Introductory Exam Guide

Version 1.0

GLOBAL COUNTER-INSIDER THREAT PROFESSIONAL CERTIFICATION

DETER DETECT PREVENT MITIGATE

UNIVERSITY OF MARYLAND 1856
APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

GSX
GLOBAL SKILLS X-CHANGE

Revision History

Version No.	Revisions
1.0	Establishment of the GCITP Introductory Exam Guide.

Table of Contents

REVISION HISTORY 1

INTRODUCTION 3

THE GCITP CERTIFICATION 3

GCITP EXAM OVERVIEW 5

ABOUT THE EXAM 5
EXAM DETAILS 7
CONTENT OUTLINE 8
FEEDBACK 10

PREPARING FOR THE GCITP EXAMS 11

RESOURCES & CONTACT INFORMATION 23

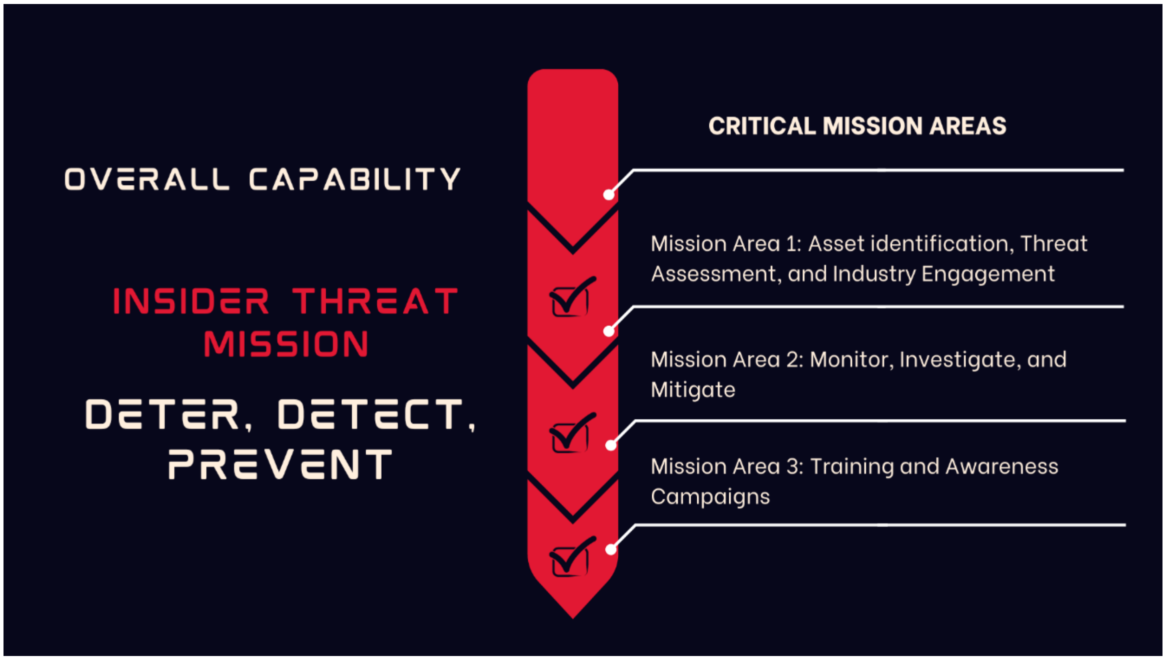
Introduction

The purpose of this Global Counter-Insider Threat Certification Program (GCITP) Introductory Exam Guide is to provide candidates with the information needed to understand the exam process and how to prepare for the GCITP certification exam.

Note: Using this exam guide does not guarantee a candidate will be successful when taking the GCITP certification exam.

The GCITP Certification

By passing the GCITP, a candidate has shown they have the skills and ability to effectively perform Insider threat tasks and demonstrate an overall understanding of insider threats in the workforce. The GCITP was designed for personnel working directly in an insider threat (InT) program and/or performing InT related analysis functions. The GCITP recognizes that the overall InT capability (or mission space) is divided into three (3) primary Mission Areas as depicted in the graphic below:


OVERALL CAPABILITY

INSIDER THREAT MISSION

DETER, DETECT, PREVENT

CRITICAL MISSION AREAS

Mission Area 1: Asset identification, Threat Assessment, and Industry Engagement

Mission Area 2: Monitor, Investigate, and Mitigate

Mission Area 3: Training and Awareness Campaigns

The GCITP covers each of the three Critical Mission Areas. The GCITP places the greatest emphasis on Mission Area 2, as it is where the bulk of the InT analysis occurs, and applied learning may be evaluated.

