The Open Group Guide

Zero Trust Commandments

The Open Group Guide

Zero Trust Commandments

ISBN: 1-947754-86-7

Document Number: G21F

Published by The Open Group, December 2021.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

1 Introduction 1
- 1.1 Objective 1
- 1.2 Overview 1
- 1.3 Level-Setting the Zero Trust Commandments 1
  - 1.3.1 Assume Failure and Assume Success 2
  - 1.3.2 Advocate for Simplicity 3
  - 1.3.3 View as a Continuous Journey 3
- 1.4 Terminology 4
- 1.5 Future Directions 4

2 Zero Trust Commandments High-Level Summary 5

3 Zero Trust Commandments 6
- 3.1 Validate Trust Explicitly 6
- 3.2 Enable Modern Work 7
- 3.3 Enable Pervasive Security 8
- 3.4 Secure Assets by Value 9
- 3.5 Implement Asset-Centric Controls 10
- 3.6 Enable Simple and Sustainable Security 11
- 3.7 Utilize Least Privilege 12
- 3.8 Improve Continuously 13
- 3.9 Make Informed Decisions 14

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 800 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

This Document

This document is The Open Group Guide to Zero Trust Commandments. It has been developed and approved by The Open Group.

This document is intended for leaders in business, security, and IT – namely, executives. The Commandments in this document originate and extend from the principles contained in The Open Group White Paper: Zero Trust Core Principles (see Referenced Documents). The Commandments are presented first together on a single page and then separately, each on its own page, with further detail.

Trademarks

Acknowledgements

(Please note affiliations were current at the time of approval.)

The Open Group gratefully acknowledges the contribution of the following people in the development of this document:

- Chris Carlson, President, C T Carlson LLC
- Anthony (Tony) Carrato, The Open Group Invited Expert
- Jim Hietala, VP, Business Development & Security, The Open Group
- Nikhil Kumar, President, Applied Technology Solutions, Inc. and ZTA Working Group Co-Chair (Architecture Forum)
- Michael (Mike) Leuzinger, AVP, Chief Architect for Information Risk Management, Nationwide
- John Linford, Security & OTTF Forum Director, The Open Group
- Carmichael Patton, Senior Program Manager & Lead Zero Trust Architect, Microsoft
- Sai Mohan Sakuru, Client Security Partner & ADH, Wipro Limited
- Mark Simos, Lead Cybersecurity Architect, Microsoft and ZTA Working Group Co-Chair (Security Forum)
- Andras Szakal, VP & Chief Technology Officer, The Open Group
- Altaz Valani, Director of Insights Research, Security Compass and Vice-Chair (Security Forum)
- Stephen (Steve) Whitlock, The Open Group Invited Expert

The Open Group gratefully acknowledges the following reviewers who participated in the review of this document:

- Vicente A. Canal, CEO, ISM3 Consortium
- Mats Gejnevall, Enterprise Architect, Biner Consulting

Referenced Documents

The following documents are referenced in this Guide.

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- Axioms for the Practice of Security Architecture, The Open Group Guide (G192), published by The Open Group, July 2019; refer to: www.opengroup.org/library/g192
- CNSSI 4009: Committee on National Security Systems (CNSS) Glossary, April 2015; refer to: https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary
- IETF RFC 2219: Key Words for Use in RFCs to Indicate Requirement Levels, March 1997; refer: to https://www.rfc-editor.org/info/rfc2119
- ISO Guide 73:2009: Risk Management – Vocabulary, November 2009; refer to: https://www.iso.org/standard/44651.html
- NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View, March 2011; refer to: https://csrc.nist.gov/publications/detail/sp/800-39/final
- NIST SP 800-53 (Rev. 5): Security and Privacy Controls for Information Systems and Organizations, September 2020; refer to: https://doi.org/10.6028/NIST.SP.800-53r5
- NIST SP 800-152: A Profile for US Federal Cryptographic Key Management Systems, October 2015; refer to: http://dx.doi.org/10.6028/NIST.SP.800-152
- NIST SP 800-171 (Rev. 2): Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations, February 2020; refer to: https://doi.org/10.6028/NIST.SP.800-171r2
- NIST SP 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview, June 2017; refer to: https://doi.org/10.6028/NIST.SP.1500-201
- NISTIR 5153: Minimum Security Requirements for Multi-User Operating Systems, March 1993; refer to: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5153.pdf
- The Open Group Standard for Risk Analysis (O-RA), published by The Open Group, November 2021; refer to: http://www.opengroup.org/library/c20a
- The Open Group Standard for Risk Taxonomy (O-RT), published by The Open Group, November 2021; refer to: http://www.opengroup.org/library/c20b
- What is Infrastructure as Code?, Microsoft®, June 2021; refer to: https://docs.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code

