# Zero Trust Strategy

*CCZT Study Guide*

cloud security alliance®

CCZT™
Certificate of
Competence in Zero Trust

The official location for SDP and Zero Trust Working Group is
https://cloudsecurityalliance.org/research/working-groups/zero-trust/

## Disclaimer

Cloud Security Alliance designed and created this Zero Trust Training course study guide (the "Work") primarily as an educational resource for security and governance professionals. Cloud Security Alliance makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

**Version Number:** 20240820

## About Cloud Security Alliance

The Cloud Security Alliance℠ (CSA) (www.cloudsecurityalliance.org) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. Cloud Security Alliance harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. Cloud Security Alliance activities, knowledge and extensive network benefit the entire community impacted by cloud—from providers and customers, to governments, entrepreneurs and the assurance industry—and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

## CSA Address

709 Dupont St.
Bellingham, WA 98225, USA
Phone: +1.360.746.2689
Fax: +1.206.832.3513

**Contact us:** support@cloudsecurityalliance.org
**Website:** https://cloudsecurityalliance.org/
**Zero Trust Training Page:** https://knowledge.cloudsecurityalliance.org/page/zero-trust-training
**Zero Trust Advancement Center:** https://cloudsecurityalliance.org/zt/
**Provide Feedback:** support@cloudsecurityalliance.org
**CSA Circle Online Community:** https://circle.cloudsecurityalliance.org/
**Twitter:** https://twitter.com/cloudsa
**LinkedIn:** www.linkedin.com/company/cloud/security/alliance
**Facebook:** www.facebook.com/csacloudfiles
**CSA CloudBytes Channel:** http://www.csacloudbytes.com/
**CSA Research Channel:** https://www.brighttalk.com/channel/16947/
**CSA Youtube Channel:** https://csaurl.org/youtube
**CSA Blog:** https://cloudsecurityalliance.org/blog/

# Acknowledgments

Dedicated to Juanita Koilpillai, a pioneer in software-defined perimeters whose contributions to the Certificate of Competence in Zero Trust (CCZT), Zero Trust training, and CSA are immeasurable.

The CCZT and Zero Trust training was developed with the support of the Cloud Security Alliance Zero Trust Expert Group, whose members include volunteers from a wide variety of industries across the globe. Made up of subject matter experts with hands-on experience planning and implementing Zero Trust, both as cloud service consumers and providers, the Zero Trust Expert Group includes board members, the technical C-suite, as well as privacy, legal, internal audit, procurement, IT, security and development teams. From cumulative stakeholder input, the Zero Trust Expert Group established the value proposition, scope, learning objectives, and curriculum of the CCZT and Zero Trust training.

To learn more about the CCZT and Zero Trust training and ways to get involved please visit: https://cloudsecurityalliance.org/education/cczt

We would also like to thank our beta testers, who provided valuable feedback on the CCZT and Zero Trust training: https://cloudsecurityalliance.org/contributors/cczt-contributors

## Lead Developers:

Heinrich Smit
John Kindervag
Michael Roza
Paul Simmonds
Prasad T.
Shruti Kulkarni

## Contributing Editors:

Jason Garbis
Mark Schlicting
Richard Lee
Roland Kissoon

## Expert Reviewer:

Chase Cunningham
Hannah Day
Jaye Tilson
Jonathan Flack
Matt Lee
Matt Meersman (Dr.), PhD
Ron Martin (Dr.), PhD

## CSA Staff:

Adriano Sverko
Andy Ruth
Anna Campbell Schorr
Chandler Curran
Daniele Catteddu
Erik Johnson
Hannah Rock
Judy Bagwell
Stephen Smith

# Table of Contents


About Cloud Security Alliance ..... iii
Acknowledgments ..... iv
List of Figures ..... viii
Course Intro ..... 1
Course Structure ..... 1
Course Learning Objectives ..... 1
1 Levels of Strategy ..... 2
1.1 Organizational Strategy - The Ultimate Goal ..... 6
1.2 Cybersecurity Strategy - Zero Trust ..... 6
1.2.1 Key Tenets of Zero Trust ..... 6
1.2.2 Strategic Alignment & Operational Integration ..... 7
1.3 IT Strategy & Technology ..... 7
1.4 Tactics ..... 8
1.5 Operations ..... 9
2 Zero Trust Drivers & Buy-In ..... 10
2.1 The Value of Zero Trust ..... 10
2.2 Risk Management as a Driver ..... 11
2.2.1 Board-Level Risk Management & Zero Trust Alignment ..... 11
2.2.2 Evolving Threat & Risk Landscape ..... 12
2.3 Create a Case for Zero Trust ..... 12
2.4 Leadership Buy-In ..... 12
3 Tactics for Zero Trust ..... 14
3.1 Zero Trust Design Principles ..... 14
3.1.1 Focus on Business Outcomes ..... 15
3.1.2 Design from the Inside Out ..... 15
3.1.3 Determine Who & What Needs Access ..... 16
3.1.4 Inspect & Log Traffic ..... 17
3.2 Zero Trust Maturity Model ..... 18
3.2.1 Zero Trust Maturity Model in Practice ..... 19
3.2.2 CISA-Based Maturity Model ..... 20
3.3 The Five Steps for Zero Trust Implementation ..... 21
3.3.1 Step 1: Define Your Protect Surface(s) ..... 21
3.3.2 Step 2: Map & Prioritize the Transaction Flows ..... 22

3.3.3 Step 3: Build a Zero Trust Architecture ..... 23
3.3.4 Step 4: Create Zero Trust Policy ..... 24
3.3.5 Step 5: Monitor & Maintain the Network ..... 24
4 Zero Trust & Operations ..... 25
4.1 Cultural & Organizational Shift ..... 26
4.2 Training & Education ..... 26
4.3 Regulatory & Compliance Shift ..... 26
4.3.1 Regional Regulations ..... 27
4.4 Legacy Systems & Infrastructure ..... 27
4.5 Usability & Friction ..... 28
4.5.1 User Experience ..... 28
4.5.2 Site Reliability Engineering ..... 28
4.5.2.1 Monitoring & Understanding System Compromises ..... 28
4.5.2.2 Resource & Component Management ..... 29
Conclusion ..... 30
Glossary ..... 30
Acronym List ..... 31

# List of Figures

Figure 1: Strategy Perspective of a Standard Org. Chart ..... 2
Figure 2: Example of Roles and Responsibilities ..... 3
Table 1: Org. Engagement Levels with Examples and ZT Considerations ..... 5
Figure 3: Zero Trust Design Principles ..... 15
Figure 4: Zero Trust From a People Perspective ..... 16
Figure 5: CISA Zero Trust Maturity Model (ZTMM) ..... 18
Figure 6: Zero Trust Maturity Journey ..... 19
Figure 7: Zero Trust Maturity Model Worksheet ..... 20
Figure 8: Zero Trust Learning Curve ..... 22

# Course Intro

This training assumes that learners are familiar with the introductory content of the Cloud Security Alliance's (CSA) Zero Trust Training: *Introduction to Zero Trust Architecture*. Additionally, we recommend that students have at least a basic understanding of networks and network security.

This course presents an in-depth exploration of Zero Trust (ZT) from an organizational strategic perspective; and it also delves into the foundational principles of ZT, its benefits, and the critical factors driving organizational buy-in and strategic alignment.

This course comprises several units, each addressing a distinct, strategic ZT aspect:

- We focus on various levels of strategic engagement with ZT;
- We examine ZT's value, drivers and business case;
- We move on to practical tactics for implementing ZT; and
- We cover the broad impact of a ZT strategy on operations, encompassing areas such as cultural and organizational change, training and education, regulatory compliance, legacy systems and infrastructure challenges, user experience, and adapting to the evolving threat landscape.

# Course Structure

- **Unit 1:** Levels of Strategy
- **Unit 2:** Zero Trust Drivers & Buy-In
- **Unit 3:** Tactics for Zero Trust
- **Unit 4:** Zero Trust & Operations

# Course Learning Objectives

By the end of this course, you will be able to:

- Understand why ZT is a cybersecurity strategy;
- Understand the key principles and components of ZT strategy, and its relationship to the organization;
- Identify how an organization's business goals, and associated IT strategy can be supported with ZT architecture;
- Understand the organization's current state (Business and IT landscape, design architecture, and more);
- Identify tactics and best practices for a ZT implementation; and
- Identify critical cultural, organizational and technical challenges for the implementation of a ZT strategy.

# 1 Levels of Strategy

Equipping cybersecurity experts with the skills and knowledge they need to successfully implement Zero Trust (ZT) security solutions is a major goal of this course. To effectively implement a ZT strategy, your approach must clearly support existing and new business goals, align with organizational objectives, and secure executive sponsorship and resources. A strong understanding of strategic concepts and an organization's particular set of strategies is essential.