The GCITP Program splits these three (3) Mission Areas into three (3) exam sections.

Exam Section	% of Exam Content	Exam Scoring
Mission Area 1: Project Management	10	Unscored
Mission Area 2: Program Operations	80	Scored
Mission Area 3: Training and Awareness Campaigns	10	Unscored

Mission Areas 1 and 3 are not scored.

Mission Area 2 is scored because it measures the skills and tasks most central to InT. Mission Area 2 is further broken down into the following three (3) Topic Areas where candidate will receive feedback on their exam performance:

- Program Management – 25%
- Program Operations – 50%
- Documenting and Reporting – 25%

Exam items for Mission Areas 1 and 3 were designed as standard multiple-choice questions targeted at the *Remember* and *Understand* levels within the Bloom's Taxonomy scale. Mission Area 2 of the GCITP exam was designed as a Situational Judgement Test (SJT). SJTs are scenario-based exams that assess the examinee's ability to choose the most appropriate action given a specific work situation. SJTs are designed to assess an individual's ability to *Analyze* and *Apply* multiple knowledge areas within a single question within the Bloom's Taxonomy scale. This feature makes the SJT the ideal exam type for multidisciplinary professions like Insider Threat.

Scenarios for SJTs are developed from real Critical Incidents. Critical Incidents are stories of real work situations that were consequential (for better or worse), where judgment was needed to make an appropriate decision, and which resulted in success or failure in carrying out an important part of the job. There are three main parts of a Critical Incident:

- Setting – the situation or problem
- Behavior – what action was taken
- Result – what outcome occurred

In an SJT, the setting of each Critical Incident is used to develop the scenario in each item. This is combined with a response instruction, such as "what should be done first," to complete the question. The behavior of each Critical Incident, along with other plausible actions, make up each response option. Each Critical Incident's result helps bring context to the situation during the item development process.

GCITP Exam Overview

About the Exam

Candidates are encouraged to use this document to help prepare for the GCITP. (**Note: this exam guide does not mean a candidate will be successful when taking the GCITP certification exam.**) To receive the GCITP certification, you must meet the eligibility criteria and pass the certification exam.

Eligibility Criteria: 4+ years of experience in an Insider Threat (InT) role or related discipline area **AND** 20+ hours of -InT training.

Related Disciplines:

- Human Resources Professionals (I/O Psychologists, HR Generalists, HR Managers; Legal Professionals (J.D., paralegals))
- Security Professionals (personnel security, physical/industrial security, cyber security, information security, operations security, communications security, special access programs, threat assessment and mitigation)
- Counterintelligence professionals; Cyber Professionals (user activity monitoring)
- Law Enforcement Professionals
- Behavioral Science Professionals (social psychologists, forensic psychologists, behavioral psychologists, social workers)
- Risk Management Professionals

NOTE: If you don't see your specific discipline area but believe it should be included as an InT discipline, please reach out to the GCITP Program Management Office (PMO) and ask if your discipline is applicable.

As stated in the introduction, the GCITP exam covers all three (3) Critical Mission Areas with an emphasis on Mission Area 2. Exam items for Mission Areas 1 and 3 are designed as standard multiple-choice questions targeted at the Remember and Understand levels within the Bloom's Taxonomy scale. Mission Area 2 of the GCITP exam is designed as an SJT. SJTs are scenario-based exams that assess the examinee's ability to choose the most appropriate action given a specific work situation. According to the Bloom's Taxonomy scale, SJTs are designed to assess an individual's ability to Analyze and Apply multiple knowledge areas within a single question, making the SJT the ideal exam type for multidisciplinary professions like Insider Threat.

Below are **example questions** for each Mission Area. **NOTE**: (*) signifies the correct answer; these questions are only examples and are **NOT** on the exam.

Mission Area 1: Project Management

Example Multiple-Choice: What must an organization identify and protect first?

Options:

A. (*) Critical assets
B. Existing policies
C. Security controls
D. Building locations

Example Multiple-Choice: Which of the following correctly defines “risk tolerance"?

Options:

A. (*) The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.
B. A structured approach used to oversee and manage risk for an enterprise.
C. Coordinated activities to direct and control an organization with regard to risk.
D. The set of assumptions, constraints, and priorities/trade-offs that shape an organization's approach for managing risk.

