The Open Group Standard

Zero Trust Reference Model (Snapshot)

NOTICE

Snapshot documents are draft standards, which provide a mechanism for The Open Group to disseminate information on its current direction and thinking to an interested audience, in advance of formal publication, with a view to soliciting feedback and comment.

A Snapshot document represents the interim results of an activity to develop a standard. Although at the time of publication The Open Group intends to progress the activity towards publication of a Preliminary Standard or (full) Standard of The Open Group, The Open Group is a consensus organization, and makes no commitment regarding publication. Similarly, a Snapshot document does not represent any commitment by any member of The Open Group to make any specific products available.

This Snapshot document is intended to make public the direction and thinking about the path we are taking in the development of the Zero Trust Reference Architecture. We invite your feedback and guidance. To provide feedback on this Snapshot document, please send comments by email to ogspecs-snapshot-feedback@opengroup.org no later than April 30, 2024.

This Snapshot document is valid through April 30, 2024 only.

For information on joining the Security Forum, please send email to https://www.opengroup.org/join-forum.

The Open Group Standard

Zero Trust Reference Model (Snapshot)

ISBN: 1-957866-32-1

Document Number: S232

Published by The Open Group, October 2023.

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

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 900 organizations includes customers, systems and solutions suppliers, tool 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 are available at www.opengroup.org/library.

This Document

This is a Snapshot document of what is intended to become the Zero Trust Reference Model Standard. It is being developed by The Open Group.

This document builds on The Open Group Snapshot: Zero Trust Commandments to provide the basic concepts for and architectural building blocks of a Zero Trust Reference Model. The document also describes the relationships among these architectural building blocks.

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:

- Didier Beyens, DXC
- Chris Carlson, C T Carlson, LLC
- Tony Carrato, The Open Group Invited Expert
- Simon Cross, (formerly of) BizzDesign
- Mats Gejnevall, Biner Consulting
- Jim Hietala, The Open Group VP, Security & Business Development
- Nikhil Kumar, Applied Technology Solutions, Inc.
- Mike Leuzinger, Nationwide
- John Linford, The Open Group Security Forum & OTTF Director
- Carmichael Patton, Microsoft
- Andy Ruth, Sustainable Evolution, Inc.
- Mark Simos, Microsoft
- Andras Szakal, The Open Group VP & CTO
- Altaz Valani, (formerly of) Security Compass
- Steve Whitlock, The Open Group Invited Expert
- Hasan Yasar, Carnegie Mellon SEI

Referenced Documents

The following documents are referenced in this standard.

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

[C119] The Open Group Standard for SOA Reference Architecture (C119), published by The Open Group, December 2011; refer to: www.opengroup.org/library/c119

[C17B] The Open Information Security Management Maturity Model (O-ISM3), Version 2.0 (C17B), published by The Open Group, September 2017; refer to: www.opengroup.org/library/c17b

[C20A] The Open Group Standard for Risk Analysis (O-RA) (C20A), published by The Open Group, November 2021; refer to: http://www.opengroup.org/library/c20a

[C20B] The Open Group Standard for Risk Taxonomy (O-RT) (C20B), published by The Open Group, November 2021; refer to: http://www.opengroup.org/library/c20b

[C220] The TOGAF® Standard, 10th Edition (C220), published by The Open Group, April 2022; refer to: www.opengroup.org/library/c220

[Cheswick, 1990] The Design of a Secure Internet Gateway, by Cheswick, B, published April 1990; refer to: https://cheswick.com/ches/papers/gateway.pdf

[G202] SOA for Business Technology, The Open Group Guide (G202), published by The Open Group, February 2020; refer to: www.opengroup.org/library/g202

[ISO 73:2009] ISO Guide 73:2009: Risk Management – Vocabulary, published by ISO, November 2009; refer to: https://www.iso.org/standard/44651.html

[Kaplan & Norton, 1992] The Balanced – Scorecard Measures that Drive Performance, by Kaplan, S. and Norton, D., published by Harvard Business Review, January-February 1992; refer to: https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2

[NIST, 2011] NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems, published by NIST, August 2011; refer to: https://csrc.nist.gov/publications/detail/sp/800-128/final

[NIST, 2012] NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide, published by NIST, August 2012; refer to: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[OEC] Digital Government in Chile – Digital Identity, published by OEC, October 2019; refer to: https://www.oecd-ilibrary.org/governance/digital-government-in-chile-digital-identity_9ecba35e-en

[S222] The Open Group Portfolio of Digital Open Standards – Glossary and Roles (Snapshot) (S222), published by The Open Group, September 2022; refer to: www.opengroup.org/library/s222

[S230] Zero Trust Commandments (Snapshot) (S230), published by The Open Group, August 2023; refer to: www.opengroup.org/library/s230

[S231] The Open Group Standard: Security Principles for Architecture Snapshot V1.0 (S231), published by The Open Group, October 2023; refer to: www.opengroup.org/library/s231

[W124] Jericho Forum® Commandments (W124), published by The Open Group, May 2007; refer to: www.opengroup.org/library/w124

[W125] Jericho Forum® Identity Commandments (W125), published by The Open Group, May 2011; refer to: www.opengroup.org/library/w125

1 Introduction

1.1 Objective

The objective of this document is to provide a set of models to support the core concepts of Zero Trust. This includes the ability to develop and implement a strategy and the ability to incorporate and define a core security framework (including Risk and Information Security Management). The document also defines a capability-based Technology Reference Model (TRM) to help define and implement Zero Trust Architectures (ZTAs), as well as the supporting philosophy.

The subject of this Snapshot document is the specification of a Zero Trust Reference Model, an aggregate of a set of models associated with ZTA.

This Snapshot document is intended to make public the direction and thinking about the path we are taking in the development of the Zero Trust Reference Model. We invite your feedback and guidance. To provide feedback on this Snapshot document, please send comments by email to ogspecs-snapshot-feedback@opengroup.org no later than April 30, 2024.

1.2 Overview

Zero Trust is a holistic security capability for the information security of a modern Digital Enterprise. It includes a strategy, an approach for how security in the modern world should be done, as well as a framework on how and what to do.

This Snapshot document presents a proposal for a standard that defines and describes all the models required for the development and implementation of a Zero Trust Strategy, including the Zero Trust Implementation Model, the Zero Trust Risk Model, The Zero Trust Information Security Management Model, and the Zero Trust Reference Model, with their underlying architecture philosophy and principles.

The Reference Model (called the “Zero Trust Reference Model”) provides a single point of reference for multiple stakeholders from across the organization to align on what ZTA means, and how it comes together. It supports and implements the core tenets of Zero Trust: data-centricity, asset-centricity, adaptive access control (policy-driven access control), modern identity management across all identities (including digital identity), and security zones. It also enables organizations to execute the strategy, integrate with business processes, and establish a model for the sustained use of the core concepts.

1.3 Conformance

This is a Snapshot document, not an approved standard. Do not specify or claim conformance to it.

1.4 Normative References

The following standards contain provisions which, through references in this standard, constitute provisions of the Zero Trust Reference Model. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

- The Open Group Snapshot: Security Principles for Architecture[1] [S231]

1.5 Terminology

For the purposes of the Zero Trust Reference Model (Snapshot) the following terminology definitions 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.

1.6 Future Directions

The following are candidates or planned for initiatives for future development on Zero Trust:

- Development of a Zero Trust Reference Architecture, which would include reference implementations
- Development of a Zero Trust Practitioners Guide to provide practitioners with a methodology to implement Zero Trust solutions

  This will elaborate on elements of various Implementation Model elements such as a Zero Trust metrics framework and provide practitioners with a guide on implementing Zero Trust.

[1] A formal harmonization initiative within The Open Group Security Forum will clearly define and describe how to use the Security Principles for Architecture, the Security/Risk Reference Architecture, the Zero Trust Reference Model, and the Zero Trust Commandments Snapshots, ensuring consistency and avoiding duplication and contradictions in future iterations of all documents.

- Business patterns for Zero Trust

  — Business Architecture patterns linking the technical, security, and Zero Trust actions with business impact and change in repeatable patterns

    This will provide business, security, and technology leaders with a quick reference on scenarios and business architecture patterns and the Zero Trust and business implications.

  — Use cases for Zero Trust – this will provide scenarios in which different aspects of Zero Trust get called out to address security implications of Zero Trust

  — Developing models in the ArchiMate® Modeling Language

- Technology and implementation patterns for Zero Trust

  For example, patterns for establishing security zones in hybrid cloud environments, data-centric implementation patterns, patterns for asset identity in Operational Technology (OT), Internet of Things (IoT), Artificial Intelligence (AI), and hybrid cloud environments.