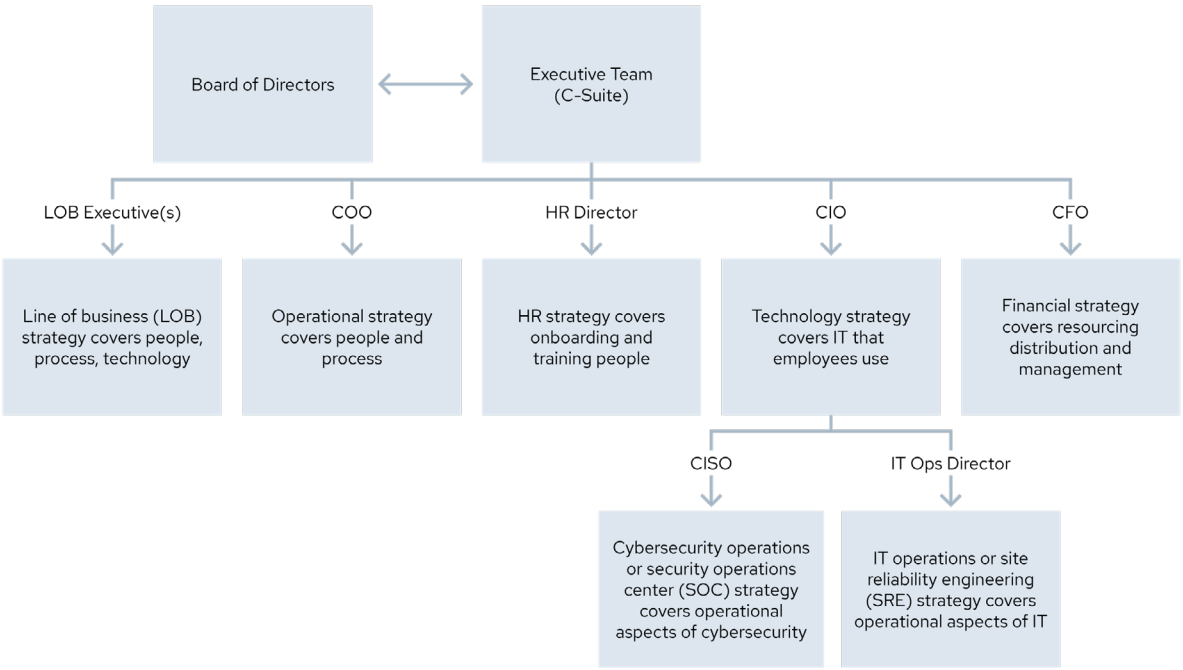


**Figure 1:** *Strategy Perspective of a Standard Org. Chart*

Though organizational structures vary widely, responsibilities for many roles are more constant, as Figure 1: Strategy Perspective of a Standard Org. Chart, above, illustrates. Hence, since ZT is integral to the cybersecurity footprint, and has a primary focus on technology, it must involve both the IT director and the Chief Information Officer (CIO).

And that's not all. A ZT strategy impacts how product teams develop, deliver and utilize IT products in their line of business (LOB). Collaboration with LOBs is important: If you can foster clarity where there is confusion, especially in the early planning phases, you can effectively convert concepts to intent, and intent to action and results.

Configuration state is important for site reliability, and monitoring for breaches or attacks. Though LOBs must focus on their own strategies and approaches to adding value, their cyber activity must be operated and monitored. In the event of breach, tools and business data must be returned to a known state, and preferably to the expected known state.

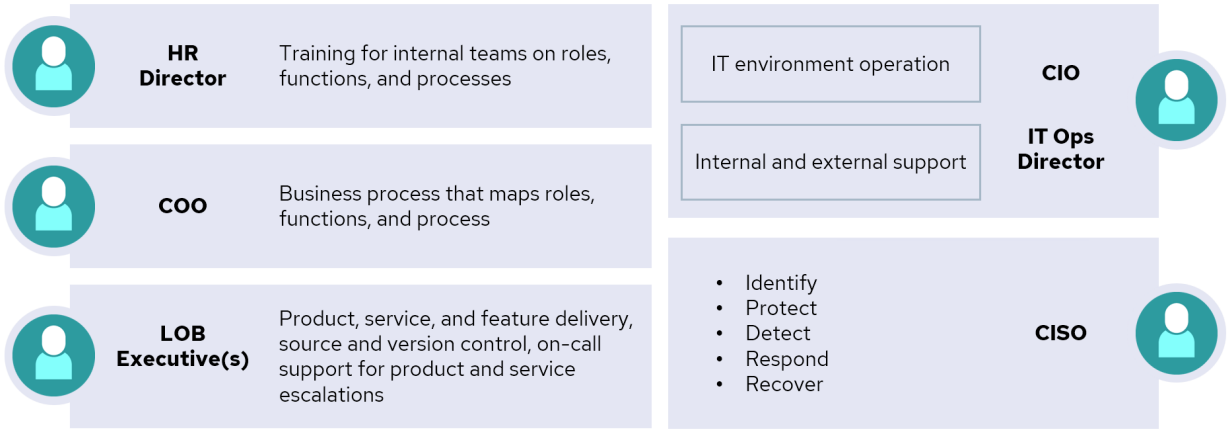


**Figure 2:** *Example of Roles and Responsibilities*

Regardless of the actual terms used in your organization for each engagement level, if you can clarify how each level influences and informs the others, you are a more effective ZT planner, architect and implementer. We hope that structuring this course around engagement levels helps you better organize and control your ZT-related projects.

One of the main goals in discussing strategic terms is to assist you in thinking and communicating clearly and with authority. Clear, concise communication may drive projects to their milestones and ultimate completion. The table below defines organizing engagement levels used in this course (depending on your organization, actual levels may vary), as follows:

- Organization strategy (this encompasses the business goals and objectives);
- Cybersecurity strategy (usually a part of IT security strategy);
- Technology and IT strategy;
- Tactics; and
- Operations.

| Engagement Level | Short Definition | Examples in Practice | ZT Considerations[1] |
|---|---|---|---|
| **Organization Strategy** | A high-level plan that outlines an organization's goals and objectives. | Corporation: Seamless integration of the organization's third parties, enabling seamless and secure collaboration for outsourcers and joint venture partners.<br><br>Departments: Gain support from decision-makers across departments. | • Familiarize yourself with the organization's common metrics, such as revenue, net income, margins, cost-related figures & cash flow.<br>• Gain insight from non-financial measurements, such as regulatory compliance, audit results and more.<br>• Embed ZT principles into the organization's mission statement and core values.<br>• Proactively identify and mitigate security risks at the organizational level.<br>• Establish a ZT culture that prioritizes security and privacy. |
| **Cybersecurity Strategy** | How an organization protects its information and systems, and responds when there are cyberattacks. | Zero Trust: a security framework that assumes that no user or device can be trusted by default. It implements security controls to verify users and devices before they are granted access to resources.<br><br>ZT strategy can help organizations protect themselves from cyberattacks, even if the attacker has already gained access to your environment. | • Conduct regular ZT security assessments and penetration tests to identify and remediate security vulnerabilities. |

[1] Note: This is *not* an exhaustive list of ZT considerations, instead it is meant to serve as an example to get students to begin thinking about the different strategic levels and how they relate to ZT.

| | | | |
|---|---|---|---|
| **Technology & IT Strategy** | How an organization uses technology and IT to achieve its business objectives. | Assets: Take inventory, classify and categorize all assets (e.g., identities, apps, networks, etc.).<br><br>Risk assessment: Conduct a thorough risk assessment to help prioritize ZT efforts.<br><br>Compliance and governance: Align with existing compliance requirements for regulatory adherence and to strengthen the organization's security posture. | • Invest in new data centers and cloud computing technologies.<br>• Develop a scalable and reliable cloud computing platform.<br>• Use automation and DevOps to improve efficiency and agility. |
| **Tactics** | The things you use. These are the specific tools, methods or actions employed to execute strategy. | Put ZT frameworks into action: ZT Design principles, five steps for ZT implementation, Zero Trust Maturity Model (ZTMM).<br><br>Integrate with standard business practices: Lean manufacturing practices, JIT inventory management, continuous improvement initiatives. | • Simplify user access and assign clear management responsibilities.<br>• Deploy a micro-segmentation solution to isolate applications and data from each other. |
| **Operations** | The way you use them. Details of how these tools and actions are successfully employed in practice to work towards the strategic objectives. | Integrate user experience (UX) and site reliability engineering (SRE) in ZT adoption, focusing on code-driven automation for enhanced operational efficacy. | • Monitor the organization's network and systems for suspicious activity.<br>• Respond to ZT security incidents in a timely and effective manner.<br>• Provide ZT security awareness training to employees. |

**Table 1:** *Org. Engagement Levels with Examples and ZT Considerations*

# 1.1 Organizational Strategy - The Ultimate Goal

Organizational strategy is the overarching, ultimate goal that guides an organization's actions and decisions. It represents the highest-level objective that an entity aims to achieve. We assume that one of the key approaches that the board of directors and executive team have chosen to improve their cybersecurity strategy is to leverage the principles of ZT.

# 1.2 Cybersecurity Strategy - Zero Trust

"Zero Trust[2] is a cybersecurity strategy premised on the idea that no entity or asset is implicitly trusted. It assumes that a breach has already occurred or will occur. Therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each entity (user, device, application, etc.), and transaction must be continually verified."[3] At the strategy level, ZT differs from traditional cybersecurity strategies by not assuming nor providing any implicit or inherited trust in anything.

ZT can impact every person and process inside an organization, as well as the entire technology stack. It should be treated as a holistic cybersecurity strategy that covers all enterprise technology domains. This includes cloud and multi-cloud environments, internal and external endpoints. The strategy also includes organizational and bring your own device (BYOD) scenarios, on-premises and hybrid systems, as well as operational technology (OT) and internet of things (IoT).[4]

## 1.2.1 Key Tenets of Zero Trust

ZT is a set of principles and practices designed to reduce cyber risk in today's dynamic IT environments. As a cybersecurity strategy, ZT requires strict authentication and verification for all entities (e.g., each person, device or service) trying to access an IT resource. It doesn't matter whether the access is inside or outside the physical network perimeter. ZT emphasizes the protection of individual assets (systems and data) rather than network segments.

Guiding ZT principles, significance and value vary for each organization, depending on factors such as location, industry and individual traits. The following is a list of some of the tenets that have been discussed[5]:

[2] As many organizations familiarize themselves with Zero Trust, they frequently discover a large amount of misinformation that makes navigating difficult. Cloud Security Alliance's Zero Trust Advancement Center (ZTAC) cuts through the noise, focusing on solutions, not vendors, and delivering trusted guidance that helps raise ZT strategy to the next level.
[3] NSTAC. (2022). Report to the President on *Zero Trust and Trusted Identity Management*. Pg.1
[4] Cloud Security Alliance (N.A) *Zero Trust Implementation Primer* - The Five Step Process (Draft). Pg. 6.
[5] See Cloud Security Alliance course *Introduction to Zero Trust Architecture* for an in-depth review of ZT tenets.

- Never trust, always verify: trust no one, either inside or outside the network perimeter (assuming you have one).
- Assume a hostile environment: Malicious actors reside both inside and outside of any environment you manage.
- Presume breach: Operate with the assumption that an adversary already has a presence in your environment. For example, by limiting the blast radius to contain the impact of a breach to a smaller number of impacted devices and services.