Mission Area 2: Program Operations

Example SJT: An alert based on badge records is triggered, indicating that the specified employee is working odd hours, including coming in several hours early and leaving several hours late. Print logs reveal the employee, a member of the communications team, printed a significant number of pages during the odd hours reflected in the badge records. The behavior meets internal thresholds and you open an inquiry.

What should be done first?

Options:

A. Analyze email content when the employee was working odd hours.
B. Contact physical security and request they perform a bag check as the individual is leaving the building.
C. Contact Information Technology and request they suspend the employee's logical access.
D. (*) Recommend Human Resources conduct an interview with the employee's supervisor to see if the work hours were approved.

Example SJT: There has been a power outage, resulting in a delay of user inputs. Once the power is restored, there is a sudden influx of behavior. You notice that a normally manageable insider threat (InT) indicator has excessively high-value results, that if deemed malicious, would have a negative impact on the company and its information.

What should be done to maintain workflow?

Options:

A. (*) Create a customer communication channel to better understand the appetite for risk.
B. Bring in other teams to attempt to handle the InT backlog.
C. Limit network capabilities significantly to catch up with the workflow.
D. Prioritize only the riskiest behaviors for review and mitigation.

Mission Area 3: Training and Awareness Campaigns

Example Multiple-Choice: Which of the following includes proven and effective insider threat messaging campaigns?

Options:

A. (*) Emailing, posters, newsletters, briefings, and training.
B. Posters, briefings, one-on-one meetings, and fireside chats.
C. Public releases, senior leader question & answer, emailing, and training.
D. Newsletters, legal briefs, surveys, and town halls.

Example Multiple-Choice: What can an organization's senior leaders employ to determine progress in achieving program objectives and to identify areas requiring improvement?

Options:

A. (*) Metrics
B. Databases
C. Schedules
D. Spreadsheets

Exam Details

Number of Questions: 124
Types of Questions: Multiple Choice and SJT
Allotted Testing Time: 150 Minutes
Passing Score: 650 or Higher

Candidates will have the ability to navigate freely within the exam and go back and forth from one exam item to the next if they so desire. Once the time limit of 150 minutes is up, any unanswered items will be marked as incorrect.

The GCITP exam is electronically delivered and scored. Four scores are computed with one overall score of a pass or fail with feedback group scores. The GCITP uses a scaled score report to provide candidates feedback on their overall performance on the exam. While the GCITP exam has 124 multiple-choice questions, a candidate's final overall score is only based on the 84 scored questions. The remaining items are unscored and added for piloting purposes. Performance on these unscored questions do not affect a candidate's overall score. Each question (scored and unscored) has only one correct answer that was validated during exam development by a representative group of Subject Matter Experts (SMEs) from the InT Enterprise.

Mission Area 2: Each of the GCITP exam items are directly linked to one of the Accountabilities in the GCITP-Essential Body of Work (EBW).

Mission Areas 1 & 3: Each of the GCITP exam items are directly linked to one of the Accountabilities in the GCITP-Essential Body of Knowledge (EBK).

The GCITP certification exam is a pass or fail exam. The exam is scored against a minimum standard established by professionals who are guided by certification industry best practices and guidelines. Finally, the exam was approved by industry senior leaders to ensure accuracy and relevancy.

Your exam results are reported as a score from 100-800, with a minimum passing score of 650. Your score shows how you performed on the exam as a whole and whether you passed.

Content Outline

This exam guide includes weightings, test areas, and objectives only. It is not a comprehensive listing of all the content on the exam. The table below lists the main content areas and their weightings.

Mission Areas	Percentage of Exam
Area 1: Project Management	25%
Area 2: Program Operations	50%
Area 3: Documenting and Reporting	25%
TOTAL	100%

Mission Area Breakdown

Mission Area 1: Unscored	● Help leadership to identify organizational assets (includes physical, digital, and human resources/products). ● Help leadership define risk tolerance levels. ● Advocate for risk/threat mitigation measures to protect identified assets.

- This is a Senior InT Professional's mission/area of responsibility.
- Inform leadership of potential risks/threats to organizational assets (includes physical, digital, and human resources/products).
- Support leadership to establish risk tolerance levels.
- Work with Red Teams to assess vulnerabilities and mitigation measures.
- Research and keep current on existing and emerging risks/threats to your organization and your organization's market sector.
- Participate in working groups/conferences/external engagements with other insider threat professionals to build strategic relationships, achieve common goals, gain awareness.
- Develop networks and build alliances with other insider threat programs (within the same industry sector and/or cross-industry) to collaborate and exchange information about current threats, trends, and solutions to current insider threat problems (as allowed by your organization).
- Coordinate with leadership and the organization's legal team to determine what information can be shared and with whom.