- Data management schemes for Zero Trust, engagement with Data Architecture and Governance, and the impact on Information/Data Architecture and Data Governance

- Model mapping to architecture

- Mapping onto technologies

  — Development of (Technical) Patterns for adopting

    These blueprints will provide practitioners with pattern languages for Zero Trust for different scenarios. This will depend on this document being published and address implementations pattern languages for specific scenarios and potentially specific technologies.

- Intersection with other Forums and Work Groups, developing White Papers and mapping artifacts

- Development of Zero Trust in the context of AI and Data Science

  The growth of the use of AI in all walks of life, and the vulnerability of AI to various security threats throughout the whole process, from initial data collection and preparation to training, inference, and final deployment, all create a large threat space, often with relatively loose controls in place, and a large opportunity for attacks. Practitioners (leader, business, technology, and security professionals) are all severely impacted, and often not very educated on this relatively new discipline. The initiative will provide guidance and scenarios on the use and implications of Zero Trust for AI and Data Science.

- Expansion on Zero Trust in IoT and OT

  All the core elements of Zero Trust apply, with nuances to IoT and OT. For example, how is Digital Identity for a $4\mu A$ circuit established? This initiative will provide guidance in this context.

- Establishment of a Threat Model for Zero Trust

  Zero Trust Threat Modeling involves expression of the threat space, and its reduction. Extension of approaches such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege STRIDE,[2] etc., would be in this scope.

- State of the Zero Trust Landscape Survey

  A standing annual survey that provides insight on the state of Zero Trust in the context of the organizations implementing it, those developing products and services for it, and for academia and standards organizations.

[2] Refer to: https://owasp.org/www-community/Threat_Modeling_Process#stride.

2 Definitions

For the purposes of this document, the following terms and definitions apply. The terms in The Open Group Portfolio of Digital Open Standards – Glossary and Roles (Snapshot) [S222] and Merriam-Webster's Collegiate Dictionary should be referenced for terms not defined in this section.

2.1 Zero Trust

(Noun) An asset-centric information security approach that enables organizations to secure and manage data/information, applications, Application Program Interfaces (APIs), and any data integrations on any network, including the cloud, internal networks, and public or untrusted (Zero Trust) networks.

(Adjective) A characteristic of an asset-centric information security approach that enables organizations to secure and manage data/information, applications, APIs, and any data integrations on any network, including the cloud, internal networks, and public or untrusted (Zero Trust) networks.

[Source: S230]

2.2 Zero Trust Architecture

The architectural implementation of a Zero Trust security strategy that follows well-defined and assured standards, technical patterns, and guidance for organizations.

[Source: S230]

3 Foundation for the Zero Trust Reference Model (Informative)

Zero Trust provides a modern approach to Information Technology (IT) security, made necessary by changes in how business is done and ever-changing security risks. With growing international adoption of Zero Trust and the rapid migration of organizations to digitization, enterprises must understand Zero Trust and provide a structure for it.

Zero Trust updates traditional IT security architecture and operations to better support contemporary business models. Traditional IT environments operated primarily inside of a private network and infrastructure boundary. This model assumed that the private network confers trust on assets hosted on it, but this assumption has proven false. Contemporary business environments are composed of an ecosystem of digital products being accessed by many stakeholders across any physical and internet locations. Zero Trust replaces the traditional IT security approach and provides security and risk management without relying on the assumption of a trusted network.

Many aspects of Zero Trust are not new concepts. Concerns with a network perimeter-centric approach can be traced as far back as 1990 (which were famously captured by Bill Cheswick's quote of "…a sort of crunchy shell around a soft, chewy center" [Cheswick, 1990]). The Jericho Forum formalized this shift away from the network perimeter-centric model starting in 2004, which was documented in the Jericho Forum Commandments [W124]. This Forum has since merged into The Open Group, making this work a foundational pillar for Zero Trust.

Today, Zero Trust is recognized as an imperative by many organizations from the US White House[3], NIST®[4], and the US Department of Defense (DoD)[5] to commercial organizations such as Microsoft®, Google®, and countless security companies. This reference model has been informed by this work and is intended as generalized guidance that applies to an organization's entire technical estate across IT, OT, and IoT types of assets.

This model is designed to mitigate both known and emerging security risks.

The definition for Zero Trust from The Open Group Snapshot: Zero Trust Commandments [S230] can be expanded and divided into three perspectives.

Zero Trust:

1. Is an information security approach that focuses on the entire technical estate – including data/information, APIs, and Operational Technology/Industrial Control Systems – throughout their lifecycle and on any platform or network.
2. Provides a security framework to protect assets anywhere based on asset-centric and data-centric security, policy-driven access controls, modern incident detection and response, modern identity management, and security zones/domains.
3. Enables organizational flexibility, agility, and adaptability while continuing to provide the same (and often stronger) security assurances of confidentiality, integrity, and availability for business assets.

[3] Refer to: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
[4] Refer to: https://www.nist.gov/publications/zero-trust-architecture.
[5] Refer to: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

3.1 What is Zero Trust?

As an information security approach, Zero Trust security capabilities enable organizations to secure data/information, applications, APIs, and any data integrations, on any network, including the cloud, internal networks, and public or untrusted (Zero Trust) networks. From a capability-centric, technology-agnostic view, Zero Trust is holistic and not bounded by a specific technology and forms the Information Security Architecture for the digital era.

Zero Trust is implemented through a comprehensive strategy and provides a security framework based on asset or data-centric security, policy-driven controls, modern identity management, and security zones/domains. It also includes the operational aspects that allow organizations to adopt and apply Zero Trust in a holistic manner. This definition, along with the operational aspects form foundational concepts for Zero Trust and should be considered when thinking about Zero Trust.

Zero Trust is the Information Security Architecture of the digital era. Organizations operating in the modern world, especially but not limited to hybrid cloud environments, should consider Zero Trust as the *de facto* approach for their information security. This involves executing a Zero Trust strategy, typically aligned with the business and IT strategy (if they exist) and establishing a runtime capability, leveraging Zero Trust capabilities.

In keeping with modern drivers of agility, flexibility, and velocity, Zero Trust enables modern organizations to operate and execute their business with confidence.

3.2 Purpose of this Document

This document has an explicit goal of providing a normative framework for all stakeholders to align against and have a shared understanding of the models used for Zero Trust. This Snapshot will eventually describe:

An architectural "point of reference" around which organizations can align. This TRM is described in terms of capabilities and Architectural Building Blocks (ABBs) and the standards around them. Where such standards do not already exist, new standards are identified and described at a high level in this document or are defined in detail in ancillary documents. The TRM also provides the baseline around which Zero Trust Architectures (ZTAs) are defined and realized.

Models which help organizations define and execute a pathway to implementing Zero Trust, including:

- Devising and implementing a strategy (strategic implementation models)
- Risk assessments leveraging quantitative risk analysis (e.g., the Open FAIR™ Standards)
- Security Management

3.3 Using This Document

This Zero Trust Reference Model Snapshot provides a set of models addressing the overall capabilities, the associated building blocks for those capabilities, and how to implement them strategically within an organization. This document will provide a normative, but not prescriptive, list of standards.

This document is intended to be a companion to the Zero Trust Commandments Standard, which provides clear definitions for Zero Trust and ZTA, presents a non-negotiable list of criteria for Zero Trust, and reviews different aspects of Zero Trust for executives and senior leaders. In short, the Zero Trust Commandments Standard presents a clear view of what Zero Trust is, and what it is not, allowing this document to focus on describing the core capabilities, ABBs, and Governance, Risk, and Compliance (GRC) considerations for Zero Trust.

The models in this document cover all the major aspects of Zero Trust, helping guide an organization's Zero Trust mission, vision, strategic roadmap, architecture, implementation, operation, and governance of Zero Trust. This is illustrated in Figure 1.

