

# Zero Trust Readiness: A Blueprint for Assessment Excellence

This guide details the **Four-Step Zero Trust Assessment Blueprint**, a proven process for evaluating and advancing your organization's Zero Trust (ZT) posture. Built from two years of self- and assisted assessments, this approach helps cut through unknowns, providing executives with clear reporting and technical teams with a precise roadmap, often saving months of planning.

## The 4-Step Zero Trust Assessment Blueprint

The blueprint is designed to build a robust, repeatable, and scalable assessment program, centered around your unique requirements.

Step	Focus Area	Key Deliverable
1	Define Your ZT Framework	A structured, foundational framework with verifiable outcomes.
2	Establish Evaluation Criteria	Clear, quantifiable data points for measuring maturity and progress.
3	Develop the Assessment Toolset	Automated, purpose-built tools for collecting and analyzing assessment data.
4	Roll Out the Assessment Process	A structured plan for communication, piloting, scaling, and support.

### Step 1: Define Your ZT Framework

A successful assessment begins with a well-defined framework that provides structure and measurable targets. This moves ZT from a paradigm shift to an actionable plan.

- **Foundation:** Start by leveraging recognized ZT standards models:
  - **U.S. DoW Zero Trust Strategy and Execution Roadmap**
  - **CISA Zero Trust Maturity Model v2.0**
  - **NIST SP 800-207, Zero Trust Architecture**
- **Structure Components:** For example, the U.S. DoW ZT Model breaks down the ZT strategy into four distinct layers, ensuring every element is measurable and linkable to defensive tools:

Framework Layer	Purpose & Mapping
<b>Pillars</b>	Foundational/High-Level ZT Areas.
<b>Capabilities</b>	Can be mapped to <b>Defensive Cyber Tools/Vendors</b> .
<b>Activities</b>	Can be mapped to specific <b>Tool Features</b> needed for ZT implementation.
<b>Outcomes</b>	Verifiable functions.

**Targeting:** Implement a **Target-Level** approach for all components to achieve a baseline ZT status by a set date, with an **Advanced-Level** for future maturity.

## Step 2: Establish Evaluation Criteria

Define the specific data points collected during an assessment to evaluate ZT implementation status against the framework established in Step 1.

### Criteria for ZT Capabilities:

Data Point	Description
<b>Tools / Vendor</b>	Collect a list of all Defensive Cyber Tools used in your environment to implement ZT.
<b>Tool Linkage</b>	Link ZT Capabilities to specific Defensive Cyber Tool(s) that satisfy it.
<b>Maturity Status</b>	Indicates the tool's lifecycle stage (e.g., Procurement, Fully Integrated).

### Criteria for ZT Activities:

- Maturity Status:** A granular status to show progress over time.
- Outcome Status:** Verification status for all sub-Outcomes (Completed, Partially Completed, Not Completed).
- Written Response:** A description of how the ZT Activity was achieved and how Outcomes are implemented.
- Artifact Upload:** Proof of successful implementation (e.g., screenshots, configuration PDFs, documentation).

### Example Maturity Statuses:

	Maturity	Description
<b>1</b>	Not Applicable (NA)	This activity is not applicable in your architecture.
<b>2</b>	Incomplete	Pending response.
<b>3</b>	Planning	Tools identified but not yet procured.

<b>4</b>	Procured	Tools procured, but no resources allocated for integration.
<b>5</b>	In Progress	Tools procured and implementation is underway.
<b>6</b>	Partially Implemented	Some outcomes achieved (Yes/Partial).
<b>7</b>	Implemented	All outcomes achieved.
<b>8</b>	Inherited	All outcomes achieved through an external provider or cloud service.

## Step 3: Develop the Assessment Toolset

Building a ZT toolset is critical for standardizing data collection and automating analysis.

Toolset Evolution	Current State & Features
<b>Phase 1: Get Started</b>	<b>Spreadsheet-Based:</b> Labor-intensive but crucial for initial flow definition.
<b>Phase 2: Repurpose/Scale</b>	<b>Survey-Based Tool:</b> Repurposing existing survey/data-collection tools for initial <b>Self-Assessments</b> .
<b>Phase 3: Purpose-Built Tool</b>	<b>A dedicated, locally deployable tool built specifically for ZT assessment. Core Features:</b> Data Collection, Automation, and Reporting. <b>Key Benefits: Leave Behind</b> for continuous maturity and a safe environment for testing ZT implementation.

## Step 4: Roll Out the Assessment Process

A structured, phased rollout ensures adoption and success across the organization.

- Communicate:** Initiate technical exchanges and conferences to communicate the assessment process, gather initial feedback, and build buy-in.
- Pilot:** Identify a **High-Value Asset (HVA) organization** or team and conduct an **Assisted Assessment** to refine the process and demonstrate value. This is an investment in early success.
- Scale:** Once the flow is proven, scale in two dimensions:
  - Self-Assessment:** Scale the survey-based ZT Readiness Assessment for bulk assessment volume (can take months per component).
  - Assisted Assessment:** Scale resources/teams for **On-Site Assessments** (streamlined to approx. **one week** for a full engagement).
- Support:** Establish a "**Front Door**" for the program:
  - User Support:** Portal for self-assessment help and assisted assessment requests.

- **Reporting Support:** Team dedicated to **Trend Analysis** and executive reporting to effectively communicate ZT progress up the chain.

## Zero Trust Resource Links

Resource	Link
CISA ZT Maturity Model v2.0	<a href="https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf">https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf</a>
NIST SP 800-207, ZT Architecture	<a href="https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf">https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf</a>
U.S. DoD ZT Strategy	<a href="https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf">https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf</a>
U.S. DoD ZT Execution Roadmap	<a href="https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf">https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf</a>
Microsoft ZT Guidance Center	<a href="https://learn.microsoft.com/en-us/security/zero-trust/">https://learn.microsoft.com/en-us/security/zero-trust/</a>