Mission Area 2 – Scored	
Program Management	**25%**
Program Operations	**50%**
Documenting and Reporting	**25%**

Mission Area 3: Unscored

- Overall goal is to make workforce aware of potential risks/threats to the organization and how to spot and report suspicious behaviors to the C-InT Team.
- Senior Int Program Managers are responsible for developing the messaging, branding.
- Analysts are charged with spreading the message throughout the organization.
- Primary methodologies for delivery include briefings, posters, newsletter updates, and email campaigns.
- Metrics for measuring success include number of departments/individuals met with, briefings delivered, number of incidents reported post briefing/training events occurred, number of investigations opened from those new reports.
- Growing from a C-InT analyst and giving briefings, into a senior C-InT program manager and developing content to brief, is based on a combination of time in the position, exposure, and experience to a

	variety of different case types, and growth in business acumen and corporate/organizational knowledge.

Feedback

A score report will be generated immediately upon completion of the exam. The report includes two sections of information.

Section 1 provides information on a candidate's overall exam performance compared to the passing standard. Candidates are provided the passing standard (known as the performance threshold), their exam score, and a pass/did not pass result. Candidates' exam score and pass/did not pass results are based on their performance on the 84 scored questions only.

Section 2 provides information on candidate performance on the exam's topic areas compared to those who "**meet requirement**" and those who "**did not meet requirement**". To increase the reliability of feedback provided to candidates, topic areas are grouped into the following feedback groups:

- Program Management
- Program Operations
- Documenting and Reporting

Candidates should not view the feedback provided in Section 2 of their score report as definitive due to the small number of questions per section. Rather, candidates should use this as additional information to decide what next steps should be taken for professional development.

Preparing for the GCITP Exams

The GCITP exam is training-agnostic, meaning candidates are not required to participate in any specific course or group of courses to prepare for the exam. Furthermore, the GCITP is not based on, nor measures knowledge of any organization-specific operations or procedures.

Candidates are encouraged to review the tasks listed in the GCITP-Essential Body of Work (EBW) and the information provided for each of the knowledge domains covered in the GCITP-Essential Body of Knowledge (EBK). The GCITP-EBK contains a list of the knowledge areas a practitioner within the InT workforce is expected to possess to perform the tasks identified in the GCITP-EBW.

Essential Body of Work	
Task	Description
Task 1	Identify stakeholder partners and establish priorities
Task 2	Define sustainable methods for detection of irregular and/or abnormal activities and relevant reporting thresholds
Task 3	Define requirements, goals, metrics, and appropriate analytics
Task 4	Apply all relevant government and organization policies and procedures to core insider threat activities
Task 5	Monitor and review technical and non-technical data sources to identify potential insider-related events
Task 6	Perform triage to eliminate false indicators and determine relevance, credibility, probability, magnitude, and imminence of potential threats
Task 7	Identify information gaps associated with potential threats
Task 8	Document and track potential insider-related events and actions in defined platforms/tools
Task 9	Aggregate information and determine appropriate level of escalation
Task 10	Conduct appropriate insider-related investigations and gather additional data needed for analysis and decision making

Task 11	Collaborate with internal and external partners, to gain access to data, expertise, and more effective use of information
Task 12	Analyze, synthesize, and evaluate all data sources to identify insider threats
Task 13	Create and deliver reports, presentations, and briefings for appropriate audiences
Task 14	Support decision makers to determine the best methods for mitigating, transferring, or accepting risk
Task 15	Assess effectiveness and efficiency of insider threat procedures to identify opportunities for continuous process improvement and provide recommendations and refinement based on learnings
Task 16	Support stakeholder by monitoring and assessing the effectiveness for potential mitigation strategies and making recommendations for potential updates
Task 17	Design, develop, and implement techniques and resources that enable the team to operate more efficiently and effectively
Task 18	Consult with stakeholders and senior leadership to influence organizational change, behavior, and results
Task 19	Follow established policies and procedures for closing an inquiry

ESSENTIAL BODY OF KNOWLEDGE

TECHNICAL COMPETENCIES

Technical Competency 1: Policies and Regulations – Complies with and stays current on relevant insider threat guidelines, policies, regulations, and laws.