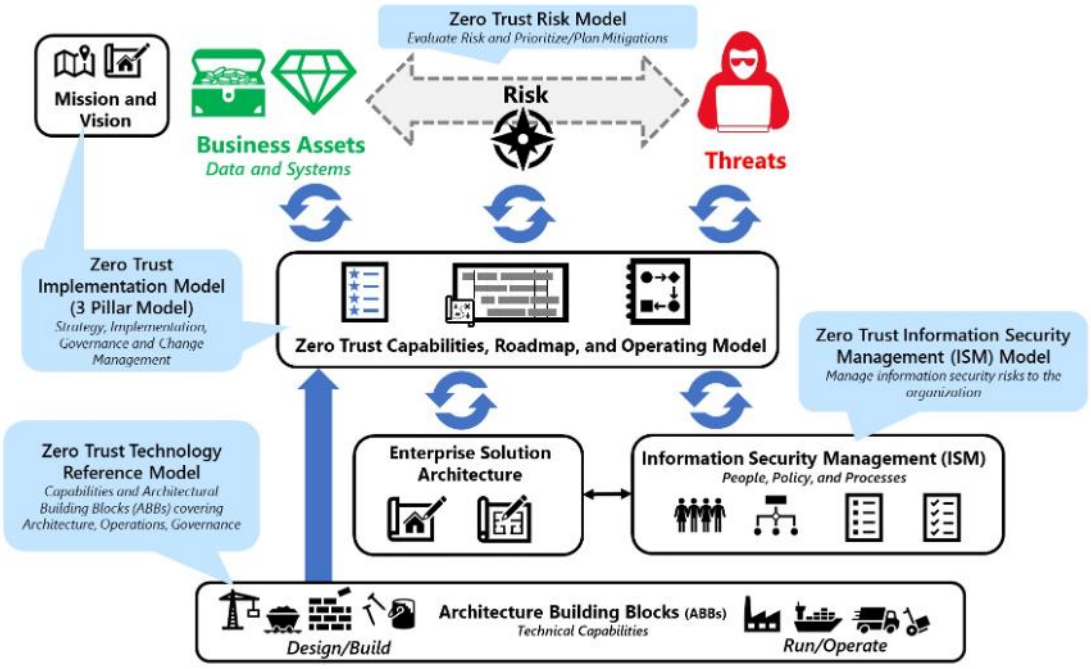

Figure 1: Zero Trust Models and Relationships

This document is composed of four specific models that are described in this document:

- The Zero Trust Implementation Model (Section 5.1) (also referred to as the 3-Pillar Model[6]) lays out the structure around which to develop and implement Zero Trust strategies

  — This defines how to *develop, implement, govern, and run* a Zero Trust Strategy and capability

  Use the Zero Trust Implementation Model to provide a framework around the development of Zero Trust strategies and their implementation. Apply the tailoring as described above to develop governance frameworks.

- The Zero Trust Information Security Management (ISM) Models (Section 5.2) lay the foundation for the operational use of Zero Trust, addressing ISM issues

[6] Note that this model is adapted from the Service Oriented Architecture (SOA) for Business Technology Guide [G202] and adds Zero Trust aspects as relevant. It provides a framework and reuses well understood concepts.

— This defines how to manage information security risks to the organization's operations using Zero Trust. This will also be closely linked to the governance frameworks that come out of the Implementation Model

Use the ISM Models to define structures and security management for operating environments, and use the ISM Model along with the Implementation and Risk Models to form the foundation for the development and implementation of Zero Trust Roadmaps.

- The Zero Trust Risk Management Model (Section 5.3) provides guidance on risk evaluation and management in a Zero Trust context

  — This describes how Zero Trust focuses on assessing and measuring risk as well as addresses both the negative role of risk as a potential business loss and the positive role of using risk management as a competitive differentiator and a necessary component of business growth

  Use the Risk Model to establish an evaluation of risk in a Zero Trust context, accounting for both loss events and opportunities.

- The Zero Trust Technology Reference Model (Chapter 6) provides a holistic capability-centric technical model

  This defines ABBs that represent capabilities which organizations can use to create tailored Solution Reference Models and architectures for Zero Trust.

Use the reference model to create solution architectures by tailoring the Zero Trust Technology Reference Model to your technology estate. Use the detailed description of the capabilities and the ABBs in Chapter 5 to map to specific standards within this document that might apply to your solution architectures. The Zero Trust Implementation Model provides a model to develop and implement a Zero Trust Strategy, leveraging the Zero Trust Reference Model to create Target and Transition State Solution Architectures.

This model should be tailored to the unique requirements of an organization including business drivers, line of business (industry/domain), organizational business and operating models, local regulatory controls, and the organization's existing technical estate and strategy. This tailoring should also consider intangibles, such as organizational maturity level, institutional knowledge, and culture. The organization should then determine capabilities, technologies, and products and their prioritization, to form Solution Reference Models, which can inform architectural decisions resulting in technology, product, and tool selection, and solution implementation. Organizations can also use these models to establish a common taxonomy and terminology across the various entities within the organization. Note that the Zero Trust Reference Models metamodel (Section 5.1.1) defines a metamodel for Architects (both security and technology) to use, including the concepts underlying ABBs, Solution Building Blocks (SBBs), capabilities, etc., and the relations between them.

Other standards bodies can also use this to develop complementary standards, establish interoperability, and support a consistent industry.

Notes:

- A separate Zero Trust Reference Architecture is planned to be developed in the future, providing illustrative best practices and reference implementations of ABBs for particular use cases and standards

  The reference architecture will help supplier organizations validate solutions and provide a usable reference point to develop products, and it will help buyer organizations adopt and implement solutions to accelerate their Zero Trust journeys. Note that the Zero Trust Reference Model is not dependent on the Zero Trust Reference Architecture, which is a reference implementation of the Zero Trust Reference Model.

- Future versions of this document might include threat models for Zero Trust environments
- This document uses "Acme Enterprises" (abbreviated frequently to "Acme") to refer to a fictitious organization in example scenarios
- The details of how the models are applied to form implementation solutions will be covered in the Zero Trust Practitioners Guide, a future publication of The Open Group
- The future reference architecture implementation components should be leveraged to implement or building standards compliant reference implementations

3.3.1 The Audience for This Document

The audience for this document includes the following:

Senior security leaders such as Chief Information Security Officers (CISOs), Chief Information Security Architects (CISAs) and Chief Information Officers (CIOs) can use this document to help set organizational vision, develop, and implement roadmaps, and set up organizational units and governance frameworks.

Security Directors and managers, IT Directors and managers, and other leaders within security and technology teams can use this document to drive direction and implementation of Zero Trust Roadmaps, align teams, and assess the impact of Zero Trust.

Any other leaders that are sponsoring, planning, and supporting security modernization initiatives and other Zero Trust-related activities can use this document to determine impact, establish a common understanding, and work on the development and implementation of a Zero Trust Roadmap.

Security architects operating at the enterprise level can use this document to support the business structure of the organization, including the ability to operate quickly and flexibly, to guide procurement of new tools (largely for security), which ensures that those tools support the organizations Zero Trust intent, and to support that Zero Trust intent in organizational governance and risk management activities.

Security architects can use this document to help develop and implement Zero Trust Roadmaps. Security architects can use this document when working with infrastructure, application, network, and other technical teams, as well as teams which enable security as part of business strategy and operation.

Enterprise Architects and solution architects can use this document to develop a holistic view of an architecture on enterprise, segment, or capability level for alignment across teams and the development and implementation of Zero Trust Roadmaps.

Application Architects and Delivery Teams, including Technology and IT teams involved in supporting activities such as Development, Security, and Operations (DevSecOps) can use this document to help establish a common shared understanding of the details of Zero Trust and the development of cross-cutting and reusable assets.

Information Architecture teams involved in data management, governance, and privacy can use this document along with Security and Enterprise/Solution Architects, Business leaders, and product owners to help identify and define data assets and their lifecycle and business value.

Security and IT engineers/developers can use this document to help establish a common shared understanding of the details of Zero Trust and the development of cross-cutting and reusable assets.

Security and IT analysts can use this document to help establish a common shared understanding of the details of Zero Trust, the development of cross-cutting, reusable assets, oversight, and governance to ensure that security is covered in general and in the context of the various viewpoints.

Audit and compliance teams can use this document to ensure on-demand audit and compliance with different risk and regulatory policies and controls.

Risk teams can use this document to define and ensure compliance with controls, and to define the business value of assets, and the evaluation and assessment of risk and appropriate protection of assets.

Testing teams can use this document to determine testing regimes, tools, and capabilities that need to be supported and provide input into the Zero Trust roadmap and its implementation.

Organizations developing products for the digital enterprise, both for internal use and sales to other organizations can use this document to develop conformant products that support the capabilities and ABBs.

Other standards bodies and institutions can use this document to develop complementary standards and to leverage a shared industry understanding of the terminology and vocabulary of Zero Trust.

Note that the different classes of users of this document may use the document in more ways than described above.

