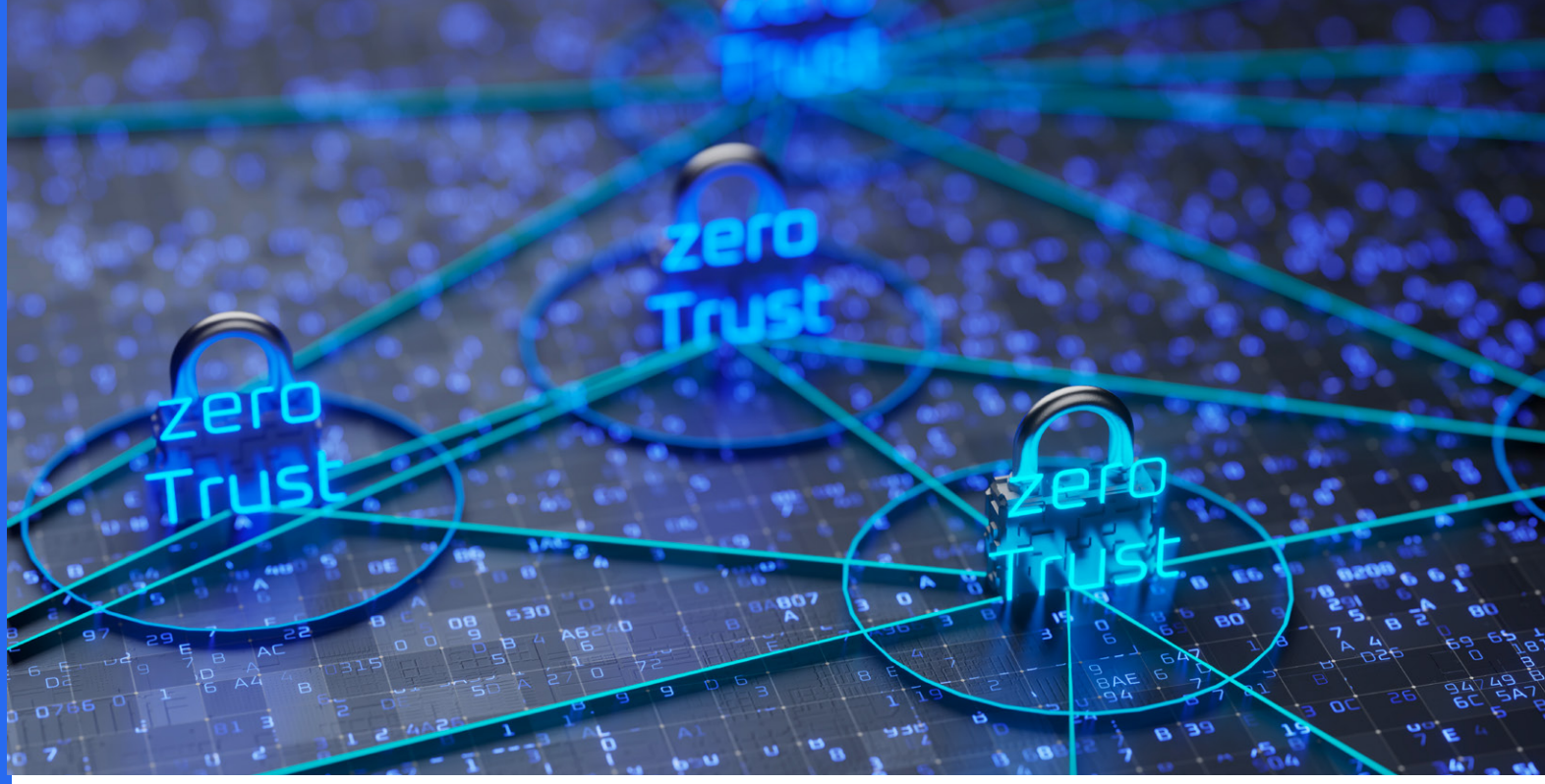
ACUITY
Your Vision | Our Focus

Advance Your Zero Trust Journey with CISA's Maturity Model v2.0

by Sara Mosley & Danny Toler



What's New in CISA's Zero Trust Maturity Model v2.0?