### 1.2.2 Strategic Alignment & Operational Integration

ZT is a holistic endeavor and not just a tactical change. As such, it represents a strategic realignment of the entire security posture. This realignment starts at the highest engagement with the organizational strategic objective[6]. For some organizations, this may be synonymous with *preventing any breach*. For others, it may not be a breach that is most important, but the resiliency in place to limit the impact of it.

Furthermore, as the table that defines the different types of organizing levels mentioned (Table 1: Engagement Levels with Examples and ZT Considerations), Zero Trust Architecture (ZTA) is not just a technical recommendation, but also a cultural shift. The shift demands that security aligns closely with business functions, acknowledging that different departments may have varied security needs. There may be other organizational objectives. Regardless of the specific organizational strategic objective, ZT should be seen as the guiding principle or the *big idea* at the strategy level. ZT should be seen as directly contributing to the organizational strategy.

## 1.3 IT Strategy & Technology

In the context of ZTA, significant adjustments extend beyond technology and IT strategy. The adjustments encompass a fundamental shift in mindset and organizational culture, embracing the "never trust, always verify" principles. Adopting a *never trust, always verify* approach means that access is continuously validated through rigorous security checks and authentication measures. A necessary transformation in adopting ZT is proliferating and enhancing network segmentation. Segmentation is the sub-dividing of the network environment into smaller, distinct segments to limit access and contain breaches.

At the tactical level, implementing ZT involves specific actions. For example, strict access control on a need-to-know basis and secure access to resources regardless of their location. These topics are discussed in more detail in the tactics and operations sections. Such alignment ensures that security enables business operations, rather than hindering them. It requires an architecture that allows for flexibility, catering to different service level agreements (SLAs), administrative controls, audit requirements, regulations and certifications.

IT strategy also encompasses user and entity behavior analytics (UEBA). Additionally, technology strategy must integrate closely with governance, while rigorously controlling and monitoring access to reduce risk. Cybersecurity goals, including ZT, should align with the organization's overall strategy and board-level roadmap, guiding various projects and technology strategies for the upcoming years.

[6] In some organizations, this is also referred to as the "grand strategic objective."

The operationalization of ZT is where ZT concepts become tangibly interwoven with the day-to-day activities of the organization. This ensures that every aspect of the network is designed from the inside out with a default perspective of verifying everything and trusting nothing. To make such a perspective functional and practical requires consolidating technologies. IT also requires enhancing security measures for critical assets, and applying specialized controls for legacy and critical infrastructure systems.

ZT and technology strategies are closely connected to governance, risk management, and every aspect of security, but it is important to clarify the role of each framework. Governance, focusing on establishing and maintaining policies, standards and guidelines, plays a crucial role in ZT implementations. The governance ensures that ZT practices not only adhere to regulatory requirements but also align with the organization's overall objectives. This relationship positions ZT as a strategic element within the governance landscape. This lesson does not cover risk management or compliance strategies because they are covered in other lessons.

## 1.4 Tactics

Tactics, within the context of a ZT strategy, are crucial for effectively addressing specific risks and aligning security measures with organizational objectives. These tactics involve prioritizing business goals, adopting an "inside out" security approach, and implementing the principle of least privilege to control resource access. Metrics and reporting improvements are vital for assessing ZT effectiveness. Monitoring and logging network traffic and identifying and protecting critical data, applications, assets and services (DAAS) also plays a pivotal role in these tactics. Additionally, transitioning to ZT requires a phased, risk-based approach that impacts tactics, such as precise policy creation, prioritization, and iterative implementation.

Tactics are fundamental in ensuring a smooth transition to a ZTA and are focused on protecting assets and resources efficiently. ZT policies, detailed access controls, monitoring network traffic, and setting progress metrics contribute to the successful implementation of ZT principles. Organizations can bolster their cybersecurity posture by adopting these tactics and gradually progress along a Zero Trust Maturity Model (ZTMM)[7], ultimately achieving improved security outcomes. Tactics and the maturity model are covered in the tactics units.

NIST *Zero Trust Architecture* (SP 800-207)[8] defines the tenets that are fundamental to a ZT environment. As such, the tenets need to be considered before deploying policy enforcement points (PEPs) and policy decision points (PDPs). To meet these foundational tenets, a dynamic policy must drive the shift away from network access. The policies must motivate organizations to implement measures that reduce the attack surface prone to lateral attacks, such as macro and micro-segmentation.

Because all communications must be secured, regardless of location, a tactical assessment is needed. Assessments can ensure adequate encryption has been used for each application, regardless of destination; and access to resources is on a per-session basis.

[7] CISA. (2023). *Zero Trust Maturity Model* (Version 2.0).
[8] NIST. (2020). *Zero Trust Architecture* (SP 800-207).

The migration to a ZTA might take from a few months to several years, depending on the maturity level of the organization (See Section *Zero Trust Maturity Model*) – the path differs for each organization. As noted above, tactical plans are needed for the platform, the tools, the monitoring and detail metrics must each be assessed for the journey.

## 1.5 Operations

Operations refers to the activities, processes and procedures involved in managing and maintaining organizational infrastructure and IT infrastructure. This includes a range of tasks, aimed at ensuring the effective and efficient functioning of all IT resources, such as hardware, software, networks and data storage systems.

Embarking on a ZT journey involves cultural and organizational shifts, emphasizing a ZT culture over technology, and securing leadership support for continuous risk management. Training and education geared toward understanding the ZT paradigm is commonly necessary. This includes a strategic appreciation of ZT that targets management, and several other initiatives that emphasize transforming business processes and roles. Regulatory landscapes are also adapting to require robust cybersecurity practices that align with ZT principles.

Achieving ZT success involves several important considerations in managing and executing day-to-day operations. When a ZT strategy is implemented, the identity management process should be automated, as should monitoring and detection. Day-to-day tasks people in the roles listed above perform include:

- Organizing log data so that input logs from different sources can be looked at and analyzed using the same tools and interfaces.
- Adjusting controls and fine tuning the automation regularly to make sure it checks the right parameters according to policy rules.
- Monitoring to ensure that the automatic checks of logs catch any activities that don't follow the policy rule.

Ensuring cybersecurity solutions enhance rather than add friction to a user's productivity and overall experience is an important organizational goal that operational leaders must focus on and defend. Operational processes, such as site reliability engineering (SRE), and a focus on automation and scalable systems, can improve operational efficiency and promote a positive user experience. Furthermore, operational procedures may need updates to align them with a new ZT framework, ensuring that response strategies and daily activities align with ZT principles.

Challenges include integrating ZT with legacy systems, where a tailored approach is necessary. Maintaining vigilance in monitoring the evolving threat landscape ensures ZT remains agile and responsive. These concepts are expanded upon in a unit dedicated to ZT operations.

# 2 Zero Trust Drivers & Buy-In

For an effective Zero Trust (ZT) implementation strategy, you must align the strategy with organizational values and drivers. The central objective of this approach is to secure buy-in from key stakeholders within the organization. The buy-in ensures that the ZT strategy is not only well-conceived but also well-received and integrated within the organization.

Remember, ZT is a context and risk-based approach: access is granted according to specific situations or conditions. Due to these characteristics, ideas that help deliver and implement ZT are usually clearer and gain wider acceptance if you prepare use-case scenarios and provide contextual applications to support them.

To get started in defining the desired state, you may wish to ask the following questions:

- Identifying Catalysts and Business Drivers:
  - What are the primary catalysts driving the adoption of ZT in our organization?
  - What are the key business drivers aligning with ZT implementation?
- Evaluating Security Posture and Data Access:
  - How does our current security posture align with common attack vectors, especially in the context of our ZT pillars?
  - Is access to confidential and regulated data restricted to registered applications?
- Enhancing Security and Privacy Strategies:
  - How can we develop a more efficient and effective security strategy under ZT principles?
  - What role does privacy play in our overall security and risk management, and how can we define our privacy objectives?
- Access Control and Authentication:
  - Are all privileged accounts secured with FIDO2 or equivalent multi-factor authentication (MFA), or are privileged access workstations (PAWs) necessary?
  - Is MFA mandatory for all (people) identities in our environment?
- Device and Data Access Management:
  - To what extent are personal (non-organization managed) devices allowed access to organizational data?
- Competitive Advantage through Security:
  - Can we gain a market advantage over competitors through a superior security and privacy strategy?
- Compliance with ZT in Development:
  - Are our development teams aligning software testing with ZT standards?

## 2.1 The Value of Zero Trust

ZT offers numerous potential benefits, including streamlined security and IT infrastructure management, enhanced data protection, regulatory compliance, reduced compliance-related efforts, increased organizational agility, stakeholder confidence, and lower IT and operational costs[9]. In other words, the benefits go beyond the security domain. For these reasons, if positioned correctly, ZT has the potential to be a business enabler rather than a hindrance to the organization or its managers. ZT transforms IT and security, aligns business and security goals, and reduces siloed activities.

[9] Cloud Security Alliance. (2023). *Communicating the Business Value of Zero Trust.*

Having established the benefits of ZT as a business enabler, the next step involves a tailored approach. The tailored approach aims to integrate ZT into the organization's unique culture, and business and cybersecurity practices. Before embarking on your ZT journey, clearly define your organization's goals and challenges, gather relevant information, and align your strategy with business needs. An organization must clearly define its strategy and governance, focusing on what is relevant, what standard (if any) it commits aligning with, who is affected, when and where each applies, and how it's implemented. Be sure to also capture why a particular strategy or governance policy is important. This exercise ensures that you can explain a new architecture, implement according to related policies, and articulate how your effort seamlessly aligns with the organization's business model and rules.

ZT principles make it easier for IT teams and network infrastructure teams to enforce policies consistently and accurately, enabling a more friction-free work environment. This is because implementation of a Zero Trust Architecture (ZTA) requires moving the access enforcement points closer to the protected asset.

## 2.2 Risk Management as a Driver

In a traditional legacy organization, the risk calculation is predominantly based on a binary trust. If the entity is inside my network environment (or area of control) it is afforded a level of trust. If it's not on my network or in my area of control then it's untrusted, and thus there is a need to provide extra security measures, for example a virtual private network (VPN).