3.4 Core Characteristics of Zero Trust

Adopting a ZTA is meant to enable contemporary business practices, in supporting collaboration between enterprises securely and enabling remote workers, while protecting enterprise data and information assets, including control systems and APIs, by moving access control and monitoring close to the protected assets. To achieve a Zero Trust vision, organizations need to use existing cybersecurity capabilities with new, Zero Trust focused capabilities.

The core characteristics that define Zero Trust implementations, both from a strategic as well as an operational perspective, are:

- Asset and data-centric protection
  - — Zero Trust supports focus on asset and data-centric protection (as opposed to network protection), enabling precision and relevancy of security controls to avoid wasted effort
- Blast radius reduction
  - — Zero Trust assumes compromise of the enterprise's assets and focuses on applying the least privilege principle, containing the damage and cost from any incident
- Reduced threat (attack) surface
  - — Zero Trust applies explicit verification and other core capabilities to reduce overall complexity and the threat surface area of any asset (sometimes called attack surface), reducing the likelihood of a damaging incident

4 Zero Trust Architectural Vision

Zero Trust allows organizations to operate securely on any network at any time in a state of assumed compromise (assumed breach).

A Zero Trust vision centers around core Zero Trust concepts:

- In a Zero Trust environment, assets shall be secure anywhere (wherever they reside or connect)

  Assets should also be accessible anywhere, subject to business requirements and regulatory controls.

- Hence, Zero Trust allows organizations to operate securely on any network at any time in a state of assumed compromise (assumed breach)

  Zero Trust assumes operation in a hostile environment where all trust must be explicitly validated, and all security assurances must be continuously monitored and improved.

- Zero Trust shall reduce the threat (attack) surface area, enabling more of the scarce organizational and information security resources to be focused on the remaining attack surface

- Zero Trust shall help localize and compartmentalize the impact of a breach (reduce the blast radius)

- Zero Trust shall empower greater organizational agility and the adoption of new business opportunities, regulatory controls, and technologies

A Zero Trust capability includes the architecture that provides the foundation for achieving this vision, a strategic implementation approach, an operational capability, and an ability to assess risk and opportunity.

4.1 The Philosophy of a Zero Trust Vision

Zero Trust is a very simple philosophy at its core – the protection of digital business assets wherever they are and wherever they go.

The implementation of security (including the simple and direct approach of Zero Trust) is complicated by the realities that security risks affect the entire organization (they are not contained to any given system or business unit) and that the measures to mitigate security risk must be part of everyone's job.

While Zero Trust is similar in mission to previous approaches to information security, it has a different fundamental assumption of trust. Instead of relying on an invalid assumption that an organization's network is (or could be) safe and trustworthy, Zero Trust assumes that assets are connected to and communicating over open (and potentially hostile) networks, like the Internet, and requires securing them accordingly. This shift is depicted visually in Figure 2.

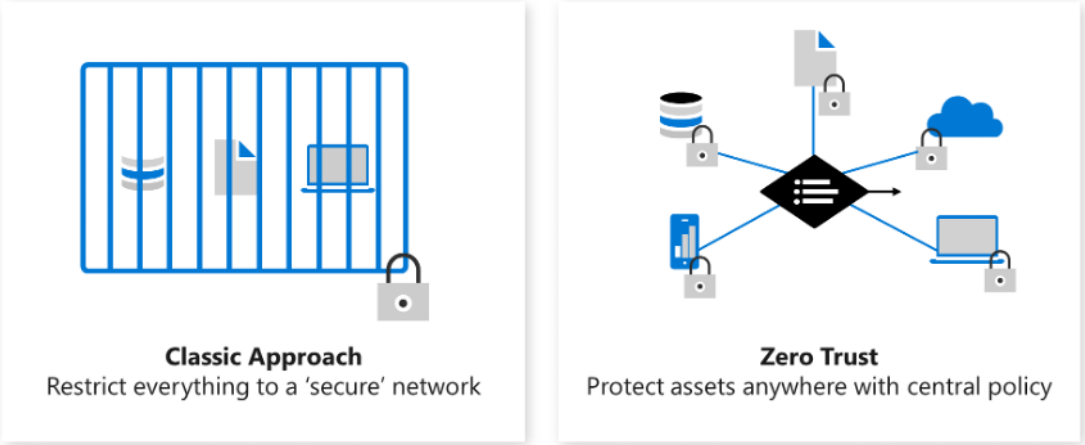

Figure 2: Illustration of how Zero Trust Approach differs from the Classic Approach

This change in assumption leads to asset and data-centric security approaches that protect each asset individually, require explicit validation of all claims of trust (rather than relying on implicit trust of network location), and limit the damage (or blast radius) from any asset that is compromised.

This also shifts security from a technology-centric approach (do you have XYZ technology?) to a capability – and outcome-centric approach (are ABC assets protected against current top threats?).

An enterprise security model based on Zero Trust assumes that an enterprise network has already been penetrated, or could be at any time. This requires security architectures and controls to be designed and prioritized differently. While Zero Trust embraces existing investments into network security, it goes well beyond this single control type.

Zero Trust:

- Moves to a policy-driven model that focuses security controls on individual assets rather than on network egress points

  This tailoring of security to each asset type naturally reduces the threat surface (or attack surface) and the blast radius of damage for those assets if they are compromised

- Prioritizes using the intrinsic business value of assets to ensure the strongest protections are applied to the most valuable assets, ensuring security resources are utilized commensurate to asset value

- Enables continuous monitoring and subsequent improvements to security controls and assurances using all available telemetry, intelligence, and data

These asset-centric Zero Trust capabilities increase the agility of the organization by ensuring the assets themselves are always protected in any situation or configurations. These protections remain even as business processes, use cases, and configurations change to meet the evolving needs of the digital ecosystem. The data-driven approach of Zero Trust also allows rapid audit, compliance, and risk capabilities, further supporting business agility to rapidly enter new markets and reduce organizational risk.

The Digital Enterprise and the environment in which it operates are ever evolving, ever more complex, and constrained by the need to deliver faster and within resource constraints. Thus, Zero

Trust approaches and architectures should look to meet these evolving factors, by reducing the threat surface area. This is also an outcome of the various philosophies discussed earlier – a shift to asset – and data-centricity, blast radius reduction, and agility.

The rate of changes in the threat environment, technical platforms, and market preferences is increasing, driving the need for Digital Business Transformation, cloud technology transformation, and a Zero Trust security transformation to keep up with them.

Figure 3 provides a view of a Zero Trust Architecture that captures the key essence of the Zero Trust Transformation.

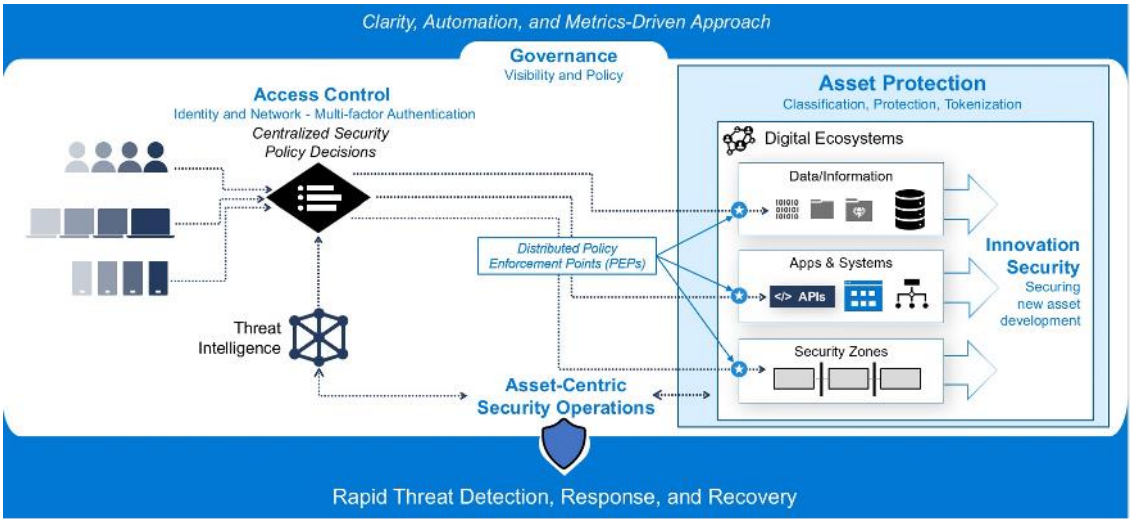

Figure 3: A High-Level Technical View of Zero Trust Architectures

Zero Trust is transformative and requires cultural change, technology change, process changes, technical operating model changes, and skills changes. In its operation, Zero Trust is also more dynamic than previous security models and approaches, requiring the adoption of Agile roadmaps that can adapt to the rapid technology, business, and cloud changes. Zero Trust is not executed as a single big overnight change, but as incremental changes that steadily realign many aspects of the strategy and organization to the new direction.