- Zero Trust Core Principles, White Paper (W210), published by The Open Group, April 2021; refer to: www.opengroup.org/library/w210

1 Introduction

1.1 Objective

The Zero Trust Commandments build on the Zero Trust Core Principles[1] to present a non-negotiable list of criteria for Zero Trust. In putting this list together, we want to present a clear definition of what Zero Trust is and what it is not. Having a clear definition allows our communities to start building frameworks and solutions that adhere to these Commandments. We believe Zero Trust is, ultimately, a business enabler, and these Commandments reflect that bias.

In an ideal scenario, these Commandments will withstand the test of time. An essential component to ensure this longevity is keeping the Commandments as assertions that can be tested. Missing the mark on any of these Commandments reflects a diversion from the definition of Zero Trust as we see it. We recognize that organizations have often made decisions that do not follow these Commandments, but these Commandments are intended to guide all current and future decisions.

The Zero Trust Commandments will underpin additional, actionable artifacts that organizations can use as they undergo their Zero Trust transformations. These Commandments also provide a defensible narrative around any actions taken during a Zero Trust transformation.

1.2 Overview

The Zero Trust Commandments in this document are presented first together as high-level statements on a single page (see Chapter 2).

Following the high-level summary, the Commandments are presented as imperative "shall" statements (see Section 1.4 for terminology definitions) with several supporting and explanatory points beneath each Commandment (see Chapter 3). These supporting points are all "must" statements.

Note: Discussion of how to implement the Zero Trust Commandments by industry in an architecture will occur in future publications.

1.3 Level-Setting the Zero Trust Commandments

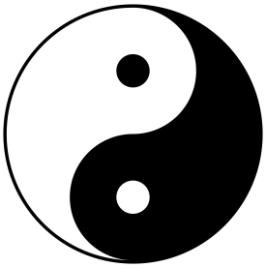
These level-setting imperatives form the foundation for the Commandments and drive full lifecycle thinking that is key to a Zero Trust transformation. These imperatives underpin all the Commandments, and the Commandments lean on them either explicitly or implicitly.

[1] Documented in The Open Group White Paper: Zero Trust Core Principles (see Referenced Documents).

We acknowledge that some Commandments or their components may at present be aspirational, dependent upon today's technology – this should not prevent an organization from attempting to implement and follow as many of the Commandments as is currently possible.

1.3.1 Assume Failure and Assume Success

Becoming resilient requires simultaneously accepting the reality of both positive and negative outcomes – attacks will inevitably happen, and you can manage them (detect, prevent, and/or recover from them). This duality is fundamental for navigating the complex challenges of security.



The Zero Trust Commandments are based on the following dual assumptions. The combination of these assumptions enables resilience by enabling realistic prioritization of security efforts across the full lifecycle: identify, protect, detect, respond, and recover. *These help drive a sense of purpose and optimism, knowing that the organization will face and overcome any security crisis.*

Zero Trust means you are as prepared as possible to handle failure and be successful.

Assume Failure

The purpose of this assumption is to expand on the concept of "assume breach/compromise" and to ground organizations in the reality of an open environment where security risk will always exist. You must assume that anything could go wrong – users will forget or make mistakes; attackers will succeed in gaining control of data and computer systems (in part or as a whole); and trusted insiders will occasionally go bad. This is the security analog of the "fail safe" engineering practice that assumes failure will happen and ensures the system fails to a safe state (to minimize harm to people, the environment, or other equipment).

Important: This negative assumption represents a fundamental shift from a classic security assumption of perfect security on internal networks or resources. This forces everyone to face the reality that perfect security is impossible for anything (data, other business assets, network, etc.). Security is not a technical problem to be solved once, but an ongoing discipline to be practiced.

Assume Success

The purpose of this assumption is to complement the assumption of failure and keep focus on preventing and rapidly recovering from incidents. Always assume that the mission and business must and will continue despite any failures that can and will happen. Many attacks can be blocked; people will overcome obstacles and learn; systems can be cleaned, restored, or rebuilt – business operations and the mission will continue.