By Sara Mosley and Danny Toler

On April 11, 2023, Cybersecurity and Infrastructure Security Agency (CISA) published its updated **Zero Trust Maturity Model v2.0**. This document represents the first formal update since the ZTMM was issued in September 2021, in response to Executive Order (EO) 14028 "Improving the Nation's Cybersecurity."

Having participated in the evolution of the Zero Trust Maturity Model (ZTMM), we offer observations and insights to help federal agencies put version 2.0 into perspective. Notably, **the model should not be viewed as prescriptive, strict requirements,** but instead as a general guide to help agencies successfully develop and implement their Zero Trust Architecture (ZTA) and adopt a continuous improvement mindset to their cybersecurity posture. The model does not impose specific steps toward a static date of achieving Zero Trust.

It is also important to note that the model encourages **incremental, horizontal progress across all pillars,** rather than vertical progress within select pillars, resulting in optimal protection of the data, systems and services facing the broadest range of threats.

Greater Clarity and a New Stage

There are several key changes to the ZTMM document, starting with the model itself. CISA added a new stage, "Initial," to the maturity model and revised the criteria for each stage. According to CISA, these maturity stages are dynamic, so planned progress from stage to stage may shift in scope over time.

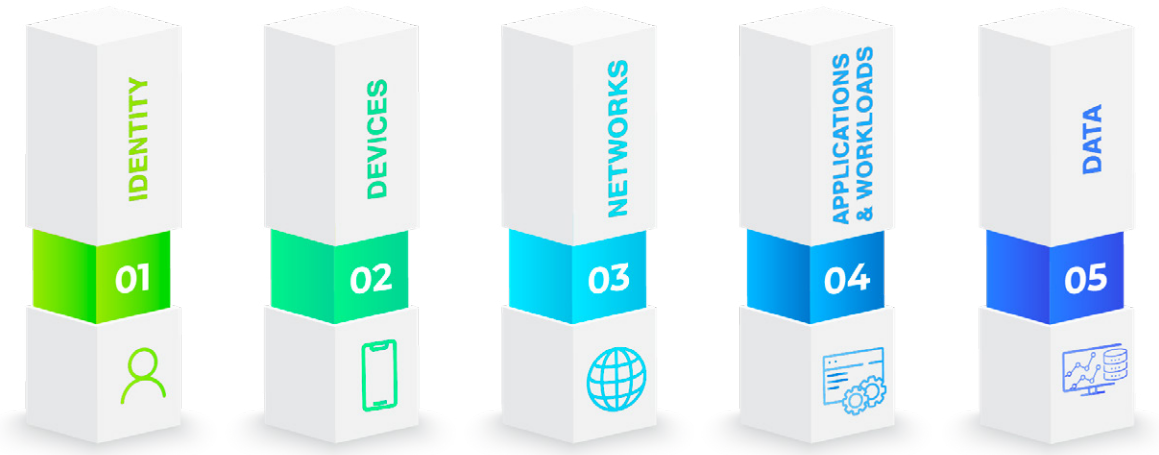
Within each of the ZTMM's five pillars: 1) Identity, 2) Devices, 3) Network, 4) Applications and Workloads, and 5) Data, the ZTTM version 2.0 offers greater clarity through specific descriptions of the **four stages of ZTA—traditional, initial, advanced, and optimal.** These stages help federal agencies assess their current state and better understand what they must do to optimize their ZTA.

Cross-pillar integration is integral to achieving Zero Trust.

CISA has added new and updated functions for each maturity stage. One of the major points emphasized throughout the document is the **need for automated and dynamic processes.** In fact, at every stage of maturity, including initial, automated processes and systems are mentioned as criteria for meeting the maturity goals.