Zero Trust breaks down silos separating security and technology teams and activities. Zero Trust drives alignment across different disciplines and organizational units such as business, security, technology, risk, and compliance. The Open Group Snapshot: Zero Trust Commandments [S230] provides a foundation for guiding that change. Organizations shall use the Zero Trust Commandments to define their Zero Trust journey and provide a shared vision of Zero Trust to all stakeholders in the organization, including business leaders.

4.1.1 Governance and Zero Trust Security

Zero Trust Governance provides the ability to establish decision rights, audit and compliance, and guardrails in implementation. It also includes the goals, principles, policies that constitute these guardrails and the education and training required to make this actionable.

Zero Trust Governance introduces security architecture and threat intelligence as governance functions to drive informed decisions across systems.

To summarize, Zero Trust Governance is distinguished by the following (Zero Trust Governance is covered in Section 6.2.7 and Section 6.4.7):

- From a strategy and design perspective by:
  - — Governance decisions based on multiple factors including data classification to support data protection (including data tokenization)
  - — The protection of assets (both data and system), the criteria and oversight of the implementation of Security Zones, asset classification, and identity management controls
- From an operational perspective by:
  - — Operational security governance and guardrails for Security Operations Capability (SOC) and Security Orchestration, Automation, and Response (SOAR) capabilities
- From an audit and compliance perspective by:
  - — Continuous monitoring
  - — Audit on demand
  - — Privacy by design
- From a people and process perspective by:
  - — The establishment of a Zero Trust Organizational structure that supports Agile delivery and oversight
  - — The establishment of Zero Trust Organizational processes that support Agile and auditable oversight of the technical estate across the entire DevSecOps space – including infrastructure, operations, and other capabilities

    These processes cover strategy, establishment of goals, principles, risk management, policies, standards, oversight of implementation and updates across the technical estate, including architecture, development, and operations.

    This includes support for both professional and citizen developers.
  - — The establishment of a continuous learning environment and the supporting capabilities

4.1.2 Posture Management

Posture management is an operational function that focuses on continual improvement of coverage and effectiveness of protective and detective security controls across the technical estate.

Posture management mitigates potential security vulnerabilities in partnership with operations teams in IT, OT, IoT, and Product/Application Teams (including Development/Development Operations (DevOps) teams). Posture management is a hallmark of ZTAs, enabling Digital Enterprises to operate proactively and to establish preventive controls that block future attacks from happening.

This Zero Trust function is a greatly expanded and integrated version of vulnerability scanning. Posture management enables a proactive holistic security approach that allows the organization to burn down the ‘technical debt’ of weak security practices that have accumulated over 30+ years

of adopting computer technology. For example, with application security mapping to DevSecOps and obtaining telemetry, to transform a limited reactive function into a proactive function focused on integrating with and enabling existing teams/processes.

Posture management includes both an inside-out and outside-in view covering internal scanning and external attack surface management. Internal scanning supports an inside-out approach uses management tools to monitor the security status of the organizations posture such as a Cloud Security Posture Management (CSPM) tool that continuously reports on and makes recommendations to improve security posture. External Attack Surface Management (Outside-in scanning) – used tools that monitor the security posture and attack surface of the organization from the internet (mimicking an attacker's view of the organization). Tools like External Attack Surface Management (EASM) products monitor what the digital footprint of the organization looks like across their platforms, websites, brands, multiple cloud types and providers, on-premises datacentres, mobile, social, third parties, and more.

4.1.3 Security Operations (SecOps) [Center] or SOC

SecOps is an operational function that focuses on mitigating realized risk (in the form of active attacks). Zero Trust broadens the role of SecOps to the full technical estate beyond the firewall and focuses on partnership and integration with IT Operations and DevOps teams. Zero Trust also highlights the value of proactive security operations functions (threat hunting, continuous improvement and automation, and red and purple team operations) and integrates them with the overall security model.

4.1.4 IT Operations

IT operations are responsible for managing enterprise-wide technical resources in the technical estate. Any changes to the production environment from posture management or security operations are done in partnership with IT Operations. Zero Trust introduces a close integration with Security Operations for rapid incident response and recovery (mitigating realized risk) and with posture management for prevention (mitigating potential risk).

4.1.5 Data Governance

Data governance is responsible for data lifecycle governance of data assets, ensuring that data-centric incorporates all stages in an asset's lifecycle including retention, provisioning, deprovisioning, compliance and legal requirements, classification, and other concerns. This function also addresses any data access concerns, and integration into the business use of the data, and the implications of any Zero Trust approaches on the business and the data.

Zero Trust Data Governance requires clear data ownership, stewardship, and accountability.

4.1.6 Asset Protection

Asset protection is responsible for applying security policy to assets throughout the technical estate. This includes protection of both systems and data.

4.1.7 Access Control

Access control manages access to business assets in the technical estate. Zero Trust updates static perimeter-based controls to an "adaptive access control" approach.

4.1.7.1 Adaptive Access Control

Adaptive access control is an updated approach to enable and secure access to any type of asset (resource) regardless of geographic or network location. Adaptive access control provides consistent access policy enforcement across assets and locations that adapts to dynamically changing factors such as threat intelligence, user behavior patterns, and more. This approach also enables rapid Agile updates to access control policies based on changes to business requirements, the technical estate, and the threat environment.

This enables building and enforcing access policy that is informed by the organization's risk appetite and continuously changing threats in real-time.

4.1.8 Innovation Security

Innovation security integrates security into development of new capabilities by professional developers (DevOps/DevSecOps teams) and Citizen Developers (low-code and no-code applications). Zero Trust shifts from a quality approval gate process that disrupts productivity and agility to an integrated approach where security elements fit smoothly into the Agile development process.

4.1.9 People Security

People security manages risk from human actions including inadvertent errors (*via* user education and enablement) and malicious insiders. Zero Trust introduces this element to combat insider threats. Zero Trust also focuses on user engagement and enablement (often with gamification) to teach security knowledge, rather than a classic "phish and punish" type of punitive education.

4.1.10 Controls Management

The "Identify, Protect, Detect, Respond, and Recover" functions support the capture, management, and definition of controls and the associated policies, and the compliance with them. Note that a Zero Trust approach includes protecting using controls, as well as dynamic, active risk-based approaches.

5 An Overview of the Models

Zero Trust transforms multiple aspects of the complex function of security, so this section introduces the models that give an overview of the Zero Trust capabilities and components, the recommended strategic implementation approach, how to integrate it into other organizational functions and capabilities, and then the operational aspects of Zero Trust.

The Zero Trust Reference Models include:

- The Zero Trust Implementation Model (also referred to as the 3-Pillar Model) which lays out the structure around which to develop Zero Trust strategies and implement them

  — This is composed of capabilities and capability categories, ABBs, and dependencies between them

  — It provides a framework to:

    - Develop Zero Trust roadmaps, governance frameworks, and strategies as organizations plan and execute strategic Zero Trust implementations
    - Integrate Zero Trust with business strategies and Digital Transformation

- The Zero Trust Information Security Management Model, which lays the foundation for the operational use of Zero Trust, addressing information security management issues

  This will be closely linked to the governance frameworks that come out of the Implementation Model.

  — This is composed of the set of controls, policies, and structures required to support the information security management function, including the organizational structure and relationship between IT and security functions

  — It provides the foundation for managing the security function in terms of ISM controls and policies, and the structural and process support (linking to the governance functions supported by the Operating Model Pillar)

- The Zero Trust Technology Reference Model which provides a holistic, capability-centric model defining capabilities and ABBs which organizations can tailor to create Solution Reference Models and architectures

  This is covered by Chapter 5. It provides:

  — A shared taxonomy that buyers and suppliers, along with other standards bodies can use

  — A starting set of capabilities, architectural building blocks, and associated standards that:

    - Organizations can use to develop their enterprise Zero Trust Solution Architectures
    - Vendors can use to develop Zero Trust products
    - Supports interoperability and standards compliance to enable buyers and sellers to move rapidly to an open, Agile capability

— This is composed of capabilities and capability categories, ABBs, and the dependencies between them

- The Zero Trust Risk Model which provides guidance on risk evaluation and management in a Zero Trust context

  — This uses the Open FAIR Body of Knowledge and Open FAIR models and approaches to represent the loss aspects of risk[7]

  This also represents the business necessity of carrying some risk in order to operate and grow a business, as well as the positive value of risk mitigation as a business differentiator and source of competitive advantage.

