



ATARC Zero Trust Lab Phase 3 – Training Track Use Cases

This document is intended to guide training organizations with developing targeted Zero Trust curriculum and syllabus documentation that addresses onsite, remote, and computer-based training formats. The curriculum should be adaptable to varying organizational roles, including executive leadership, program and project management, as well as operators and deployment personnel, to ensure holistic adoption of Zero Trust principles. Each module's curriculum should include real-world applications, scenario-based exercises, and metrics to assess and help reinforce the principles of Zero Trust.

People, process, and technology are all required for successful Zero Trust adoption and implementation. This lab is the first ATARC Zero Trust lab to focus on the people aspect and is slightly different than a traditional technology demonstration lab. Providers are asked to demonstrate curriculum tailored for each of the training audiences, to include CBT (computer-based training) if applicable. The providers must also demonstrate an understanding of coordinating training for government audiences through use case scenarios.

Scenarios:

Senior Leadership Scenario:

- An executive briefing on the strategic alignment of Zero Trust with the agency's mission focusing on guidance from Executive Order 14028, relevant mandates, and NIST SP 800-207 to help strengthen their cybersecurity posture. The scenario could involve an organization's Zero Trust culture change and how the organization's leadership have responsibility to ensure the successful staff adoption of this security strategy. The scenario should be designed to help leaders understand the alignment of people, processes, and tools to support the integration of Zero Trust across the five pillars (identity, devices, networks, applications, and data) enhancing mission success and protecting critical national assets.

Program Management Office Scenario:

- A program manager creates a detailed roadmap for implementing Zero Trust, following CISA's Zero Trust Maturity Model. The scenario demonstrates the steps required for migrating from perimeter-based security to Zero Trust across the five pillars and two cross sectional functions, highlighting how this proactive approach mitigates security risks, as outlined in NIST SP 800-207.

Tactical and Operational Staff Scenario:

- A practitioner-focused exercise showing how daily operational processes change when implementing Zero Trust, using CISA's Maturity Model as a guide. The scenario includes user authentication, data access, and application security in a multi-cloud environment. Practitioners are trained to continuously monitor and secure systems in compliance with NIST Zero Trust Architecture principles and federal requirements from Executive Order 14028.

Use Cases:

Use Case 1 – A training officer needs to provide Zero Trust Computer-Based Training for employees disbursed across the United States and abroad.

The following assumptions should be applied to this use case:

- All three levels of the training audience (senior leadership, program management, and tactical operational staff) need to be trained.
- Training needs to be available on demand.
- There must be a way to track and access training.
- The user may be operating out of a CONUS or OCONUS location.

- Content should be available in standard LMS formats allowing organizations to import content into their existing Learning Management Systems.
- A web-based LMS platform should also be available for those organizations who would like to have their stakeholders and contractors access training online.
- Training platform and content should be 508 compliant.

Use Case 2 – A training officer needs to provide a Remote Zero Trust training to employees disbursed across the United States and abroad.

The following assumptions should be applied to this use case:

- All three levels of the training audience (senior leadership, program management, and tactical operational staff) need to be trained.
- Training needs to be available to attendees in multiple locations.
- Materials may need to be provided to attendees in advance of scheduled sessions due to limited access.
- Users should be able to access training via phone and online.
- There must be a way to track attendance.

Use Case 3 – A training officer needs to facilitate in-person Zero Trust training.

The following assumptions should be applied to this use case:

- All three levels of the training audience (senior leadership, program management, and tactical operational staff) need to be trained.
- The training organization should be prepared to facilitate training for individuals in a secure or nonsecure environment.
- Handouts and presentation materials may need to go through additional security review before being able to be shared at secure facilities and systems.

Use Case 4 – A training officer needs to facilitate hybrid Zero Trust training

The following assumptions should be applied to this use case:

- All three levels of the training audience (senior leadership, program management, and tactical operational staff) need to be trained.
- Some staff will be onsite, and others will dial in or will be on web conference.
- The trainer needs to ensure that materials can be provided to all attendees regardless of technical access and location.
- The trainer should assume that some attendees will not have access to live internet and web conference content.
Physical training packets may need to be provided to some locations in advance.