In the realm of ZT, the foundational principle is *never trust, always verify*. An organization shifts its capabilities, such that it can continually assess and contextualize the risk or risks involved in granting an entity access to an asset.

Remember, this assessment that leads to a decision is not just about having a static defense mechanism in place. It is about creating a proactive, dynamic control plane that evolves with the changing risk landscape. In a ZT environment, access is not only based on contextual factors, it is also temporal. The access needs to adapt to new emerging threats, requiring a continuous review of existing controls and emerging threats. The continuous review must ensure the organization can function without friction from security controls while retaining sufficient protection. The emphasis here is on maintaining consistent, measurable effectiveness.

### 2.2.1 Board-Level Risk Management & Zero Trust Alignment

Aligning a ZTA with an organization's risk appetite is a strategic process, aiming to deliver security solutions that support the board's strategic vision.

The board plays a crucial role in organizational alignment, as they are responsible for setting and defining the risk appetite, setting budgets and determining the appropriate risk oversight structure. Strategic alignment and budget influences technology and control selection, resource allocation, and policy-making, ensuring a viable cybersecurity strategy.

### 2.2.2 Evolving Threat & Risk Landscape

Monitoring the evolving threat and risk landscape is part of risk management. Cyber threats evolve continuously, and implementing continuous monitoring involves regularly assessing and updating an organization's understanding of potential threats and vulnerabilities. This process includes analyzing cyberattack trends, identifying new methods employed by attackers, and understanding the implications of technological advancements on security. Organizations need to address these challenges to secure their systems. ZT offers a framework that facilitates a shift in mindset that promotes securing and protecting what is important for the organization.

## 2.3 Create a Case for Zero Trust

Organizations measure their health and progress using key financial metrics like revenue, net income, margins, costs, and cash flow. Organizations also consider non-financial indicators such as stock performance, compliance, audit outcomes, reputation, and employee productivity for a comprehensive view. Different stakeholders prioritize various metrics. Understanding these measures is vital for asking more effective questions, understanding drivers, and constructing a meaningful case for adopting ZT.

The primary goal of the business case, which is defined further during Cloud Security Alliance's *Zero Trust Planning* training, illustrates how an initiative delivers organizational value and return on investment (ROI). The business case also requires alignment with organizational strategy.

Consider these organizational elements during the buy-in phase to lay a solid foundation for a successful and strategic implementation of ZT:

- Alignment with, and assistance in, delivering key business goals and objectives.
- The value to the business in implementing a ZTA, both tangible and intangible.
- Key stakeholder buy-in: ZT is everyone's responsibility, not just the purview of IT or the Chief Information Security Officer (CISO). Gaining support from the key stakeholders across departments is essential.
- Assets inventory, classification, and categorization of business critical assets or asset classes. These must also be defined in terms of risk to the business.
- Compliance and governance: Confirm that any changes made by implementing ZT align with existing compliance requirements. This ensures regulatory adherence and strengthens the organization's security posture.
- Strengths, weaknesses, opportunities, and threats (SWOT) analysis or cost/benefit analysis (CBA): Perform a SWOT analysis to help identify internal strengths, weaknesses, opportunities and threats. CBAs are also helpful. These help guide IT professionals in the initial stages of a ZT implementation.

## 2.4 Leadership Buy-In

You should look to map the ZT journey so that leadership, especially non-technical leadership roles, can appreciate how it may affect their area of responsibility. The following examples illustrate how

ZT may serve as a foundation for areas such as privacy, security, compliance, third-party risk management (TPRM), and simplicity and efficiency at your organization[10]. These need translating into examples of ZT success using current business problems that your business leaders recognise are improved by ZT.

**Privacy**

- Data Minimization and Access Control: By adhering to the principle of "never trust, always verify," ZT ensures that access to sensitive data is tightly controlled and monitored, reducing the risk of unauthorized data exposure.
- Enhanced User Privacy: ZTAs can protect user privacy by limiting access to personal data and ensuring that only necessary data is processed and stored.

**Security**

- Reduced Attack Surface: ZT requires strict access controls without implicit trust and micro-segmentation. The two limit the pathways an attacker can use to move laterally across a network.
- Real-time Monitoring and Response: Continuous monitoring is a key tenet of ZT, allowing for real-time detection and response to threats, thereby enhancing security postures.

**Compliance**

- Regulatory Alignment: Many regulatory frameworks require strict access controls and data protection measures, which are core components of a ZT model.
- Audit and Reporting: ZT architectures make it easier to log access and changes, thus supporting compliance reporting and auditing requirements.

**Third-Party Risk Management (TPRM)**

- Vendor Access Limitations: ZT principles can be applied to third-party vendors to ensure they have only the access and visibility that is necessary to perform their functions.
- Continuous Verification of Third-Party Credentials: Regular re-verification of credentials and access rights helps to manage and mitigate the risks associated with third-party partners.

**Simplicity and Efficiency**

- Often the implementation of ZT-based access simplifies the traditional access mechanism for the user, enhancing productivity. ZTA helps with quick and seamless access to the assets irrespective of location and network boundaries.
- It is essential to designate a person or a limited number of people with the accountability and authority to manage a particular area. A clear owner ensures issues are identified and highlighted at the appropriate level.

[10] Cloud Security Alliance. (2023). *Zero Trust Guiding Principles*.

# 3 Tactics for Zero Trust

In this unit, we delve into the tactical aspects of implementing Zero Trust (ZT). We discuss nine crucial sub-sections contributing to building a resilient architecture. Alongside these, we'll also introduce CISA's *Zero Trust Maturity Model (ZTMM)*, which, while not a part of the nine steps, is important in understanding the overall progression in ZT implementation. The initial four subsections outline the foundational principles of ZT design, while the subsequent five subsections detail the step-by-step process for ZT implementation.

- ZT Design Principles
  - Focus on Business Outcomes: Understanding how ZT aligns with and supports the organization's primary business goals.
  - Design from the Inside Out: Developing a security strategy that starts within the organization before extending outwards.
  - Determine Who/What Needs Access: Identifying which users and devices require access to specific resources.
  - Inspect and Log Key Traffic: Aim to monitor and record critical activity for potential threats as a targeted approach.
- Foundational Principles of ZT Design
  - **Step 1:** Define Your Protect Surface(s): Identify and secure critical data and resources within the network (environment).
  - **Step 2:** Map the Transaction Flows: Understand the movement of data within and outside the organization and the potential classification of each transaction type.
  - **Step 3:** Build a Zero Trust Architecture (ZTA): Develop the infrastructure and capabilities necessary for ZT.
  - **Step 4:** Create ZT Policy: Establishing guidelines and rules for network, system and data access and security.
  - **Step 5:** Monitor and Maintain the Network (Environment): Continuously oversee the ZT environment to ensure ongoing security and adapt to new threats.

These elements are vital in shaping and executing an effective security approach aligning with an organization's objectives.

## 3.1 Zero Trust Design Principles[11]

This section explores the foundational design principles that shape an effective ZT security strategy. These principles guide organizations in transitioning from traditional security models to a more robust approach suited for today's dynamic digital landscape. The focus is on setting goals like designing security from the inside out, accurately determining access requirements, and aiming for thorough inspection and logging of network traffic. It is important to note, however, that the realization of these goals may differ based on an organization's specific capabilities and resources.

[11] (2023) *Zero Trust Explained* by John Kindervag

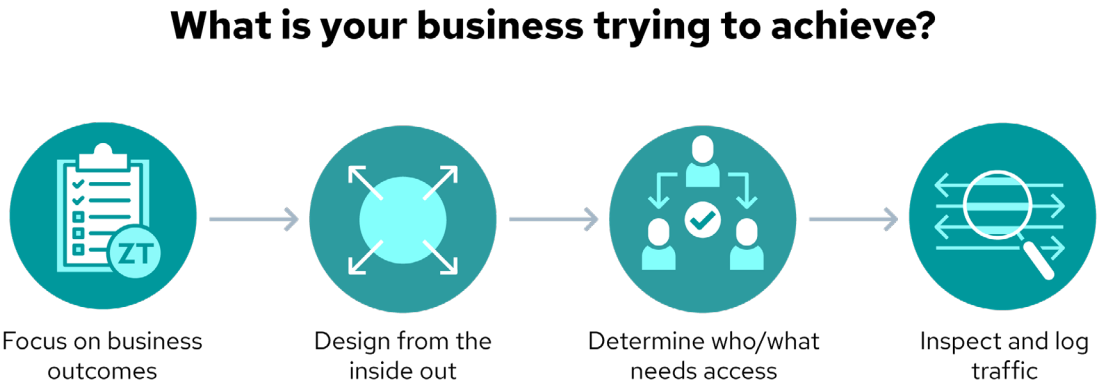


**Figure 3:** *Zero Trust Design Principles*[12]

### 3.1.1 Focus on Business Outcomes

Shaping a ZT strategy begins with a clear understanding of the organization's strategic direction and its IT needs. This understanding should incorporate the organization's specific business threats and the broader spectrum of risks posed by factors like organized crime and nation-state actors. The priority is to safeguard business-critical assets—considered the crown jewels—within a ZT framework.

If ZT is the chosen strategy, it's crucial to prioritize business objectives tailored to your organization's specific goals and requirements. From the outset, ZT demands a clear vision, whether it's to manage risks within acceptable limits, reduce compliance costs, or minimize the impact of security incidents. An effective ZT strategy balances security with the cost and value of security and available-resource use to deliver on security initiatives versus other business initiatives like product or feature development, while avoiding excessive measures that could hinder competitiveness.

### 3.1.2 Design from the Inside Out

ZT marks a shift from traditional perimeter-centric security models, which operate on the obsolete premise that everything inside a network is safe, while external entities pose threats. ZT flips this notion, recognizing that threats can originate from anywhere—both inside and outside the network. This paradigm shift dictates a security architecture designed from the inside out. The design begins with the organization's most critical assets and data at its core and securing access from inside the network, and then extending protection outward. This strategy reorients IT policies to move from a stance of broad threat defense to a focused asset protection approach. The reorientation ensures that the most vital resources are safeguarded at their heart to mitigate the risk of unauthorized access and data breaches.