  — It provides the foundation for evaluating risk and opportunity, while remaining bound to the well understood and established Open FAIR structure and standards

The relationship of these models is depicted in Figure 4.

Figure 4: Zero Trust Models in the Zero Trust Reference Model Standard

5.1 The Zero Trust Implementation Model

The 3-Pillar Model provides a framework for developing, implementing, governing, and running a Zero Trust Strategy and capability. It describes "how" a Zero Trust Strategy and its associated Roadmap is developed and implemented. This model also helps integrate Zero Trust into the overall organization business model, process model, and governance framework to ensure that security is not operating outside of normal organizational functions.

This section presents the 3-Pillar Model and its key components. Details about how to apply it will be covered in the eventual Zero Trust Practitioners Guide. Practitioners can use this Zero Trust Implementation Model to establish and execute a Zero Trust Roadmap even in the absence of the Zero Trust Practitioners Guide.

Figure 5 shows the three pillars of the model: Strategy, Operational, and Operating Model.

[7] The term "risk" in this document utilizes the definition from the Open FAIR Body of Knowledge: "Risk is the probable frequency and probable magnitude of future loss." Where discussion of potential gain occurs, the term "opportunity" is instead used for consistency and to delineate the concepts.

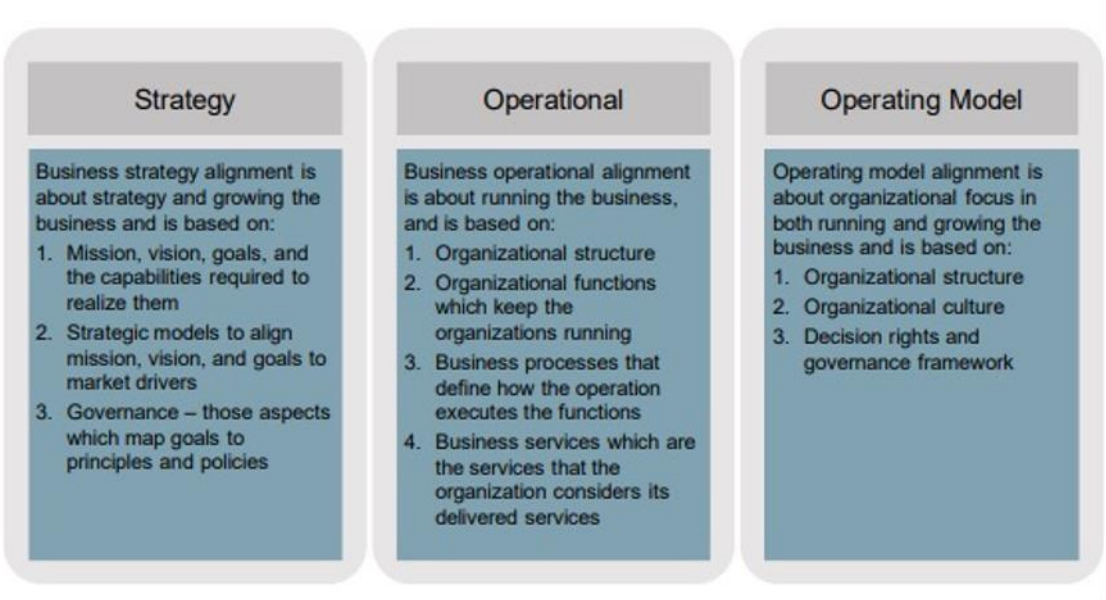

Figure 5: Pillars of Business/Technology Alignment and Organizational Business Service Enablement

The Strategy Pillar defines the development of the roadmap by identifying the mission, vision, and goals and mapping them into Business Capabilities. Capabilities in the context of this model can be divided into business, technical, security, and Zero Trust capabilities. Capabilities may be supported by people (organization), processes, and technology.

The primary outcome of the Strategy Pillar is a tailored, capability-centric roadmap. Roadmaps are typically broken down into phases, with metrics and maturity levels helping tailor and tune the roadmap over time. They are usually highly accurate in the short-term, have medium level of fidelity and confidence in the mid-term, and represent high level directional guidance for the long-term. Roadmaps link the delivery of these capabilities together and are updated regularly, providing alignment with an evolving business, technical, regulatory, and security landscapes. Note that as the organization develops its roadmap, legacy applications will typically use compensating controls while they migrate to a Zero Trust Architecture (ZTA).

The Operational Pillar defines the execution of the roadmap and the tailoring of it to organizational or departmental constraints, helping create solution architectures, map the people and organizational units, the business processes, and build out the roadmap while the organization is running the business.

The Operating Model Pillar provides governance and change management, helping establish key elements of a digital culture – a culture of continuous learning, change, and improvement. It runs simultaneously with the other two pillars, forming communications, decision rights, guardrails, continuous learning, and other elements of a Zero Trust enterprise. The organizational operating model forms a filter to assess the organization from a culture and business operating model perspective and determine spending, business model, and cultural drivers. This in turn determines the approach to take in the implementation of the roadmap.

Note: People-centricity is an important element of Zero Trust. Because mitigating security risk is part of everyone's job and security risks affect the entire organizations, Zero Trust requires that organizations adopt organization-wide cultural elements and processes to

educate people on their role in security (why, what, and how to help). This requires having a governance framework, a cultural change plan, and a skills management plan, that are all part of the roadmap (many of which are covered in the Operating Model Pillar). When developing employee engagement and skills plans, think about gamification, certifications, and a culture of continuous learning.

5.1.1 The Strategy Pillar

The Strategy Pillar is used to help create and implement a capability and metrics-based Zero Trust roadmap. This provides organizational alignment, focused initiatives, quantifiable metrics, governance, and cultural change management frameworks.

The Strategy Pillar is usually composed of:

- A clear definition of the Mission, Vision, and Goals accompanied with both aspirational and quantifiable metrics
- A capabilities definition that includes the business, technical, security, regulatory, and Zero Trust capabilities involved from different perspectives

  This can leverage any existing repositories (e.g., Business Architecture repository). It also uses standards driven capabilities, such as those provided in this document, to determine Zero Trust capabilities. These are tailored to the specific needs of the organization to help determine specific capabilities.
- A framework of metrics[8] that measures the current state at different levels and progress against strategic initiatives, typically composed of scorecard level metrics, Key Performance Indicators (KPIs), and Objectives and Key Results (OKR)
- A definition of strategic initiatives that defines the strategic initiatives to build and mature the capabilities, using metrics, to curate and guide the development of the initiatives

  This allows the organization to rebalance, realign, and execute on the implementation of the initiatives in an Agile manner, keeping the initiatives aligned to business, security, regulatory, and technology drivers and strategies. These strategic initiatives establish new capabilities or increase the maturity level for existing capabilities as depicted in Figure 6.

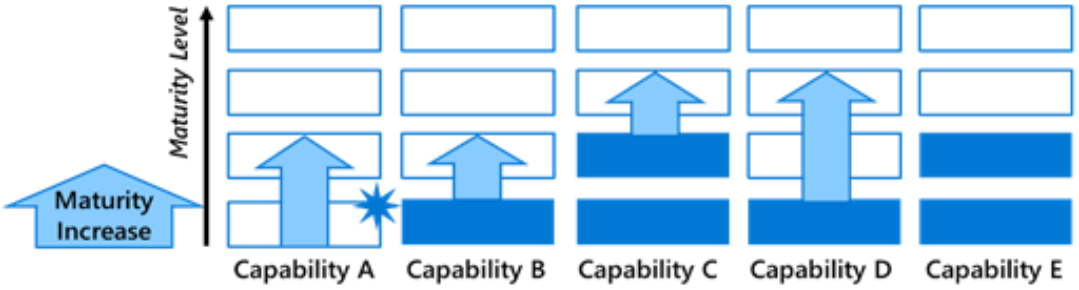

Figure 6: Illustration of How Strategic Initiatives Mature Capabilities

[8] The next version of this document will provide more details on this content.

OKRs are typically the best metrics to use to measure success and evolution of security initiatives as they will allow strategic initiatives to adapt based on changing roadmap priorities (which are driven by changes in the environment, continuous learning, and continuous improvement). These metrics can be used to provide continuous improvement and guidance for the teams executing the initiatives.

- A governance, culture, and operating model that defines the governance framework, tailored business operating model, and cultural change management process to support and guide the strategic initiatives that deliver on the capabilities
- A tailored roadmap that links the capabilities and dividing them up into phases that can be monitored for success in the initiatives

  The roadmap can (and should) be viewed with a relatively high level of confidence in the short term, medium level of confidence in the mid-term and low level of confidence in the long term.