1.3.2 Advocate for Simplicity

In addition to driving simplicity of security processes (captured in the Commandments below), security teams should also act as an advocate for understanding and simplifying the technical environment and business processes of the organization. Constraining complexity of the environment reduces the number of variables, considerations, and exceptions that must be managed by people or by automation (scripts, programs, etc.). Any simplification to and/or standardization of the technology environment benefits many aspects of the organization (manageability, agility, etc.), and security teams become more able to provide effective, pervasive, and sustainable assurances.

Many organizations deal with multiple generations of platforms, legacy systems, and architectural patterns. These lead to an ever-expanding growth in complexity over time, which is often exacerbated by consumer expectations of businesses to move faster and rapidly adopt new platforms. This complexity growth is even more explosive if governance does not restrain the procurement of duplicative technology solutions, further adding overhead to and difficulty of providing security and other assurances. Instead, the organization should aim for a simple environment in which the same solutions are provided consistently for the same needs (uniformity), reusing patterns, technologies, and business processes that are known to work.

Security teams must advocate for simplicity as a means of reducing business risk while the organization undergoes digital, cloud, and Zero Trust transformations. As part of this, the security teams should clearly and concisely communicate Zero Trust strategy and implementation across the organization.

1.3.3 View as a Continuous Journey

The transition to Zero Trust Architecture (ZTA) is a journey, and change does not happen all at once. Any organization undergoing the transition to Zero Trust Architecture must acknowledge and accept that progress will happen incrementally and that the organization and its environment must evolve continuously.

The Zero Trust Commandments should be applied to all current and future decisions. Implementing the Commandments will require an initial investment of time, effort, and energy that will potentially cause business disruption and delay, but the Commandments – when implemented – will result in increased security and business agility.

Zero Trust ultimately represents a change in strategy or perception of security, ensuring continuous enablement of business objectives while managing risk. These Commandments enable organizations to address the shifting mindset and culture change required for Zero Trust, linking people, processes, and technology.

As progress occurs, it should be celebrated within the organization. A “fully implemented” Zero Trust Architecture is not needed to benefit from the transition.

1.4 Terminology

For the purposes of this document, the following terminology definitions[2] apply:

Can	Describes a possible feature or behavior available to the user or application.
May	Describes a feature or behavior that is optional. To avoid ambiguity, the opposite of "may" is expressed as "need not", instead of "may not".
Shall	Describes a feature or behavior that is a requirement. To avoid ambiguity, do not use "must" as an alternative to "shall".
Shall not	Describes a feature or behavior that is an absolute prohibition.
Should	Describes a feature or behavior that is recommended but not required.
Will	Same meaning as "shall"; "shall" is the preferred term.

1.5 Future Directions

These Zero Trust Commandments will act as the foundation for future publications of The Open Group Zero Trust Architecture Working Group. These future publications include:

- A Zero Trust Reference Model that describes the core capabilities, architectural building blocks, and governance, risk, and compliance considerations for Zero Trust
- A Practitioners Guide to provide actionable steps for implementing Zero Trust
- A Business Guide to provide guidance to senior and C-level executives on Zero Trust
- A Zero Trust Reference Architecture that defines Zero Trust capabilities and implementation and interoperability requirements and allows contribution of Reference Implementations for different industries

[2] These definitions are consistent with other well-known and widely utilized definitions, such as those from IETF RFC 2219.

2 Zero Trust Commandments High-Level Summary

The Zero Trust Commandments are presented here together, on a single page, as high-level statements.

Table 1: Zero Trust Commandments – Summary

Commandment	High-Level Statement
Validate Trust Explicitly	Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.
Enable Modern Work	Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.
Enable Pervasive Security	Security discipline shall be integrated into the culture, norms, and processes throughout the organization.
Secure Assets by Value	Security controls shall be designed to protect business assets appropriate to their business value and expected risk.
Implement Asset-Centric Controls	Asset-specific security controls (*versus* broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.
Enable Simple and Sustainable Security	Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.
Utilize Least Privilege	Access to systems and data shall be provided only as required, and access shall be removed when no longer required.
Improve Continuously	Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.
Make Informed Decisions	Security teams shall make informed decisions based on the best information that can be made available.