To connect the design shift to operational strategy, it's important to consider the constraints of limited resources, which all organizations face. This constraint necessitates effective prioritization based on asset value. Conducting a business impact assessment (BIA) or an asset inventory categorized by value helps in identifying critical resources. By ranking assets according to their criticality or value, organizations can efficiently allocate their resources, aligning their security efforts with ZT principles and securing both protect and attack surfaces more effectively.

[12] Figure adapted from: (2023) *Zero Trust Explained* by John Kindervag.

To connect the design shift to operational strategy, it's important to consider the constraints of limited resources, which all organizations face. This constraint necessitates effective prioritization based on asset value. Conducting a business impact assessment (BIA) or an asset inventory categorized by value helps in identifying critical resources. By ranking assets according to their criticality or value, organizations can efficiently allocate their resources, aligning their security efforts with ZT principles and securing both protect and attack surfaces more effectively.

### 3.1.3 Determine Who & What Needs Access

Today, organizations operate on a global scale, leveraging remote work, joint ventures, outsourced services, and cloud technology. In a ZT security approach, the principle of least privilege (attribute of never trust, always verify) necessitates a precise determination of who or what needs access to certain resources, along with the duration and associated risks of such access. This principle ensures that each entity – be it a user or a system – has access strictly as per their need, thus narrowing the attack surface and enhancing security. An asset's visibility should strictly conform to the need-to-know basis, remaining invisible to those without a legitimate requirement for access.

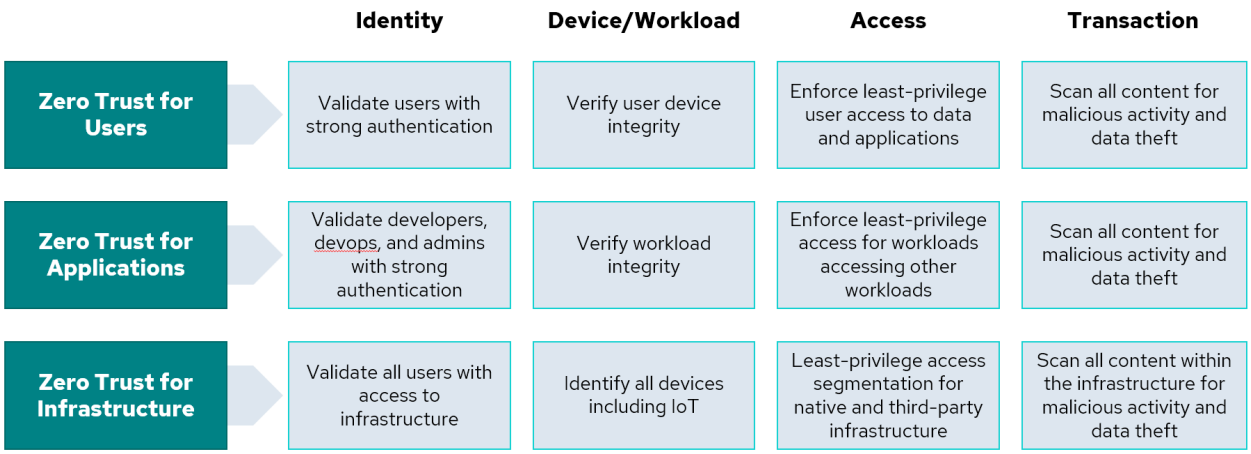


**Figure 4:** *Zero Trust From a People Perspective*[13]

The concept derived from the Identity Security Alliance, as depicted in Figure 4 Zero Trust From a People Perspective, encompasses seven elements: users, applications, infrastructure, identity, device/workload, access, and transaction. Training individuals outside of security roles, like network teams and developers, to identify and manage trust relationships across these elements is a key challenge. Critical tasks include mapping out where trust is established. Examples include between users and identities or infrastructure and identities, and adopting secure practices like proper firewall configurations and secure coding. A thorough understanding of these trust points allows for the effective identification and mitigation of vulnerabilities that cybercriminals target. Benefit is derived from the insights gained through extensive penetration testing experience.

[13] Cloud Secuirty Alliance. (2023) *The Most Important Part of Zero Trust: People* by George Finney

### 3.1.4 Inspect & Log Traffic

Two key principles of ZT, as outlined in NIST *Zero Trust Architecture* (SP 800-207)[14], are: Continuously monitoring and assessing the security and integrity of all assets and resources. Gathering extensive information on the current state of assets, network infrastructure, and communications to enhance security measures.

In the journey towards ZT adoption, organizations require some sort of logging and monitoring capabilities. The level of sophistication will vary greatly, depending on the level of organizational maturity, and the resources available.

This process typically begins with the establishment of foundational log management practices. This means starting with the basic yet important step of implementing systems to gather user and entity activity logs, particularly focusing on privileged credentials, coupled with routine manual analysis. This initial phase should cover all essential ZT pillars, laying the groundwork for more advanced security measures.

As the organization's maturity in the ZT framework advances, supplemented by adequate resources and expertise, it can evolve these practices into more sophisticated systems. A key development in this evolution is the integration of a security information and event management (SIEM) system. SIEM serves as a pivotal tool for automated log aggregation and analysis, setting the stage for the adoption of security, orchestration, automation, and response (SOAR) capabilities.

In scenarios where the organization has control over network-level infrastructure or can log traffic at the access gateway, it's strategically important to incorporate relevant and contextual ZT logs into a SIEM system or log management tool. This integration not only enhances the organization's security posture but also aligns with the fundamental principles of ZT. The integration ensures continuous monitoring and adaptation to the ever-evolving security landscape. The ability to assess and log relevant and contextual traffic from both internal and external sources can significantly enhance operational intelligence.

Additionally, at high levels of maturity, the carefully selected log data from various layers or applications can be unified into a common data structure. Data captured includes device, time, user, and the resource or asset access (e.g., server, service, application, etc.) requested. By coupling monitoring and logging, engineers can continuously improve security by rapidly countering any suspicious activity. Continuously scrutinizing traffic patterns in such a manner is a powerful, strategic asset.

Capturing data and monitoring it in real time requires the development of reactive controls, including system and organization controls (SOC) assessments, analysis, response staff and automation in the response pipeline. Logging is only any good if you do something with it, but for the many organizations without a SOC in place, there is no reason for a major consolidated log database. It is acceptable for the ZTA configuration to simply monitor and log:

- At the policy decision points (PDPs);
- All admin operations; and
- All user access event logs.

[14] NIST. (2020). *Zero Trust Architecture* (SP 800-207)

## 3.2 Zero Trust Maturity Model

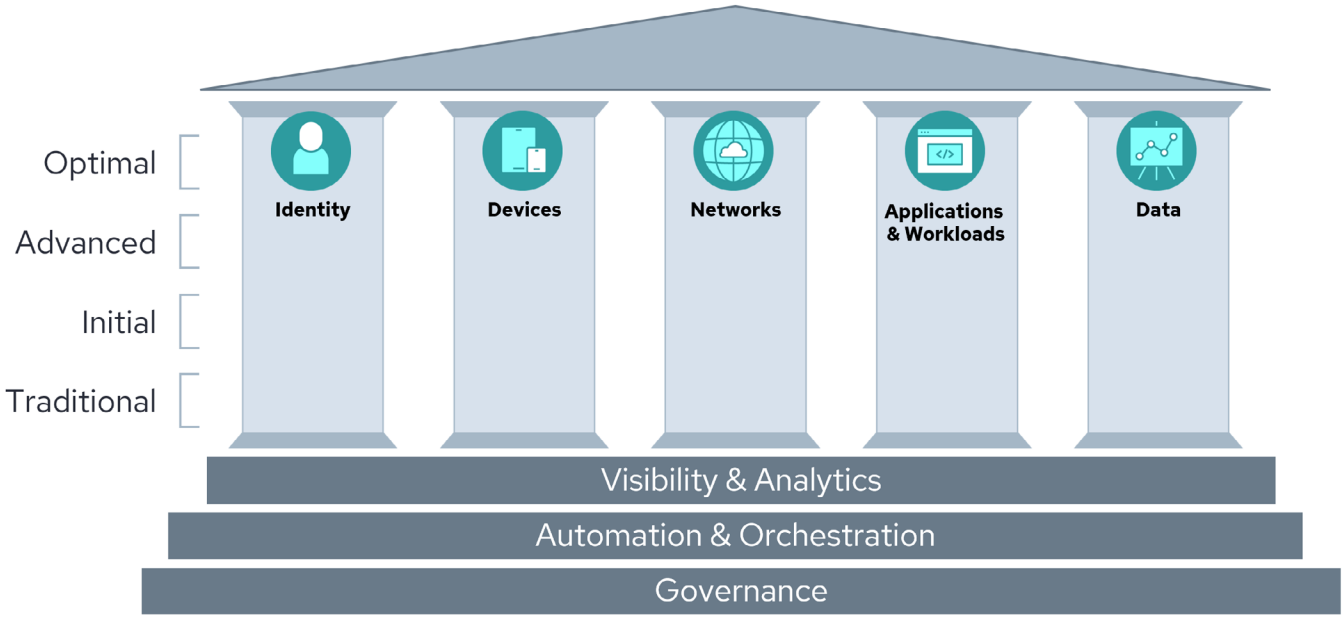


**Figure 5:** *CISA Zero Trust Maturity Model (ZTMM)*[15]

This section covers the CISA *Zero Trust Maturity Model (ZTMM)*[16], which helps organizations enhance their ZT strategies. The CISA ZTMM outlines maturity stages – Traditional, Initial, Advanced, Optimal – across ZT pillars (Identity, Devices, Networks, Applications and Workloads, and Data) and capabilities (visibility, automation, governance). These maturity stages help organizations assess, plan and implement the necessary measures to progress toward a more secure ZTA. The CISA ZTMM journey, depicted in the accompanying figure, represents a path towards achieving optimal ZT maturity. This journey, a practical visual representation, shows how companies advance through ZT's various maturity levels.