5.1.1.1 A Framework of Metrics for Zero Trust

5.1.1.1.1 Overview

As Figure 7 shows, metrics must be considered in the context of:

- Scorecards which are typically used to communicate enterprise or departmental direction
- KPIs used to evaluate relatively durable and stable criteria for unit or organization level performance over time
- OKRs which are used to evaluate and train organizational performance at a unit or enterprise level

5.1.1.1.2 A More Detailed View

Scorecard level metrics are KPIs intended for senior leaders and boards, represented as a scorecard, typically framed as a variant of a Kaplan Scorecard Model [Kaplan & Norton]. Scorecard changes related to Zero Trust must align to both the Zero Trust strategy and the enterprise business strategy.

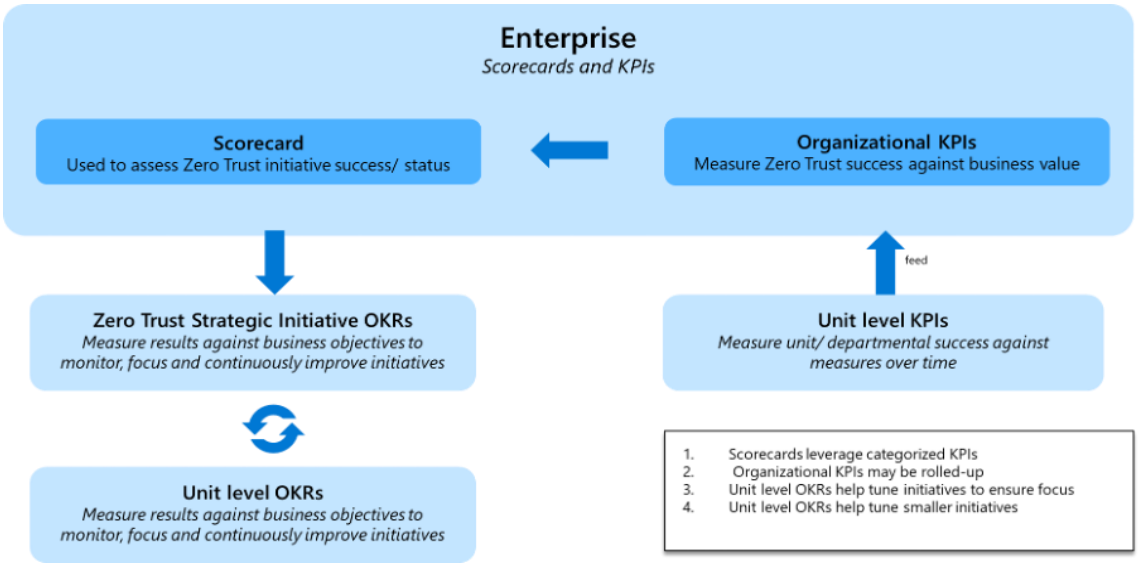

Figure 7: Illustration of Metric Relationships

They typically measure:

- Zero Trust Impact on Existing Scorecard Metrics[9] – measure how existing scorecard metrics will be impacted by Zero Trust metrics

  Illustratively, this might include measuring improvements to the revenue, new channels, compliance, and time-to-market axes from the enablement of Zero Trust adaptive access control capabilities for all users and tokenization of all Personal Identifiable Information (PII) and high-value data. Another example could be improvements to the learning and growth axis (reflected in the annual employee survey and retention statistics) because Zero Trust enabled secure remote work, increasing employee flexibility and satisfaction.

[9] The next version of this Snapshot will provide more details on this content.

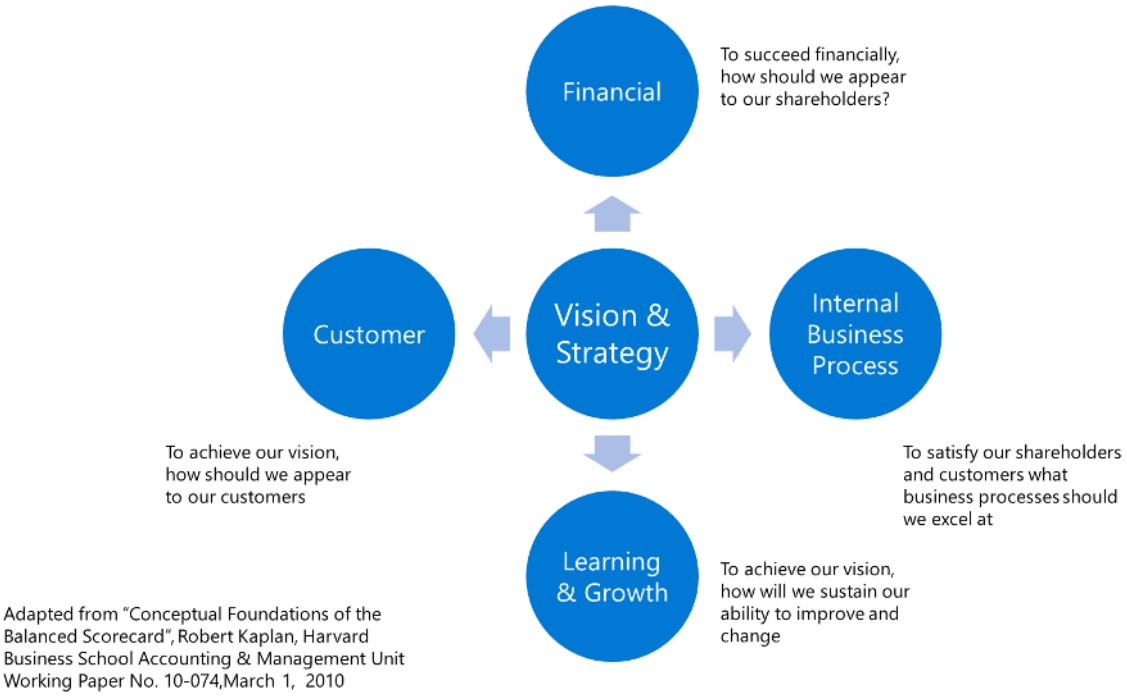

Figure 8: Kaplan Balanced Scorecard

- Zero Trust Program Status and Progress – creation of new Zero Trust metrics aligned to the Zero Trust mission, vision, and goals (described below)

  Illustratively, these could provide measurements of how well the organization is able to prevent risk or to respond to and remediate risk, and how well security enables business processes and productivity goals.

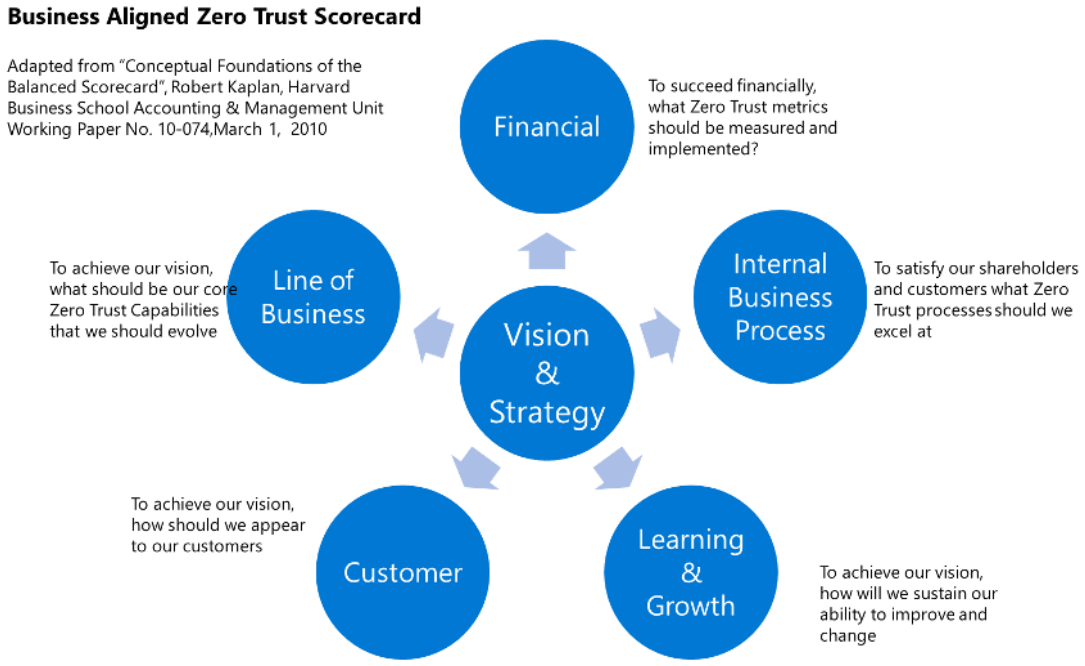

Figure 9: Zero Trust Scorecard

Illustratively, for the Financial Axis, consider risk (both loss prevention and business opportunity creation metrics). For the Learning and Growth Axis, consider Continuous Learning (e.g., enterprise-wide training on the Zero Trust Core Principles and Commandments training, learning on Data Tokenization related processes for business personnel, and learning objectives for practitioners (architects and engineers)). For the Customer axis, consider establishing reputational metrics, ease of doing business metrics (due to Adaptive Access Control), etc.