Another key theme is the need for **cross-pillar integration,** starting in the initial maturity stage. CISA states that federal agencies should expect that required levels of effort and realized benefits will significantly increase as Zero Trust maturity progresses across and within pillars. Acuity's experience demonstrates that cross-pillar integration is integral to achieving Zero Trust.

Figure 1: CISA's Zero Trust Maturity Model Pillars



Breakdown of Changes within the 5 Pillars

As stated above, CISA made several changes within the pillars. Here's a quick breakdown:

IDENTITY PILLAR

CISA added **Access Management,** a new function that provides criteria for least privilege and continuous validation of access to resources. This distinction calls out Authorization as a separate function from Authentication, a key to implementing least privilege access.

DEVICES PILLAR

In this pillar, CISA takes a realistic view of the challenges agencies face for both on-premises and cloud asset management of government-owned and personal devices. CISA advises that devices should encompass all virtual and network assets, including end-user and machine-to-machine devices.

There are **three new functions** and one updated function in this pillar. The new functions provide stricter controls and policies for device management to reduce supply chain risk and improve threat protection. The Data Access function was renamed "Resource Access" to better articulate that Zero Trust must be applied to any resource, including but not limited to data.

NETWORK PILLAR

In this pillar, CISA adds **two new functions:** Network Traffic Management and Network Resilience. The former focuses on profiling and managing application traffic to optimize and prioritize resources. It evolves traditional network routing – which was void of any application-aware capabilities – to dynamically profile applications and allow for the prioritization of critical application traffic.

Now that applications are primarily running in the cloud, Network Resilience emphasizes the need for continuous availability to meet the demands of the new environment.

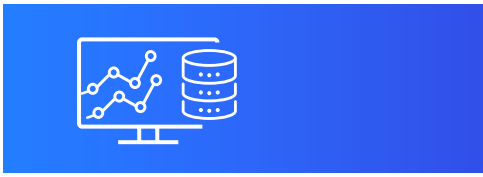
The Encryption function within the Network pillar was renamed Traffic Encryption and now incorporates requirements for full lifecycle key management.

APPLICATION PILLAR

This pillar has one new function: Secure Application Development and Deployment Workflow. The pillar now identifies the criteria for agencies to move towards **immutable workloads,** as directed in OMB M-22-09.

Application Access (formerly Access Authorization), Application Threat Protections (formerly Threat Protections), Accessible Applications (formerly Accessibility), and Application Security Testing (formerly Application Security) are updated with additional criteria required to meet the maturity stage.

DATA PILLAR



CISA added **two new functions** to the Data pillar: Data Categorization and Data Availability. Both functions provide foundational building blocks for the data protection focus of Zero Trust.

5 Steps to Speed Progress toward Zero Trust

Based on our federal agency experience, we recommend the following essential activities to accelerate progress toward achieving Zero Trust, in line with the updated CISA ZTMM.

1 Assess Your Current State Before Diving into Further Investments

Agencies should assess their current enterprise systems, resources, infrastructure, personnel, and processes before investing in new Zero Trust capabilities (including those that address the pillars and functions outlined in this model). This assessment assists agencies in understanding their capabilities that support Zero Trust maturity and identifying gaps.

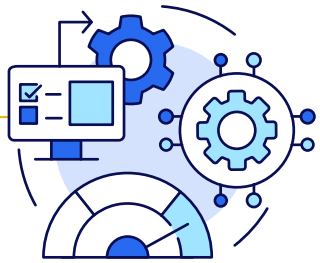
1A. FOCUS ON CRITICAL SYSTEMS AND DATA STORES

We recommend that agencies prioritize their assessment with regard to the state of their most critical systems and/or data stores, i.e., their High Value Assets (HVAs) and systems. Focusing first on these systems provides the highest return on investment and accelerates the protection of the agency's most important assets.