[15] Figure adapted from: CISA. (2023). *Zero Trust Maturity Model* (Version 2.0).
[16] CISA. (2023). *Zero Trust Maturity Model* (Version 2.0).

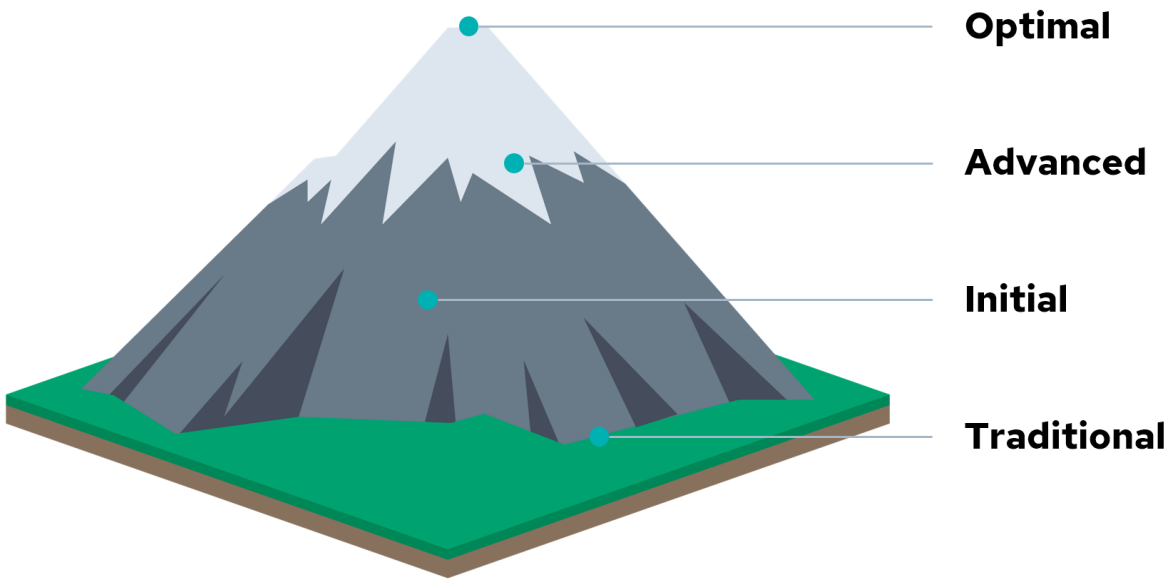


**Figure 6:** *Zero Trust Maturity Journey*[17]

To utilize the CISA ZTMM effectively, grasp the framework, refine your functions and assess your current ZT maturity. Finally, plan steps for maturity advancement and align them with organizational projects and priorities, using a prioritization model to guide you.

### 3.2.1 Zero Trust Maturity Model in Practice

Tailoring the CISA ZTMM to fit your needs may seem overwhelming. It is not advisable to strive to achieve optimal maturity across all pillars simultaneously. Nor is it advisable to focus on a single pillar and expect to perfect it across the entire organization. Attempting to perfect one pillar (like identity) across all systems before moving to the next is not only impractical but can lead to stagnation in overall security posture improvement. It is important, instead, to evaluate each protect surface, using worksheets such as the one illustrated below, which is based on the NSTAC report. Each worksheet identifies the protect surface and critical data, assets, application, and services (DAAS) element being evaluated, with 5 (optimized) representing the best possible score for each attribute. The total perfect score on a worksheet would be 25. This is a rare occurrence. Such worksheets help teams prioritize projects, based on safeguarding business-critical assets. This targeted approach allows for a more accurate assessment of maturity gaps and enables the development of specific projects to enhance the security and maturity of each protect surface. Furthermore, by evaluating each protect surface individually, organizations can create a more nuanced and actionable cybersecurity roadmap. Finally, all the protect surfaces can aggregate to define an overall score for the organization as well as an average score per protect surface.

[17] Figure adapted from: (2023) Zero Trust Explained by John Kindervag.

| Protect Surface: _____<br>DAAS Element: _____ | Initial | Repeatable | Defined | Managed | Optimized |
|---|---|---|---|---|---|
| 1. Define your protect surface | 1 | 2 | 3 | 4 | 5 |
| 2. Map the transaction flows | 1 | 2 | 3 | 4 | 5 |
| 3. Architect a zero trust environment | 1 | 2 | 3 | 4 | 5 |
| 4. Create zero trust policy | 1 | 2 | 3 | 4 | 5 |
| 5. Monitor and maintain the network | 1 | 2 | 3 | 4 | 5 |

Total Score: _____

**Figure 7:** *Zero Trust Maturity Model Worksheet*[18]

This methodology simplifies the complexity inherent in managing multiple and discrete identity solutions across an organization. For example, if an organization focuses on improving the security maturity of its directory services (as a protect surface), it can methodically elevate the maturity level in this specific area, thereby making tangible progress and ensuring continuous improvement in cybersecurity defense. Finally, it helps you monitor progress across various ZT projects to stay aligned with your organization's IT strategy and cybersecurity strategy.

### 3.2.2 CISA-Based Maturity Model

You may also wish to explore this interactive CISA ZTMM Spreadsheet model[19], a comprehensive tool with status bars for monitoring progress. After a ZT assessment, approach the journey systematically, with the same considerations that we suggested if you choose to use the National Security Telecommunications Advisory Committee (NSTAC) based assessment model:

- Analyze all functions, adjusting the depth as needed;
- Avoid tackling all functions simultaneously so as to not be overwhelmed;
- Focus on enhancing specific areas within individual projects, addressing a single protect surface at a time; and
- Ensure projects align with business drivers and deliver tangible business value, not just security benefits.

You are encouraged to tailor the ZTMM approach to your organization's needs. This pragmatic approach ensures that the journey towards a mature ZT environment is both achievable and manage-

[18] Figure adapted from: NSTAC. (2022). NSTAC Report to the President on *Zero Trust and Trusted Identity Management*. Pg. A-1

[19] Jason Garbis and Numberline Security have created The Zero Trust Maturity Model Resource Center and associated worksheets (GCP Sheets and Excel), aligned with the CISA ZTMM. Learn more about these tools here.

able, because it keeps you flexible. Remember that the goal is delivering tangible value to your business, with ZT maturity serving as a measure of progress and a guide for prioritizing enhancements in your implementation.

## 3.3 The Five Steps for Zero Trust Implementation

In the journey towards an ideal ZT architecture, there are five essential steps to follow to operationalize each protect surface project. These steps provide a structured approach to enhance cybersecurity and ensure a successful transition to a ZT paradigm. Organizations can gain a deeper understanding of their data interactions by:

- Beginning with the definition of protect surface(s) and a risk-based strategy in Step 1;
- Mapping transaction flows in Step 2;
- Building and implementing protect surface projects (tailoring the ZTA), that emphasize flexibility and customization to work alongside existing network environments in Step 3;
- Focusing on creating precise ZT policies, addressing the who, what, where, when, why, how, and for how long of access controls in Step 4; and
- Continuous monitoring and maintaining the network (environment) as it enters production (fundamental to the sustained success of a ZTA) in Step 5.

These five steps collectively form the foundation for implementing a comprehensive ZT strategy.

### 3.3.1 Step 1: Define Your Protect Surface(s)

As you embark on your ZT journey, shift your perspective to focus on what you're protecting rather than what you're defending against. Visualize your end goal and prioritize safeguarding critical and vulnerable components within your protect surface, known as DAAS. Organizations should prioritize identifying protect surfaces, and then document attack surfaces to complement them, steering clear of a traditional, attack-surface-centric approach. Examples include:

- Data: Sensitive information. Examples include:
  - Payment card industry (PCI);
  - Protected health information (PHI);
  - Personally identifiable information (PII); and
  - Intellectual property (IP) that can cause significant harm if compromised.
- Applications: Software interacting with sensitive data or controlling essential assets and processes related to the business.
- Assets: IT, OT, or IoT devices such as point-of-sale (PoS) terminals, supervisory control and data acquisition (SCADA) controls, and networked medical devices.
- Services: Examples include:
  - Domain Name System (DNS);
  - Dynamic Host Configuration Protocol (DHCP);
  - Active Directory; and
  - Network Time Protocol (NTP).

To deploy ZT environments, organizations should focus on two factors: the criticality of the protect surface and the duration of the ZT journey, ideally ongoing. Data classification – as identified above (data sensitivity) – is a critical starting point. Start with low-sensitivity learning protect surfaces, like lab environments or non-critical web pages, allowing for safe experimentation and failure. Progress to practice protect surfaces, which are more sensitive but not the organization's most critical assets. This step-by-step approach builds confidence in ZT principles before moving to the most sensitive areas. After securing high-value assets, the focus shifts to less critical protect surfaces, gradually covering all significant areas in the ZT environment.