3 Zero Trust Commandments

3.1 Validate Trust Explicitly

Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.

1. **Verify Access Control** – The organization must validate user authentication strength, session context, and device integrity before allowing a user or device to access the organization's assets (and continuously during each session if available).
2. **Verify Application Development** – The organization must define and follow secure development lifecycle processes and infrastructure as code and verify that they are followed.
3. **Verify Technology Supply Chain** – The organization must be able to verify on-demand the provenance and integrity (i.e., lack of counterfeiting or tainting) of technology components.
4. **Verify Host Configuration** – The organization must be able to verify on-demand that operational deployment complies with the security control requirements established per platform.
5. **Verify Incident Processes** – The organization must be able to verify security and business continuity processes (e.g., ability to detect and respond to incidents, including restoring business operations).

3.2 Enable Modern Work

Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.

1. **Work Anywhere** – People must be able to work on any network, in any location, with appropriate security assurances and access restrictions. People should have access to all applications required to do their jobs.
2. **Align to Mission** – Security strategy, success metrics, and policies must map directly to the organizational mission and business model or plan.
3. **Assign Security Risk to Asset Owners** – The organization must assign accountability for security risk to business asset owners, like all other risks. Security teams must act as subject-matter experts to advise asset owners on security risk.
4. **Align Risk Management** – The organization must measure and manage risk using its risk management framework and processes (thresholds, prioritization, stakeholders, etc.).

3.3 Enable Pervasive Security

Security discipline shall be integrated into the culture, norms, and processes throughout the organization.

1. **Integrate in Business Environment** – The organization must integrate security context into business strategy, planning, operations, acquisition, contracting, and outsourcing.

2. **Integrate in Technical Environment** – The organization must integrate security controls into modern workflows, application and solution architectures, migrations to hybrid-cloud and cloud environments, new application development, Artificial Intelligence (AI) and Machine Learning (ML) projects, implementation of agile practices, and other emerging technologies.

3. **Incorporate Security Education and Awareness Training** – The organization must incorporate security education and awareness training for employees, partners, contractors, and suppliers to demonstrate the importance of Zero Trust and how it should be adopted in new acquisitions, application development, and IT changes on a regular basis so that it is understood and adopted throughout the entire lifecycle.

3.4 Secure Assets by Value

Security controls shall be designed to protect business assets appropriate to their business value and expected risk.

1. **Map Technology to Business** – The organization must identify important business assets and translate them into technical assets[3] that compose them, including consideration of systems with direct administrative control.

2. **Classify Information Assets** – Organizations should classify mission-critical assets that drive certain business process (e.g., for insurance companies, a business process can be life insurance, health, savings, retirements, etc.) essential to meeting end-client business objectives. The classification of assets will support arriving at Confidentiality, Integrity, and Availability (CIA) ratings.

3. **Increase Security for Sensitive Assets** – Security controls must match asset value and sensitivity to ensure protection of high-value data and applications.

4. **Reduce Unneeded Sensitivity** – The organization must reduce asset sensitivity where possible to avoid wasting efforts of security and other teams (e.g., retire or replace unneeded sensitive assets, remove sensitive or regulated data with low-value tokens, etc.).

5. **Stay Current** – The organization must update security assurances for the asset (CIA, safety) as the asset use-cases, threats, and value change over time.

[3] Defined in the Glossary.

3.5 Implement Asset-Centric Controls

Asset-specific security controls (*versus* broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.

1. **Implement Data-Centric Controls** – Data-centric security controls must enable appropriate protection for data in any location and on any network.

2. **Implement Application-Centric Control**s – Application-centric security controls must help ensure workloads are protected on any location (cloud, on-premise, or otherwise), including when attackers can access the corporate network. This may include controls on the application itself or application-aware infrastructure controls (identity, network, etc.) that focus on the context of the application, its users, and related context (sometimes called micro-segmentation).

3. **Determine Trust beyond the Network** – Broad network security controls (not application-centric) must be focused on proven use-cases, such as filtering basic Internet traffic, isolating networks with legacy applications or devices (e.g., Operational Technology (OT)), meeting regulatory requirements, and providing high-quality threat detections (e.g., high true positive rate). This is because a network does not impart trust on an asset; network security controls can protect assets, but cannot protect "the network" itself and derive asset security or trust from it.

3.6 Enable Simple and Sustainable Security

Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.