1B. INTEGRATE ALL FEDERAL GUIDELINES

Our approach to performing an effective assessment is to map capabilities relative to all available federal guidelines, including NIST 800-53; NIST Security Measures for "EO-Critical Software" Use; CISA Maturity Model v2; and OMB 22-09.

2 Start by Automating Processes and Workflows



Following the assessment, implementation begins with automation of processes and workflows. As agencies progress towards optimal Zero Trust implementation, their maturity increasingly relies on automated processes and systems that more fully integrate across pillars and more dynamically enforce policy decisions.

3 Invest in Tabletop Exercises

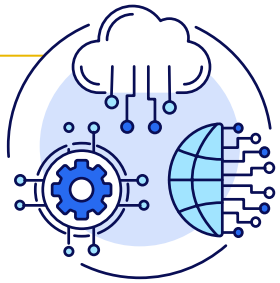
Scenario-driven tabletop exercises are an excellent way to assess your governance, capabilities, standing procedures, and organizational workflows. During tabletop exercises, agency leaders uncover gaps in these areas. Leaders can then address and close the gaps to prepare for (and hopefully prevent!) a possible future occurrence of the scenario.

4 Avoid the "Shiny Object"

Zero Trust cannot be achieved by buying a single tool. Zero Trust is a journey. Tools that replicate or perpetuate the traditional perimeter-centric approach to cybersecurity are, for the most part, inconsistent with Zero Trust. Most agencies have the foundational tools needed to start on their Zero Trust journey; however, they will need to change the way these tools are used and integrated.

For example, agencies generally have one or more device management solutions for enterprise assets but have not integrated these solutions with their identity platforms to enable granular-level authentication. There's a temptation to add new solutions, such as a Secure Access Service Edge (SASE) cloud-based security solution. This helps with the management of devices for remote workforces but does not address all the objectives for Devices pillar maturity.

5 Emphasize Horizontal Integration vs. Vertical Excellence



The model encourages incremental progress achieved horizontally across the pillars, rather than vertically within select pillars. This approach favors integration across pillars to optimize protection to data and services against the broadest range of threats. Without an integrated approach, an organization can achieve optimal maturity in one pillar and remain in the traditional or initial stage in other pillars. This uneven maturity results in gaps in achieving the main objective of Zero Trust, which is to protect critical data.

Zero Trust is a Strategic Undertaking for Federal Agencies

We are grateful to CISA for the investment and collaboration resulting in a refined Zero Trust Maturity Model, especially contributable to the diligence of John Simms and Sean Connelly. The model is not a strict set of proscriptive requirements, nor is it a step-by-step recipe for full Zero Trust maturity. It is, however, a definitive way for agencies to determine where they stand in their Zero Trust journey and allows them to track their progress.

By identifying the criteria for achieving progressive levels of Zero Trust maturity, CISA has recognized Zero Trust as a strategic undertaking. Agencies must assess their current state to determine their specific starting point and set a path that recognizes budgetary, technical, and organizational boundaries. Most importantly, they need to track progress each step of the way.

Accelerate Your Zero Trust Journey – Starting NOW

By using our approach outlined above, agencies will dramatically accelerate their journey. To that end, **Acuity** provides several offerings that can be scaled to fit your needs:

Zero Trust Readiness Assessment

We use the approach outlined in the Recommendations section above to baseline your agency's current Zero Trust posture and existing technology. Our baseline highlights gaps that need to be closed to meet regulatory requirements and position for Zero Trust maturity. We can quickly coordinate our assessment, collaborating with agency counterparts to gather needed documentation, perform our assessment with our expert team, and provide an Agency Roadmap that includes highlighted, prioritized gaps and recommended actions based on critical mission demands.

Tailored Tabletop Exercises

Using your Agency Roadmap, we provide a holistic view of the organizational, operational, procedural, talent, and other changes needed to make progress along the path to Zero Trust. These exercises are tailored to the specific needs of the agency and allow all stakeholders to have a fuller understanding of their roles and the impact that integrated Zero Trust capabilities will have on avoiding or mitigating potential security incidents.