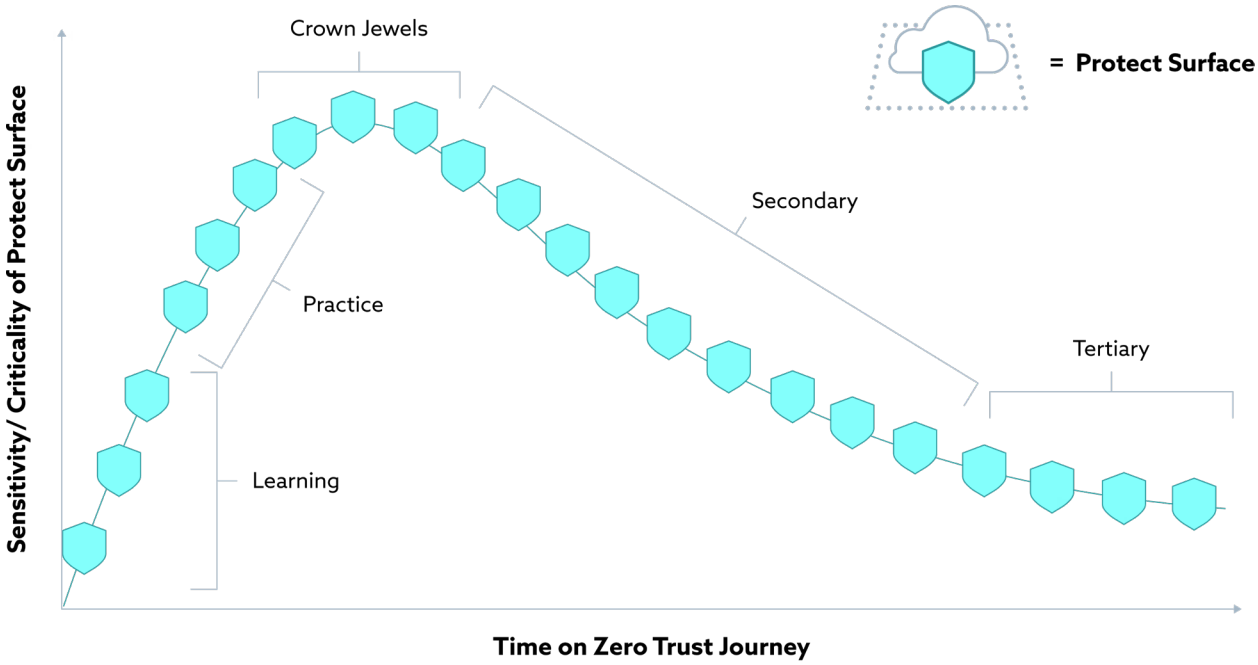


**Figure 8:** *Zero Trust Learning Curve*[20]

## 3.3.2 Step 2: Map & Prioritize the Transaction Flows

The fundamental objective of this step is to prove to your audience that you have an understanding of how the whole cybersecurity system works. Mapping transaction flows for each protect surface is critical for understanding how DAAS components interact (how the system works). The mapping is also critical for determining the optimal placement of controls for data protection. These network traffic patterns, specifically tailored to the protect surface data, are essential for shaping the overall design.

Once the transaction flows have been mapped, the next task involves prioritizing, which may also be shaped by the reality of the readily available resources. This process involves determining how resources, such as personnel, time and budget, should be allocated to these prioritized flows to implement the ZTA efficiently.

From a strategic viewpoint, defining protect surfaces and prioritizing transaction flows are necessary inputs to request and allocate necessary resources (e.g., budget and personnel). For example,

[20] Figure adapted from: (2023) *Zero Trust Explained by John Kindervag.*

business processes involving sensitive data should be prioritized, as these processes are crucial for establishing access rights and conditions within the ZTA[21]. To ensure a smooth transition to ZTA, starting with a low-risk business process is advisable, minimizing disruption and gaining valuable experience before moving on to more critical processes.

### 3.3.3 Step 3: Build a Zero Trust Architecture

Implementing a ZTA through protect surface projects is a journey that modifies the existing infrastructure and processes rather than replaces what has already been implemented. Designing protect surface projects involves mapping transaction flows, identifying controls and secondary protect surfaces, and ultimately designing a system or solution. Even in a completely new environment, transitioning to ZTA within a single technology refresh cycle is improbable. Adapting existing workflows to ZTA likely necessitates, at the very least, a partial overhaul. How an enterprise migrates to a strategy depends on its current cybersecurity posture and operations. Migrating to ZTA requires an organization to have detailed knowledge of its assets (physical and virtual), subjects (including user privileges), and business processes.

Let us put these principles into plain and practical language. The protect surface with the most sensitive assets is in most need of ZT. Temptation: address this surface first. However, the services, assets or business data contained therein might need approvals from more than one department. As we mentioned earlier, as a strategic thinker, you may benefit from delivering a faster or easier win. To establish confidence and trust within the organization, you can opt to improve a protect surface that needs less approvals and less time to complete – the low-hanging fruit.

Another strategy might be to look at protect surfaces where you can build some shared services, or consolidate some technologies. Your benefit here is in showing value and then repeating what you have done on other protect surfaces. With each consecutive instance producing better results in less time. Something complex, such as centralization of Identity Providers (IdP centralization), may be challenging in situations where you are implementing a centralized IdP in a large or complex organization, running legacy systems and diverse application environments. Visible benefits may include simplified management, a better user experience or improved compliance with regulatory requirements[22].

ZT frameworks are not tied to any specific technology, allowing organizations to fully customize their security measures based on their unique protection needs. This flexibility allows for a security approach that is focused on critical protect surfaces within the organization. Dividing the network into smaller, distinct segments to limit access and contain potential breaches, ensuring that even if one segment is compromised, others remain secure heightens security and control over data flow within the organization. Enterprises can adopt various approaches to implement ZTA, emphasizing different components and policy rules. These approaches, namely governance-driven enhanced identity, logical micro-segmentation, network-based segmentation, cloud usage and outsourcing, and even removal of the corporate network altogether, all can adhere to ZT principles.

[21] NIST. (2020). *Zero Trust Architecture* (SP 800-207)

[22] See NSTAC. (2022). NSTAC Report to the President on *Zero Trust and Trusted Identity Management*. Appendix A and B for more ideas.

Typically, a complete ZT solution incorporates many different elements. The suitability of each approach varies, depending on the strategic business direction and risk defined by the board, and should flow down into the architectural solution chosen. While one approach may align seamlessly with a chosen use case and policies, it doesn't imply that other approaches wouldn't work. Indeed, alternative approaches, while more challenging to implement, may provide better long term alignment with the overall strategic business direction.

Depending on the enterprise, multiple ZTA deployment models may be employed within a particular organization for various business processes.[23]

### 3.3.4 Step 4: Create Zero Trust Policy

ZT policies form the cornerstone of a secure ZTA. While these policies are initially static, they should be designed to evolve dynamically in tandem with the organization's progression in implementing and maturing its ZTA.

To effectively implement ZT, organizations should use the 5 W's plus How for policy creation. This method helps the effort focus on defining granular access controls and considerations for resource access. It also helps you to write specific policy statements and procedures, tailored to the protect surface access perspective. The list below outlines the key aspects that should be factored into any risk evaluation when creating ZT policies:

- **Who:** Determine which entities (people, devices, organizations, code, agents, etc.) should be allowed to access a particular resource.
- **What:** Understand the context in which the entity tries to access systems and/or data
- **When:** Define the time frames or conditions under which the entity may access the resource.
- **Where:** Identify the location, network, or geo-fence that allows the entity access.
- **Why:** Establish why the entity (the "Who") needs access to the resource, emphasizing the justification.
- **How:** Define the technological controls necessary to deliver appropriate risk-based controls to satisfy the 5 W's.

### 3.3.5 Step 5: Monitor & Maintain the Network

In the CISA ZTMM, visibility and analytics provide the insights that improve ZT operations. Knowing the current and dynamic state of each protect surface's security posture within the network (environment) is critical to any potential response. This involves a focus on logging, monitoring and prompt alerting. These components enable continuous improvement and an effective incident response framework. Regular feedback loops, efficient incident detection, a robust response plan, and the ongoing monitoring of activities are key to maintaining and updating policy rules.

It's also important to regularly review and modify the protect surface and automated policies, which can be achieved through quarterly reviews of ZT identity, devices, access, policies, and protect surfaces.

[23] To learn more about model variations, review these Cloud Security Alliance courses: *Introduction to Software-Defined Perimeter* and *Architectures and Components of Software-Defined Perimeter*.

By continually monitoring and updating each subsequent protect surface, organizations can progressively strengthen their security posture. Such continuous oversight not only enhances security but also improves operational efficiency, speed of access, and flexibility, contributing to overall productivity. Communicating these returns on investment to leadership is essential to acknowledge the long-term benefits of the ZT strategy.

# 4 Zero Trust & Operations

When organizations conduct a detailed technology landscape assessment, they should identify specific areas where Zero Trust (ZT) principles can and should be applied to optimize or extend existing controls. These enhancements encompass a range of security technologies, including continuous authentication and authorization, user and entity behavior analytics (UEBA), and dynamic policy enforcement points (PEPs). Automation and orchestration, based on the designed Zero Trust Architecture (ZTA), are ZT enablement items.

Here is a list of common operational areas impacted by ZT strategy:

- System administration;
- Network management;
- Data management;
- Performance monitoring;
- Helpdesk and support; and
- DevOps and engineering (access workflow).

This section delves into the multifaceted approach necessary to effectively adopt and integrate ZTA. It also emphasizes the need for a shift in corporate culture, tailored to each organization's unique business type and directorial objectives. Education initiatives are vital for both staff and senior management to understand and communicate the business value of ZT. This educational aspect is pivotal for gaining board buy-in and aligning ZT with the organization's strategic goals.

In response to the evolving cybersecurity regulatory landscape and the inadequacy of traditional security models, ZT offers a proactive and comprehensive framework to protect sensitive data and infrastructure. Organizations need to be aware of regulatory requirements in different regions and adapt their ZT strategy accordingly, especially those with legacy systems. The organization may need to adopt a vendor-based readymade solution to construct the automated workflow to integrate multiple ZTA elements. More orchestration at each step, such as during access and monitoring, can make the operation easier and more adoptable.

Finally, the integration of user experience (UX) and site reliability engineering (SRE) plays a critical role in the successful adoption of ZT. By focusing on UX and automated, code-driven solutions, organizations can foster greater team support, reduce human error, and ensure that security measures are both effective and user-friendly, ultimately enhancing their security posture and operational efficiency.

## 4.1 Cultural & Organizational Shift

The following list highlights areas for corporate culture shifts, tailored to each organization's specific business type and directorial objectives.

- Cultivate a ZT culture:
  - Emphasize people, processes and organizational aspects over technology acquisition.
  - Implement continuous monitoring, logging and responsive actions.
- Change the tone from the top:
  - Secure executive endorsement and support for ZT initiatives, ensuring leadership commitment.
  - Develop a communications plan for consistent stakeholder alignment and guidance on the ZT journey.
- Instill a culture of continuous risk management:
  - Continuously assess and measure risk to guide access decisions and align with risk appetite.

