fall protection and arrest
- Arc flash labels and hazard analysis
- Global Harmonization System
- Confined space access and ventilation

2.2 Given a scenario, execute security methods and best practices.

- Physical security
 - Gates
 - Vehicle barriers
 - Locked doors
 - Special industry classifications
 - Penetrations
 - Access Control Vestibule (e.g. mantrap)
 - Intrusion detection
 - Intercom or radio system
 - Video surveillance
- Access control systems
 - Biometrics
 - Card readers
 - Keypad
 - Key lock

2.3 Identify basic emergency response procedures.

- Incident reporting
- Call tree
- Building or critical area emergency action plan
 - Mass notification methods
- Hazardous material spill procedure
 - Refrigerant leak
 - Fuel leak
 - Battery electrolyte leak
- Severe event preparation and reporting
 - Inclement weather event
 - Internal/external site event
 - National/Regional event
 - Natural disaster

3.0 Critical Production Space

3.1 Explain the importance of common items and best practices that affect various critical environments.

- Component redundancy within the critical space
- Raised access floor
 - Loading
 - Bridging
 - Ramps
- Rack layout/installation
 - Power cabling
 - Labeling
 - Rack power distribution
 - Rack placement
 - Rack cooling
- Best practices
 - Blanking panels
 - Ensure integrity of space
 - Return air plenum
 - Supply air plenum
 - Room envelope
 - Cleanliness
 - Dust
 - Cardboard
 - Pallets
 - Power load balancing
 - Phase balance
 - Redundancy balance
- Alternative technologies
 - Fluid cooled processors
 - Direct Current (DC) power
 - Alternate voltages
 - Compact server cabinets (all-in-one)
- Grounding
 - Signal reference ground grid system
 - Rack grounding
 - Cable tray grounding and bonding
 - Master ground bus bar

3.2 Explain air flow management techniques and strategies.

- Computer room air conditioners / computer room air handler unit
- In-row cooling
- Containment
- Perforated tile placement
- Tile removal limitations
- Return air methodologies
- Hot aisle/cold aisle
- Thermal considerations
- Temperature / pressure control strategies

3.3 Summarize data cable management techniques and cable types.

- Types
 - Fiber
 - Copper
 - Coaxial
 - Category 3 (CAT3)
 - Category 5e (CAT5e)
 - Category 6a (CAT6a)
- Labeling
- Bend radius limitations
- Cable segregation
 - Power, data and fiber
- Cable dressing and placement
- Cable tracing and testing

4.0 Facility and System Documentation

4.1 Compare and contrast various types of record documentation (“as-built”).

- Single line diagram / One line diagram
 - Electrical
 - Mechanical
 - Plumbing
 - Fire protection
- Panel schedules
- Submittals
- Flow diagrams
- Floor plans
- Equipment layout plans
- Equipment schedules
- System architecture diagrams
 - Networking
 - Building Management System (BMS)/ Building Automation System (BAS)/ Supervisory Control and Data Acquisition (SCADA)
- Control diagrams

- Design specifications

4.2 Interpret and explain the contents of various operating and maintenance (O&M) manuals and their associated purpose.

- Shop drawings
- Sequence of operations
- Warranty information
- Seasonal operation
- Preventative maintenance procedures and schedules
- Maintenance procedures
- Troubleshooting procedures

4.3 Identify the contents and purpose of testing reports.

- Commissioning reports
 - Electrical testing reports
 - InterNational Electrical Testing Association (NETA)
 - Functional Performance Testing
 - Integrated System Testing
- Short circuit, protective device coordination, arc flash study
- Testing, adjusting and balancing reports

5.0 Networking and Communications

5.1 Identify basic networking concepts.

- Basic IP address concepts
 - Private vs. public
 - Numbering schemes
- Domain Naming Service (DNS) concepts
- Network types
 - Corporate networks
 - Building management networks
 - Special purpose networks
 - Supervisory Control and Data Acquisition (SCADA) transmission networks
 - Fire system network
 - Programmable Logic Controller (PLC) / Direct Digital Control (DDC) control networks

5.2 Identify essential networking structures and their purpose.

- Components
 - Router/switch
 - Patch panel
- Locations
 - Manhole / duct bank
 - Service entrance / demarcation point (demarc)
 - Communication room / service closet

- Main Distribution Frame (MDF) / Intermediate Distribution Frame (IDF)

5.3 Identify various types of communications systems.

- Wired systems
 - Plain Old Telephone Service (POTS)
 - Private Branch Exchange (PBX)
- Wireless systems
 - Radio system
 - Microwave
 - Satellite
 - Cellular
 - Distributed Antenna System (DAS)
 - Wireless Fidelity (Wi-Fi)
 - Wireless Access Point (WAP)