PR-AoE 1 - Insider Threat Policies	Be familiar with and stay current on relevant insider threat regulations, guidelines, laws, and directives (organizational, local, state, federal, international as appropriate/needed); examples include: • Executive Order (EO) 13587 • National Insider Threat Policy and Minimum Standards • NISPOM Change 2 (CFR Title 32, Part 117) • National Institute of Standards and Technology (NIST)

PR-AoE 2 - Counter Insider Threat Program - Operational Process	Knowledge of and compliance with: • Insider Threat Case Management process • Reporting chain(s) for information sharing, dissemination, and escalation • Insider Threat Program goals and objectives • Concepts and terminologies (e.g., thresholds and priorities, Multi-disciplinary Insider Threat Working Groups, Potential Risk Indicators)
PR-AoE 3 - Privacy and Civil Liberties	Complies with and stays current on relevant privacy and civil liberties protections; examples include: • Ethics and Compliance Policies (e.g., retaliation and whistleblower act(s)) • Health Insurance Portability and Accountability Act (HIPAA) • Equal Employment Opportunity (EEO)/Americans with Disabilities Act (ADA) compliant • General Data Protection Regulation (GDPR) • California Consumer Privacy Act (CCPA) • Payment Card Industry Data Security Standard (PCI DSS) • Federal Trade Commission (FTC) guidelines • Federal Communications Commission (FCC) guidelines • Sarbanes-Oxley Act (SOX)
PR-AoE 4 - Information Protection	Understands and complies with proper handling of sensitive information; examples include information related to: • Privacy and civil liberties • Protection of Personally Identifiable Information (PII) • Information collection & storage limitations • Protection of intellectual property and proprietary information (e.g., Non-Disclosure & Confidentiality Agreements)
PR-AoE 5 - Investigative and Operational Viability	Familiar with the investigative lifecycles related to associated pillars/disciplines and how the insider threat program might provide support (i.e., complies with proper investigative procedures and protocols for preserving chain of custody and integrity of collected information)

Technical Competency 2: Researching – Identifies a need for and knows where or how to gather information. Obtains, evaluates, organizes, and maintains information. Understands the Potential Risk Indicators (PRIs), capabilities, and when to engage with each pillar.	
R-AoE – 1 Counterintelligence Pillar	Understands basic terms of reference, concepts, and principles related to the Counterintelligence Pillar to include: • Foreign Intelligence Entity (FIE) collection priorities, tactics, techniques, and procedures • Potential risk indicators (PRIs) (e.g., contact with foreign nationals, foreign visits, foreign travel, finances, elicitation, polygraph results) • Capabilities, authorities, and jurisdictions of counterintelligence (CI) organizations and/or elements • Reporting and escalation procedures Identifies anomalous behaviors within the Counterintelligence Pillar and knows when and how to engage with relevant counterintelligence professionals who: • Provide detailed risk and threat assessments • Provide CI data in support of Insider threat assessments and mitigation
R-AoE 2 - Cyber Pillar	Understands basic terms of reference, concepts, and principles related to the Cyber Pillar to include: • User activity monitoring (UAM) for data analysis • UAM trigger development • Users, privileged users, and trusted agents • Potential risk indicators (PRIs) (e.g., unauthorized downloads, unauthorized access, sharing credentials, misuse of organizational systems and tools) • Reporting and escalation procedures Identifies anomalous behaviors within the Cyber Pillar and knows when and how to engage with relevant cyber professionals who: • Provide enterprise audit monitoring, audit logs, profile data, printer log data, and download history • Conduct long term analysis of UAM data • Provide cyber data in support of Insider threat assessments and mitigation • Identify users, privileged users, and trusted agents

R-AoE 3 - Human Resources Pillar	Understands basic terms of reference, concepts, and principles related to the Human Resources Pillar to include: • Basic employment records (e.g., disciplinary actions, performance reviews, transfer applications, awards information, timesheet data, leave approvals, corporate credit card data) • Basic employee rights (e.g., EEO, ADA, FMLA, HIPAA) • Potential risk indicators (PRIs) (e.g., changes in employee behavior and/or changes in employee performance, Equal Employment Opportunity issues, workplace complaints, lying about application information (i.e., resume) • Reporting and escalation procedures Identifies anomalous behaviors within the Human Resources Pillar and knows when and how to engage with relevant human resource professionals who: • Provide human resources (HR) data in support of Insider threat assessments and mitigation • Identify the field of work assigned to potential insider threat • Identify minimum access potential insider threat needs to perform their job
R-AoE 4 - Law Enforcement Pillar	Understands basic terms of reference, concepts, and principles related to the Law Enforcement Pillar to include: • Public records (e.g., arrest records, court records, civil actions) • Potential risk indicators (PRIs) (e.g., harassment, making threats, signs of extremism) • Reporting and escalation procedures Identifies anomalous behaviors within the Law Enforcement Pillar and knows when and how to engage with relevant law enforcement professionals who: • Report and/or prevent suspected criminal activity • Provide law enforcement (LE) data in support of Insider threat assessments and mitigation
R-AoE 5 - Legal Pillar	Understands basic terms of reference, concepts, and principles related to the Legal Pillar to include: • Potential risk indicators (PRIs) (e.g., NDA/confidentiality violations, misuse of company systems/resources, finance violations, ethical violations, data handling violations, sabotage