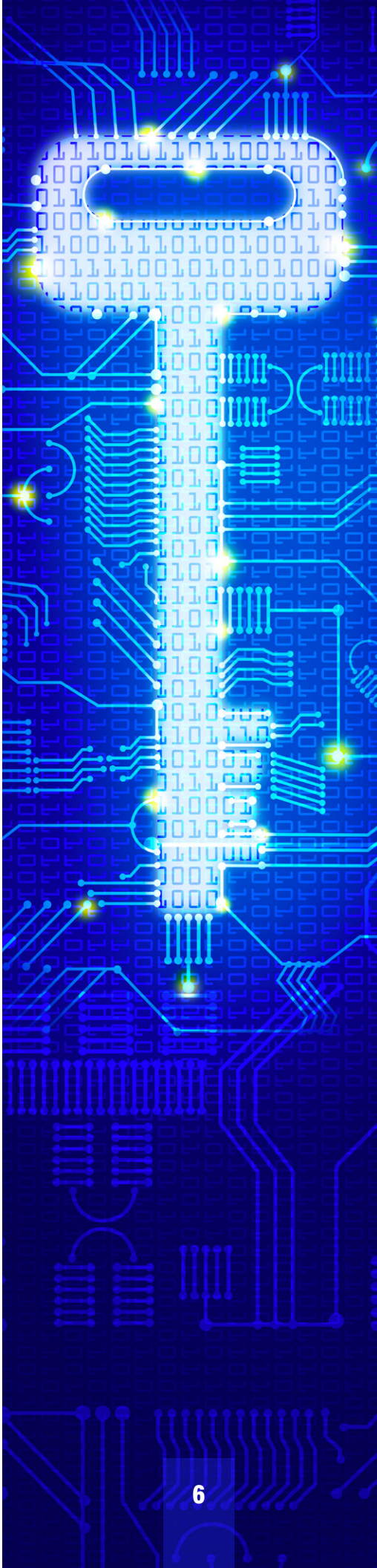
Zero Trust Implementation Services

Acuity's Innovation Lab is developing a suite of capabilities to support known Zero Trust use cases that meet federal requirements. Our risk-based approach is built on the CISA ZTMM v2.0.

ZT Subject Matter Experts – On Call

Acuity offers subject matter expert consultation services for agencies who are interested in advisory, planning and/or review sessions in support of Zero Trust.

For more information, or to request a meeting, please contact:
BD@myacuity.com



About the Authors

Sara Mosley

Cyber Practice Lead, Acuity

Former Acting CTO and TIC PM at CISA

Sara Mosley joined Acuity after more than a decade serving in the public sector. She served as a special advisor in the U.S. Department of State's (DOS) Chief Information Security Office, and as the acting Chief Technology Officer for the Department of Homeland Security's (DHS) CS&C (now CISA). At FDIC, Ms. Mosley revamped the CISO security methodology and architecture. Since joining Acuity, she has helped government clients tackle a myriad of security challenges, including assessing and plotting a practical and logical path to Zero Trust maturity.

Danny Toler

Senior Vice President, Acuity

Former Deputy Assistant Secretary for Cybersecurity and Communications at DHS (now CISA)

Danny Toler joined Acuity after 38 years providing government service. During his tenure, Danny served as the Deputy Assistant Secretary for Cybersecurity and Communications at DHS (now CISA) and previously as the Director of Enterprise Network Management at Department of State. Since joining Acuity, Mr. Toler has proven to be an invaluable advisor to government customers in the areas of IT and cyber strategic planning, governance, policy and procedural development, and subsequent organizational refinements to advance Zero Trust maturity.

Acuity, Inc. is a leading federal technology consulting firm headquartered in Reston, VA. Acuity provides deep domain expertise to help clients optimize mission effectiveness while realizing real, measurable, and impactful results in the national security and public safety missions.

11710 Plaza America Dr Suite 700, Reston, VA 20190
(703) 766-0977 | **www.myacuity.com**