1. **Simplify Human Experience** – Security controls must minimize manual steps required and workflow disruption for business users and IT personnel, including providing self-service resolution where possible.

2. **Simplify Security** – The organization must favor automated controls and reporting for security risk to enable security teams to execute at speed commensurate with the organization.

3. **Provide Clarity** – The organization must clearly define accountability, written policy, and aspirational visions to enable consistent security decision-making.

4. **Configure before Customize** – The organization must base security controls on accepted best practices and implemented (incrementally or fully) within a reasonable time considering available resources – people, process, technology, time. To the degree possible, standardize on organization-wide platforms for IT and security to ensure consistent visibility, management, and control.

5. **Secure for the Full Lifecycle** – Security programs and strategies must cover the full lifecycle of the business asset, including identify, protect, detect, respond, and recover.

6. **Utilize an End-to-End Approach** – Security governance must sustain security assurances for the full lifecycle of the data, transaction, or relationship.

3.7 Utilize Least Privilege

Access to systems and data shall be provided only as required, and access shall be removed when no longer required.

1. **Grant Just Enough Access** – The organization must limit access (for a person, in a session, etc.) to only the systems and data required to perform a task.

2. **Grant Just-in-Time Access** – The organization must provide access on-demand, as needed, and only with appropriate approval and validation.

3. **Utilize Adaptive Access** – The organization must adjust access permissions over the lifetime of the session in real time (as possible) and the lifetime of the account to prevent accumulation of unneeded privilege and unnecessary risk.

3.8 Improve Continuously

Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.

1. **Consider People, Process, and Technology** – Security teams must continuously improve all aspects of the security program, tooling, and skills, constantly monitoring and seeking and applying feedback.
2. **Consider Business Evolution** – Security teams must continuously adapt to evolving business drivers and models, preventing the creation of obstacles for business and/or mission success through either action or inaction.
3. **Consider Technical Evolution** – Security teams must continuously adapt to feature and product release and adoption cycles of technology.
4. **Consider Security Evolution** – Security teams must continuously monitor and adjust to current and future threats as they emerge, as well as new best practices, architectures, technologies, etc.

3.9 Make Informed Decisions

Security teams shall make informed decisions based on the best information that can be made available.

1. **Decide with Data** – Security teams must use all applicable data to inform security decisions regarding access control, anomaly detection and investigation, risk assessment, planning, design, etc.

2. **Constantly Gather Telemetry** – Security teams must build and sustain a current and accurate understanding of the technical environment by continuously monitoring all assets (services, apps, identities, data, etc.) for insights and anomalous patterns.

3. **Prioritize using Data** – The organization must prioritize security investments based on risk analyses informed by current information on active threat actors and technical attack techniques (from the organization, industry peers, and other organizations).

4. **Combine Data with Human Wisdom** – Security teams must minimize the impact of any decision bias by applying critical thinking and human experience to available data. Consider any differences between actual and expected outputs as learning opportunities to examine further.

5. **Constantly Grow your Telemetry** – Security teams must continuously seek new information sources as the organization's business model, technical platforms, threats, and security capabilities evolve. Security teams must constantly increase visibility into known assets, discovery of expected assets, and discovery of new asset types.

Glossary

Access

The ability to make use of any information system resource. [Source: CNSSI 4009-2015]

Access Control

The process of granting or denying specific requests:

1. For obtaining and using information and related information processing services
2. To enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances)

[Source: CNSSI 4009-2015]

Asset

The information, information system, or information system component that is breached or impaired by the threat agent in a manner whereby its value is diminished or the act introduces liability to the primary stakeholder. [Source: The Open Group O-RT Standard]

Business Value

Refers to value to the organization, whether defined in business terms and/or mission success.

Capacity for Loss

An objective measure of how much damage an organization can incur and still remain solvent. [Source: The Open Group O-RA Standard]

Cyber-Physical Systems (CPS)

- Comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic
- Provide the foundation of critical infrastructure
- Form the basis of emerging and future smart services
- Improve quality of life in many areas – bring advances in personalized healthcare, emergency response, traffic flow management. [Source: NIST SP 1500-201]

Infrastructure as Code

The management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as a DevOps team uses for source code. [Source: Microsoft®]

Internet of Things (IoT)

The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information. [Source: NIST SP 800-171 (Rev. 2)]