	of company systems, theft) • Reporting and escalation procedures Identifies anomalous behaviors within the Legal Pillar and knows when and how to engage with relevant legal professionals who: • Provide legal data in support of Insider threat assessments, mitigation, and potential prosecution • Provide guidance on legal requirements and boundaries
R-AoE 6 - Social and Behavioral Sciences Pillar	Understands basic terms of reference, concepts, and principles related to the social and behavioral sciences to include: • Psychology of insider threat • The Critical Path Model (e.g., predispositions, stressors, concerning behaviors, organizational responses to concerning behaviors) • Basic behavioral models and psychological profiles to differentiate between normative behaviors vs. anomalous behaviors • Potential risk indicators (PRIs) (e.g., access attributes; professional lifecycle and performance; foreign considerations; security and compliance incidents; technical activity; criminal, violent, or abusive conduct; financial considerations; substance abuse and addictive behaviors; judgment, character, and psychological conditions) • Role of social and behavioral sciences (SBS) in production of Insider Threat products Identifies anomalous behaviors within the Social and Behavioral Sciences pillar and knows when and how to engage with relevant behavioral science professionals who: • Gain a general understanding of what is included and how to interpret mental health data found in workforce vetting forms • Differentiate between behavioral considerations vs. health considerations • Conduct real-time case reviews • Case studies
R-AoE 7 - Security Pillar	Understands basic terms of reference, concepts, and principles related to the Security Pillar to include: • Different types of security and security related policies (e.g., Personnel, Physical, Cyber, Information, Industrial, and Special Access Programs) • Potential risk indicators (PRIs) (e.g., unauthorized access/entry, unauthorized disclosure/leak, other incident

<table>
<tr><td></td><td>reports)
• Reporting and escalation procedures

Identifies anomalous behaviors within the Security Pillar and knows when and how to engage with relevant security professionals who:

• Provide security data in support of Insider threat assessments and mitigation
• Provide guidance on employee eligibility and access to sensitive/protected information
• Interpret background investigation and workforce vetting/suitability data</td></tr>
<tr><td colspan="2"><b>Technical Competency 3: Information Analysis & Synthesis – Identifies anomalous behavior(s) and/or pattern(s) of behaviors; analyzes, interprets, and integrates data (technical and non-technical) or other information; differentiates between primary and secondary sources; evaluates and prioritizes alternatives; and assesses similarities and differences in data to develop findings and conclusions.</b></td></tr>
<tr><td><b>S-AoE 1 - Insider Threat Referral Triage</b></td><td>Conduct insider threat referral triage by compiling, reviewing, interpreting, correlating, and analyzing insider threat referral data to:

• Differentiate between false -positive indicators and true indicators that are potentially indicative of a threat
• Determine relevance, credibility, probability, magnitude (impact), and imminence of potential threat
• Identify known information gaps associated with potential threats
• Develop and recommend referral and analytic strategies
• Document triage activities detailing reasons for referral closure or escalation</td></tr>
<tr><td><b>S-AoE 2 - Insider Threat Trend Analysis</b></td><td>Conduct timely, preventative, and relevant insider threat trend analysis to:

• Identify anomalous behavior/patterns of behavior indicative of an insider threat
• Identify new Potential Risk Indicators (PRIs) thresholds and referral guidance
• Provide direct support to senior leaders and stakeholders for organizational mitigation considerations</td></tr>
<tr><td><b>S-AoE 3 - All-Source Analysis</b></td><td>Understand collection capabilities and reporting cycles from the primary Pillars (e.g., CI, Security, Cyber, HR, SBS, LE) and use a multi-disciplinary approach to:</td></tr>
</table>