6.0 Real-Time Information Management

6.1 Explain the fundamentals of environmental and system monitoring.

- Critical production environmental conditions
 - Static pressure
 - Humidity
 - Temperature
 - Air flow
- Systems and equipment parameters
 - Water flow
 - Leak detection
 - Moisture detection
 - Indoor air quality
 - Hydrogen concentration
 - Outdoor ambient environment
 - Weather station
 - Corrosion monitoring
 - Battery monitoring
- Metering
 - Power
 - Utility / generator power
 - Conditioned power
 - Branch circuit power
 - Power Distribution Unit (PDU)
 - Floor (Transformer)
 - Remote Power Panel (RPP)
 - Rack/ Cabinet Distribution Unit (CDU)
 - Outlet
 - Water levels

- Cooling tower basin
 - Make-up water storage
 - Water treatment/chemical levels
- Fuel
 - Fuel level
 - Fuel quality
- Gasses
 - Compressed air
 - Nitrogen
 - Medical gas
 - Natural gas
- Process variables
 - Temperature
 - Pressure
 - Differential Pressure
 - Flow

6.2 Identify common engineering units and conventions.

- Power
 - Kilo-Volt-Ampere (KVA) / Kilowatt (KW)
 - Power factor
 - Power Usage Effectiveness (PUE) / Data center Infrastructure Efficiency (DCIE)
 - Voltage/Current/Frequency
 - Medium vs. low voltages
 - Three phase vs. single phase
 - Alternating Current (AC) vs. Direct Current (DC)
 - Three wire vs. four wire
 - Power density
- Cooling and air flow
 - Ton
 - British Thermal Unit (BTU) / Kilowatt (KW)
 - Gallons per Minute (GPM) / Liters per Minute (LPM)
 - Cubic feet per Minute (CFM)
 - Celsius/ Fahrenheit
 - Head pressure
 - Pounds per Square Inch (PSI)
 - Inches of water column
 - Sensible and latent heat
 - Wet/dry bulb temperature
 - Relative and absolute humidity/dew point
 - Approach temperature
- General measurements
 - Pounds per square foot
 - Pounds per linear foot

- Loading requirements
- Torque
 - Foot – pounds
- Sound / noise
 - Decibels

6.3 Explain common monitoring platforms and controls.

- Platforms
 - Building Management System (BMS) / Building Automation System (BAS)
 - Electrical Power Monitoring System (EPMS)
 - Supervisory Control and Data Acquisition (SCADA)
 - Programmable Logic Controller (PLC)
 - Human Machine Interface (HMI)
 - Meters, gauges and relays
 - Local control systems
- Controls
 - Adjust set point
 - Equipment status
 - On/off schedule
 - Alarm thresholds and reset
- Process control devices
 - Variable Frequency Drive
 - Thermostat
 - Actuator
 - Variable Air Volume
 - Control valves

6.4 Interpret output from system and monitoring reports and explain the overall impact of these reports on a mission critical environment.

- Normal state vs. abnormal state
- Alarm condition
- Trending
- Predictive results
- Mitigate risks/failures
- Integration of information across multiple systems to provide overall status
- Effects of local failures on other mission critical systems
- Verify corrective actions

7.0 Operations and Procedures

7.1 Given a scenario, execute proper change management procedures.

- Restricted change periods / blackout dates
- Maintenance windows
- Switching windows / cutover windows
- Methods of procedures
 - Dry run / testing
 - Switch tag
 - Back-out / contingency plan
 - Tool / materials inventory
 - Pre / post change documentation
- Permit to work / End user approval
- Hot work permit
- Energized work
- Double custody switching (e.g. two-person rule)
- Standard Operating Procedure (SOP), Emergency Operating Procedure (EOP) and Preventive Maintenance (PM)

7.2 Explain common organizational structure concepts.

- Chain of command
- Escalation path
- Organizational chart
- Client - contractor relationships
- Vendor management

7.3 Explain the importance of security procedures.

- Authorization procedures
- Site access rules
- Escorting vendors/visitors
- Material shipping/receiving and inspection
- Security patrolling / fire watch
- Confidentiality policies
- Sensitivity of equipment, information, and mission
- Awareness of cyber security best practices

7.4 Identify general and industry specific regulatory, standard and compliance organizations/associations.

- Uptime Institute
- Occupational Safety and Health Administration (OSHA)
- American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE)
- American National Standards Institute (ANSI)
- Telecommunications Industry Association (TIA)

Appendix B: How to Register for the CMCO Exam

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

The CMCO 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 is 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 “CMCO” from the “Select Institution” drop down menu.
4. Click “Sign up”.

Step 2 - Requesting Eligibility for CMCO Application

1. Log into Credicycle.
2. Click on click “Store”.
3. Select “Learn More” next to the CMCO delivery method you are choosing (e.g., CMCO Test Center or CMCO 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 Operator (CMCO) 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](#).

CMCO 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: Appeals Form

Certified Mission Critical Operator 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 Operator 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: _____