## 4.2 Training & Education

Educational initiatives help ensure IT staff, senior management and line-of-business (LOB) managers understand the new ZT paradigm. ZT-informed executives are key to communicating ZT's business value, especially in getting board buy-in. This involves demonstrating how ZT aligns with the organization's strategic objectives. In parallel, it is important to educate the broader workforce. This education should focus on differentiating ZT principles from mere technology tools, helping employees understand the fundamental concepts of ZT. Training reaching the broader workforce should also provide an understanding of revised roles within the ZT framework.

Where applicable, the organization's audit functions (both internal and external) need to participate in the educational process. Auditors need to be informed about how ZT architecture enhances organizational security and resilience.

Lastly, ZT training should be integrated into the existing training program for all staff. This integration ensures that future updates, scheduling and necessary refreshes are consistently applied and not overlooked by the organization's training and education functions.

## 4.3 Regulatory & Compliance Shift

The cybersecurity regulatory landscape is undergoing a dynamic transformation, spurred by the escalating complexity and frequency of cyber threats. Traditional security models are increasingly inadequate in this environment, prompting governments and industry regulators to endorse proactive and comprehensive frameworks like ZT for safeguarding sensitive data and critical infrastructure.

In this evolving scenario, specific regulations and compliance standards, such as General Data

Protection Regulation (GDPR)[24] and Health Insurance Portability and Accountability Act (HIPAA)[25], are being updated to necessitate the adoption of ZT-aligned security controls. This trend is especially pronounced in the finance, healthcare and government sectors, where the sensitivity of stored personal data heightens the urgency. While not all regulations mandate ZT principles yet, the shift is undeniable in these highly regulated industries, where compliance is not just a legal formality but a critical defense against modern cyber threat.

### 4.3.1 Regional Regulations

Organizations must stay informed about the regulatory requirements in the countries and regions where they store data and operate. The advent of new regulations often brings the need for specific assessments or attestations, particularly during transitions to ZTAs.

In the United States, for instance, compliance with the Federal Information Security Management Act (FISMA) becomes crucial for US federal government entities, and their suppliers and service providers. This often necessitates optimization and automation of compliance tasks. The reasoning behind this is linked to the requirements of FISMA, which mandates that agencies undergo a rigorous cycle of assessment and reauthorization of systems, especially when making significant changes like adopting ZT. The challenge lies in legacy environments, where agencies frequently find it difficult to keep pace with these demanding tasks, resulting in potential delays or constraints in fully transitioning to a ZT framework.

## 4.4 Legacy Systems & Infrastructure

Specialized technologies – sometimes legacy-based – such as OT, IoT or industrial control systems (ICS) devices, are often deployed within critical infrastructure services and often have significant technical constraints in key areas, such as patching and access control. This and similar technologies may require implementing specialized micro-perimeter access control technologies and strategies to achieve ZT objectives for such infrastructure.

Organizations with legacy systems and traditional trust models often encounter challenges in adopting ZT, particularly due to limited network and asset visibility. As we have mentioned in other sections, the transition to ZT varies with each organization's unique attributes, including its maturity level, mission and specific challenges. Not all legacy systems require immediate ZT upgrades, but any updates should be strategically planned to address emerging threats and system modernization.

Legacy infrastructure influences the adoption of ZT models. For example, the Information Security Continuous Monitoring (ISCM) model requires adaptable systems for its data movement workflows. Legacy systems' rigidity can hinder the implementation of such models. Additionally, an organization's experience with measurement programs affects its ability to adopt ZT, with more mature organizations adapting more easily than those with less developed measurement capabilities.

[24] General Data Protection Regulation is designed to protect data and privacy of European Union citizens.

[25] Health Insurance Portability and Accountability Act is United States legislation designed to, in part, protect a patient's health information.

## 4.5 Usability & Friction

This section explores the integral role of user experience (UX) and SRE[26] in promoting the adoption of ZT architecture in organizations. The focus is on refining UX to boost the acceptance of ZT principles while shifting towards a more automated, code-driven approach. This shift not only enhances team support but also minimizes human error, thus strengthening SRE practices. The synergy between UX and SRE ensures that security measures are not only effective but also user-friendly, enhancing the organization's security posture and ensuring smooth operational processes. The key to fostering ZT acceptance among employees is to prioritize UX and implement solutions through code and automation, leading to greater team buy-in and improved SRE outcomes.

### 4.5.1 User Experience

Incorporating UX helps encourage ZT acceptance and adoption within an organization. A key aspect of this is transitioning from manual processes to code-based automation. By leveraging automation and code, team acceptance is increased, and the likelihood of human error is significantly reduced. This shift improves SRE practices. A well-designed UX ensures that security measures are robust and user-friendly, fostering a more secure and efficient work environment.

### 4.5.2 Site Reliability Engineering

SRE combines software engineering and IT operations to build scalable and reliable systems. Focused on proactive management through continuous monitoring, automation, orchestration and scalability, SRE planning is a key part of ZT security, helping to maintain system integrity and resilience, including early vulnerability detection and efficient resource management.

Applicable to both cloud-based and on-premises environments, SRE's principles, such as automation, performance monitoring and incident management, universally enhance system reliability, regardless of the hosting setup.

Automation and orchestration (AO) are usually coupled terms, enabling ZT improvement in two important ways. First, AO provide automated feedback that improves access controls, policies, and enforcement, based on feedback loops.

Second, with infrastructure as code (IaC) and automated compliance checks, automated scripts and tools can continuously check compliance with ZT policies, ensuring that any deviations are quickly detected and rectified. AO also enables rapid response to detected threats by automatically adjusting access controls and network configurations in real-time. IaC helps prevent infrastructure drift – the phenomenon where the live state of the network diverges from the state defined in code. This alignment is vital for maintaining the integrity of ZT policies.

#### 4.5.2.1 Monitoring & Understanding System Compromises

In ZT security, monitoring the technology stack is crucial for vulnerability detection, with SRE enhancing this through continuous system monitoring and logging. This approach enables quick iden-

[26] Google. (2016) Site Reliability Engineering.

tification of potential breaches and supports proactive security measures. Additionally, SRE aids in understanding system compromises through postmortem analysis and learning from failures, which is essential for secure recovery and resilience enhancement. Practices like thorough incident documentation and blameless postmortems help teams understand root causes and reinforce system defenses.

### 4.5.2.2 Resource & Component Management

In the context of ZT security, deploying immutable resources may play a crucial role, and this is where SRE becomes significant. Immutable resources refer to infrastructure components that, once deployed, are not modified. Instead, if changes are needed, new instances of the resources are deployed. SRE facilitates this by automating the deployment process, ensuring that new instances are consistent, reliable, and verifiable. This approach reduces the risk of configuration drift and unauthorized changes, aligning well with the ZT principle of "never trust, always verify." SRE's focus on automation and reliability ensures that deploying immutable resources is efficient and secure.

A decisive and swift response may be necessary when a system component is compromised. This approach is akin to rapidly decommissioning and replacing – effectively and quickly removing and substituting the compromised component with a new, secure instance. SRE supports this rapid response strategy with practices like infrastructure as code and automated deployment pipelines. These practices allow for the quick rollout of new, unaffected instances, minimizing downtime and exposure to threats. By automating the replacement process, SRE ensures that the response to security incidents is fast and reliable.

# Conclusion

In Zero Trust (ZT), the levels of strategic engagement include several components. At the top is the organization's strategy, guiding overall actions and decisions. Below this, at the strategy level, ZT redefines traditional trust concepts in computing, emphasizing continuous verification due to the inevitability of breaches.

Aligning ZT with organizational values involves understanding its adoption drivers, like compliance and security enhancement, and how it offers competitive advantages such as streamlined security and cost reduction. Risk management is key, focusing on protecting digital assets and requiring clear ownership for risk handling.

Building a business case for ZT involves assessing financial and performance impacts, gaining cross-departmental stakeholder buy-in, and aligning it with organizational strategy. Tactics for ZT implementation include focusing on specific business outcomes, internal security design, and managing access permissions.

Successful ZT adoption necessitates a cultural shift, integrating continuous risk management, executive support, and comprehensive education across all organizational levels. It also involves adapting to regulatory changes. Overall, ZT is a cybersecurity approach that requires strategic alignment, planning, and execution for full effectiveness.

# Glossary

For additional terms, please refer to our Cloud Security Glossary, a comprehensive glossary that combines all the glossaries created by CSA Working Groups and research contributors into one place.

# Acronym List

| Acronym | Term |
|---|---|
| AD | Active Directory |
| AO | Automation and Orchestration |
| BYOD | Bring Your Own Device |
| C-Suite | Chief-Suite |
| CBA | Cost/Benefit Analysis |
| CFO | Chief Financial Officer |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| COO | Chief Operating Officer |
| DAAS | Data, Applications, Assets and Services |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| FISMA | Federal Information Security Management Act |
| HR | Human Resources |
| IaC | Infrastructure as Code |
| ICS | Industrial Control Systems |
| IdP | Identity Providers |
| IoT | Internet of Things |
| IP | Intellectual property |
| ISCM | Information Security Continuous Monitoring |
| IT Ops | Information Technology Operations |
| LOB | Line of Business |
| MFA | Multi-Factor Authentication |
| NSTAC | National Security Telecommunications Advisory Committee |
| NTP | Network Time Protocol |
| OT | Operational Technology |

| | |
|---|---|
| PAW | Privileged Access Workstations |
| PCI | Payment card industry |
| PDPs | Policy Decision Points |
| PEPs | Policy Enforcement Points |
| PHI | Protected health information |
| PII | Personally identifiable information |
| PoS | Point-of-Sale |
| ROI | Return on Investment |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| SOAR | Security, Orchestration, Automation, and Response |
| SOC | Security Operation Center |
| SRE | Site Reliability Engineering |
| SWOT | Strengths, Weaknesses, Opportunities, and Threats |
| TPRM | Third-Party Risk Management |
| UEBA | User and Entity Behavior Analytics |
| UX | User Experience |
| VPN | Virtual Private Network |
| ZT | Zero Trust |
| ZTA | Zero Trust Architecture |
| ZTMM | Zero Trust Maturity Model |