	• Gather, integrate, and analyze threat-related information • Leverage open-source intelligence as authorized by local, state, and/or federal regulations and organizational policies • Aggregate and synthesize and place information in context • Identify patterns and trends • Present summary findings in support of insider threat assessments and mitigation
S-AoE 4 - Insider Threat Assessment	Develop threat/risk assessment(s) on a potential insider threat using a multi- disciplinary approach including concepts, principles, and standards related to: • Potential insider threat indicators • Research strategies for an insider threat inquiry • Thresholds for reporting and action • Aggregation and synthesis of all-source data • Risk scores (risk = threat * impact * probability)
Technical Competency 4: Tools and Method – Applies tools and methods to substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for substantive discipline, domain, or area of work. A tool is defined as a physical or virtual device, application, or database used to perform work rather than something that is studied, exploited, or targeted. A method is defined as a structured and repeatable process for carrying out work.	
TM-AoE 1 - Analytical Communication	Support senior leaders, stakeholders, and mitigation activities by providing analytic assessments that incorporate: • Analytic Standards for Analytic Products (e.g., Objective, Independent, Timely, Holistic, Descriptive) • Intellectual Standards (e.g., clear, accurate, precise, relevant, in-depth, logical) • Best practices and challenges of working with multi-disciplinary teams • Strategies to prevent group polarization, group think, and/or artificial consensus
TM-AoE 2 - Critical Thinking and Structured Analytic Techniques	Exercise critical thinking and structured analytic techniques when conducting insider threat activities. Document analytic processes in a clear and understandable method. These techniques include but are not limited to: • Hypotheses/scenario generation • Alternative analysis techniques • Argument mapping

	• Bias elimination (e.g., confirmation, hindsight, foresight, availability, overconfidence) • Occam's Razor • Diagnostic techniques (e.g., Key Assumptions, Quality of Information, Indicators or Signposts of Change, Analysis of Competing Hypothesis) • Imaginative Thinking (e.g., Brainstorming, Outside-In Thinking, Red Team Analysis) • Contrarian Techniques (e.g., Devil's Advocacy, Team A/Team B, High Impact/Low Probability Analysis)
TM-AoE 3 - Databases/Data Feeds, Dashboards, and Analytic Tools	Understand how to access relevant databases/data feeds (e.g., local/national, government, and commercial) and understand the basic functions/capabilities of relevant dashboards and analytic tools to: • Collect relevant insider threat related data • Document and track potential insider-related events and actions • Aggregate information and determine appropriate level of escalation • Conduct trend analysis
Technical Competency 5: Vulnerabilities Assessment and Management – Conducts assessments of individuals and organizational vulnerabilities to identify changes in the likelihood of an insider event, determines deviations from acceptable configurations of enterprise or local policy, assesses the level of risk, and, when appropriate, supports potential mitigation countermeasures.	
VAM- AoE 1 - Counter Insider Threat Program - Organizational Structure	Understand the mission, capabilities, and structure of the organization to: • Support organizational leadership to identify key assets and vulnerabilities • Identify key stakeholders within the organization and their roles in the insider threat process • Create and/or participate in multi-disciplinary Insider Threat Working Groups (formal/informal and/or internal/external) • Support your organization's Insider Threat program model (e.g., Point-to-Point vs. Hub-and-Spokes)
VAM-AoE 2- Individual Risk Assessment	Understand procedures for determining an individual's current level of risk based on the following factors: • Placement and access (e.g., badges and credentials) • Exposure (e.g., clearance levels, administrative privileges) • Influence/seniority • Historical disciplinary actions

	• Performance reviews • Pervasiveness of all factors
VAM-AoE 3 - Insider Threat Mitigation: Individual	Understand how an insider threat or potential insider threat may be impacted (positively or negatively) by individual or organizational mitigation actions; considerations include: • Where the individual falls along the critical pathway • Predispositions, stressors, and concerning behaviors exhibited • Previous organizational responses • Available mitigation options (individual and organizational) Understand and support the implementation of individual mitigation response options – CI, Cyber, HR, LE, Legal, SBS, and Security (e.g., administrative actions, performance counseling, remedial training, compliance mandate, performance improvement plan, employee assistance referral, access suspension and/or downgrades, suspension and/or termination of employment) Monitor and assess the effectiveness and impact of chosen mitigation strategies and report findings to appropriate leaders and stakeholders
VAM-AoE 4 - Insider Threat Mitigation: Organizational	Understand how an insider threat or potential insider threat may be impacted (positively or negatively) by individual or organizational mitigation actions; considerations include: • Where the individual falls along the critical pathway • Predispositions, stressors, and concerning behaviors exhibited • Previous organizational responses • Available mitigation options (individual and organizational) Understand and support the implementation of organizational mitigation response options – CI, Cyber, HR, LE, Legal, SBS, and Security (e.g., changes in policy, processes and procedures, and/or additional education/training/awareness) Monitor and assess the effectiveness and impact of chosen mitigation strategies and report findings to appropriate leaders and stakeholders

ESSENTIAL BODY OF KNOWLEDGE

NON-TECHNICAL COMPTENCIES

Non-Technical Competency 1: Communication – Understands effective and appropriate communication patterns and the ability to use and adapt that knowledge in various contexts.