Least Privilege

The principle that principals (people, things, processes, etc.) shall be granted only the rights necessary to perform their authorized tasks. [Source: Axioms for the Practice of Security Architecture]

Privilege

A special authorization that is granted to particular users to perform security-relevant operations. [Source: NISTIR 5153]

Risk

The probable frequency and probable magnitude of future loss. [Source: The Open Group O-RT Standard]

Risk Analysis

The process to comprehend the nature of risk and determine the level of risk. [Source: ISO Guide 73:2009]

Risk Assessment

The overall process of risk identification, risk analysis, and risk evaluation. [Source: ISO Guide 73:2009]

Risk Management

Coordinated activities to direct and control an organization with regard to risk. [Source: ISO Guide 73:2009]

Security Assurance

The measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. [Source: NIST SP 800-39]

Security Control

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. [Source: NIST SP 800-53 (Rev. 5)]

Technical Assets

IT systems (such as data, applications, and APIs), Operational Technology (OT), Internet of Things (IoT) devices, analog assets, networks, and Cyber-Physical Systems (CPS).

Telemetry

A collection of data that provides an understanding of environments, measures risk reduction, and enables machine learning and artificial intelligence for anomaly detection. Telemetry can come from endpoint log collection, auditing authentication requests, application monitoring, or any other source of data that can be derived from the environment. Telemetry must be aggregated in a way that allows for disparate data sets to reflect common data patterns in order to allow for simple correlation between the sets.

Threat

Anything that is capable of acting in a manner resulting in harm to an Asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures. [Source: The Open Group O-RT Standard]

Threat Agent

Any agent (e.g., object, substance, human) that is capable of acting against an Asset in a manner that can result in harm. [Source: The Open Group O-RT Standard]

Tolerance for Loss

The subjective preference and management mandate for loss in an organization. [Source: The Open Group O-RA Standard]

Trust

A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly, and impartially, along with assurance that the entity and its identifier are genuine. [Source: NIST SP 800-152]

Zero Trust

An information security approach that focuses on data/information security, including lifecycle, on any platform or network. [Source: The Open Group White Paper: Zero Trust Core Principles]

Zero Trust Architecture

The implementation of a Zero Trust security strategy that follows well-defined and assured standards, technical patterns, and guidance for organizations. [Source: The Open Group White Paper: Zero Trust Core Principles]

Acronyms & Abbreviations

AI	Artificial Intelligence
API	Application Program Interface
CIA	Confidentiality, Integrity, and Availability
CNSSI	Committee on National Security Systems
CPS	Cyber-Physical Systems
IoT	Internet of Things
ML	Machine Learning
NIST	National Institute of Standards and Technology
O-RA	The Open Group Standard for Risk Analysis
O-RT	The Open Group Standard for Risk Taxonomy
OT	Operational Technology
SP	Special Publication
ZTA	Zero Trust Architecture

Index

access....15
access control....6, 15
adaptive access....12
agility....3
application-centric controls....10
assertions....1
asset....15
  classification....9
  owners....7
  sensitivity....9
assume failure/success....2
awareness training....8
broad network controls....10
business asset....9
  lifecycle....11
business enabler....1
business environment....8
business evolution....13
business value....15
capacity for loss....15
CIA....9
Commandments
  high-level statements....5
  level-setting imperatives....1
consistency....11
continuous improvement....13
continuous journey....3
CPS....15
data-centric controls....10
development lifecycle....6
host configuration....6
incident recovery....2
informed decisions....14
infrastructure as code....6, 16
IoT....16
just-in-time access....12
least privilege....12, 16
mobility....7
organizational mission....7
pervasive security....8
prioritization....2
privilege....16
provenance and integrity....6
risk....16
risk analysis....14, 16
risk assessment....16
risk management....3, 7, 16
security assurance....16
security attack....2
security control....17
security discipline....2
security education....8
security evolution....13
security governance....11
security incidents....6
security risk....2
simplicity....3
simplification....11
sustainable security....11
technical assets....17
technical environment....8
technical evolution....13
technology supply chain....6
telemetry....14, 17
threat....17
threat agent....17
tolerance for loss....17
transformation....3
trust....6, 17
uniformity....3
user authentication....6
Zero Trust....17
  definition....1
  transformation....1
Zero Trust Architecture....3, 18
Zero Trust Reference Architecture....4
Zero Trust Reference Model....4
ZTA Working Group....4