COM-AoE 1 - Information Sharing	Shares information, as appropriate, with customers, colleagues, and others. Ensures colleagues receive organizational information and recognizes the responsibility and takes action to provide information within the intelligence community, to other federal, state, and local law enforcement or authorities, the private sector, and/or foreign partners, as appropriate.
COM-AoE 2 – Oral Communication	Makes clear and convincing oral presentations. Listens effectively; clarifies information as needed.
COM-AoE 3 – Written Communication	Writes in a clear, concise, organized, and convincing manner for the intended audience.
Non-Technical Competency 2: Collaboration – Implements a working practice whereby individuals, other organizational/office departments, and Insider Threat Programs work together for a common purpose to complete a task or achieve a common goal. Negotiates ~~one's~~ needs to create a shared objective; cooperates and coordinates resources to execute a plan to reach goals.	
COL-AoE 1 - Influencing, Advocating, Negotiating	Tailors presentations to an audience's unique blend of goals, values, and knowledge to persuade others, build consensus through give and take, and gain cooperation from others to obtain information, resources, and/or accomplish goals.
COL-AoE 2 - Partnering	Develops networks and builds alliances; collaborates across boundaries to build strategic relationships and achieve common goals.
COL-AoE 3 - Team Building	Inspires and fosters team commitment, spirit, pride, and trust. Facilitates cooperation and motivates team members to accomplish group goals.
Non-Technical Competency 3: Solution Development – Determines the best way of satisfying requirements for an output by evaluating baseline requirements and alternative solutions to achieve them, selecting the optimum solution, and creating a specification for the solution.	
SD-AoE 1 - Problem Solving	Identifies and analyzes problems; weighs relevance and accuracy of information; generates and evaluates alternative solutions; perceives the impact and implications of decisions; and makes recommendations.
SD-AoE 2 - Systems Thinking	Understands how variables within a system interact with one another and change over time. Applies this understanding to solve complex problems and drive integration.

SD-AoE 3 - Flexibility	Is open to change and new information; rapidly adapts to new information, changing conditions, or unexpected obstacles.
SD-AoE 4 - Creativity & Innovation	Develops new insights into situations; questions conventional approaches; encourages new ideas and innovations; designs and implements new or cutting-edge programs/processes.
SD-AoE 5 - External Awareness	Understands and keeps up to date on local, national, and international policies and trends that affect the organization and shape stakeholders' views; is aware of the organization's impact on the external environment.
Non-Technical Competency 4: Project Coordination – Determines the best way of satisfying requirements for an output by evaluating baseline requirements and alternative solutions to achieve them, selecting the optimum solution, and creating a specification for the solution.	
PC-AoE 1 - Decisiveness	Makes well-informed, effective, and timely decisions needed to execute core insider threat activities even when data are limited, or solutions produce unpleasant consequences.
PC-AoE 2 - Planning & Evaluation	Organizes work, sets priorities, and determines resource requirements; determines short- or long-term goals and strategies to achieve them; coordinates with other organizations or parts of the organization to accomplish goals; monitors progress and evaluates outcomes.
PC-AoE 3 - Customer Service	Anticipates and meets the needs of both internal and external customers. Delivers high-quality products and services; is committed to continuous improvement.
PC-AoE 4 - Accountability	Holds self and others accountable for measurable, high-quality, timely, and cost- effective results. Determines objectives, sets priorities, and delegates work. Accepts responsibility for mistakes. Complies with established control systems and rules.
PC-AoE 5 - Integration	Searches for opportunities to collaborate and actively promotes collaboration on work products and across work domains to enhance the quality of results.

Resources & Contact Information

To register for the exam, please go to the GCITP website at www.gcitp.umd.edu. You can also find more information on registering in the Candidate Handbook at www.gcitp.umd.edu/gcitp-certification/resources.

If you have any questions, please contact the GCITP PMO via email at gcitp@umd.edu or phone at 703-653-0240.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

GSX
GLOBAL SKILLS X-CHANGE