- Organizational-Level KPIs – these business unit success measures need to be modeled around the Zero Trust strategy and the business unit goals and metrics

  Illustratively, a business unit might have a 50% transition of sales to sales using AI and predictive analytics, 80% increase in sales on mobile channels. The corresponding Zero Trust metrics, in alignment with Acme's Zero Trust strategy might be to provide an adaptive access control incorporating mobile channels, and the use of tokens for user account IDs to reduce the risk and threat of breach, with a 100% conversion of user account IDs.

- Unit level OKRs – these goals for specific units and teams set clear direction based on the local mission and function

  Illustratively, the sales organization would have an objective of expanding sales to new, different channels, and the use of Zero Trust will reduce time to market by 50% by allowing them to rapidly add new vendor partners and client channels, while meeting compliance requirements.

- Zero Trust Strategic Initiative Progress – these OKRs measure the progress of the strategic initiatives, both the completion of tasks as well as the increase in maturity level of Zero Trust capabilities

  This framework of measurable outcomes and specific quantifiable goals make the shared vision and mission clear at all levels in the organization. They also ensure that progress and priority evolution can be tracked at different levels, and that delivery on goals are appropriately tailored and adjusted as needed.

5.1.1.2 A Quick Note on the How

While the details of the "how" will be covered in the eventual Zero Trust Practitioners Guide, a short summary is:

The mission, vision, and goals are established early to ensure the organization aligns around an aspirational mission and a vision to get there.

Regarding alignment, organizations exist in a context which incorporates business, technology, regulatory, and security environments and drivers. Regardless of the industry or type of organization, organizations exist to meet some "business" mission – whether a government agency, commercial organization, Non-Governmental Organization (NGO), or any other entity. Technology and security exist to support this mission and must adapt to evolving trends in order to keep the organization both Agile and secure to deliver on this mission.

Developing a Zero Trust Mission, Vision, and Goals aligned to the organization's mission helps ensure that Zero Trust and Security teams are aligned to the context of the organization and its business drivers. These guide the Zero Trust journey while incorporating Zero Trust standards and capabilities and must be kept in mind when launching a Zero Trust.

The Zero Trust mission is aspirational and focused for the organization, developed with the overall background in mind. Illustratively, for a fictitious Acme Healthcare, the business vision might be "Acme exists to provide high-quality, affordable health care and improve the health of our members and their communities". The associated Zero Trust vision might be "providing secure delivery of our services in an affordable, timely manner at any time and any place".

The Zero Trust vision is usually time-limited and has specific constraints. In the case of Acme Healthcare, it could be: "Our vision at Acme is to be a leader in total perfect health by improving the lives of our members and the quality of health of their communities". The associated Zero Trust vision might be "being a leader in delivering the services in a secure manner in any environment, with the highest level of availability, on any channel, with the ability to support the Agile addition of deletion of partners and capabilities into the organizational ecosystem, and in an environment of assumed breach, in alignment with Acme Healthcare's Digital Transformation and Cloud Migration initiatives". Enabling the business vision but focused on Zero Trust. Ensuring alignment with both the organizational and technology strategies.

The vision is then decomposed into more specific Zero Trust goals associated with specific metrics (usually KPIs). The associated goals could then be "the ability to support Health Insurance Portability and Accountability Act (HIPAA) compliance for the delivery of data on any channel, and on any platform, in an environment of assumed breach", "the ability to localize and limit the impact of a breach to 99% of Acme's component systems, with complete isolation of the rest", "the ability to recover from a disaster or breach in xxx time", "the ability to securely share data with our partners in an Agile manner in 2 years", and "the ability to support the addition or removal of 90% of Acme's partners in a secure manner with full verifiability in a hybrid cloud environment in 3 years".

These illustrative mission, vision, and goals must be adapted and tailored to the individual organization's business and technology strategies. Use the Operating Model's "business operating models" to help focus on prioritization and approach keeping how an organization focuses business structure and philosophy. This is critical for success as it focuses on both the spend, organizational structure, and leadership support.

The capabilities enable achieving the defined goals. There may be different ways to achieve these goals, and these will usually be curated by the organization's business and technical environment, its operating model, ongoing strategies, etc. Roadmaps will achieve goals using these capabilities, typically in the form of multiple strategic initiatives. The term used to describe these initiatives may vary based on the organizational process model (e.g., in an Agile organization, they may be called programs or epics). These initiatives may then be associated with both metrics and maturity levels to ensure they are able to track performance improvements.[10] They will develop metrics such as KPIs or OKRs to assist with this. Typically, OKRs provide a clear actionable model, while KPIs are used to assess high-level organizational goals.

Illustratively, a Zero Trust capability may be data-centricity and data protection. In the Acme context, in order to meet the goals of "the ability to securely share data with our partners in an Agile fashion in 2 years" and "the ability to support the addition or removal of 90% of Acme's partners in a secure manner with full verifiability in a hybrid cloud environment in three years", the Zero Trust approaches of data-centricity, asset-centricity, security zones, and blast radius reduction might be followed. Usually, a combination of these is used. For example, a roadmap might have initiatives such as: "establish policy based adaptive access control and identity for 90% of participants in the technical estate (ecosystem) in the Acme enterprise in one year" and

[10] This Snapshot does not address a maturity model or assurance framework for Zero Trust.

"establish data-tokenization for or eliminate all sensitive data, supporting different tokens for data not eliminated by entity in two years". Another might be to: "define the segmentation of zones in the hybrid cloud environment".

The maturity measure may be the "adoption of one or more data-centric protection mechanisms by the organization", while metrics may be that 80% of the organization has either eliminated, obfuscated, or established format preserving encryption of its data, and the rest is encrypted at rest. For an illustrative OKR in this context, the objective would be obfuscation or format-preserving encryption across the enterprise, and a key result would be 80% obfuscation or format-preserving encryption. For a Zero Trust SOC, the organizational objective might achieving the lowest Mean Time To Acknowledge (MTTA) (how long it takes to start work) and Mean Time To Remediate (MTTR) (how long it takes to remove attacker access) in a particular geography or industry, and the key result would be that the MTTA incidents should be less than "X" number of minutes (say 10 minutes) and the MTTR incidents should be within "X" hours (say 12 hours).

5.1.1.3 Key Strategy Pillar Considerations

Never use security operations measurements punitively. Security operations metrics shall never be punitive, or they are likely to backfire (or never make their way into the roadmap). All security operations metrics can be impacted by external factors not under control of the organization such as recent vulnerabilities, attacker competency and skill, and what attack tools and automation are available to the attacker. If people are held accountable for forces they cannot control, they have gained an incentive to skip the work and lie to their leadership. Metrics shall be used to provide feedback and be aspirational as OKRs are. They shall be used to train and educate people to improve operational performance.

Zero Trust initiatives involve both significant investment and have a broad, usually enterprise-level impact on an organization. It is important to be able to incorporate the organization's business Zero Trust operating model into determining what to focus on when developing the roadmap. The operating model is covered in more detail in the review of the operating model pillar.

A metrics framework and maturity measures are used to determine the extent of success and fine-tune requirements towards evolving organizational needs. Metrics frameworks for Zero Trust will be elaborated on in the Zero Trust Practitioners Guide and are out of scope for this document. Maturity models may separately be used to help define high level measures of success. OKRs are used in Agile delivery organizations to tune organizational delivery at the unit level.

The roadmap is based on business, technical, security, regulatory, and Zero Trust capabilities. It provides quantified targets, initiatives with the assignment of resources, and alignment with business, technical, security, and regulatory disciplines, establishing the people skills (through developing a culture of continuous learning) and governance framework. It leverages these elements from the operating model pillar, using the operating model viewpoint to focus the roadmap. The operating model helps determine what leadership focuses on and considers to be important. This helps identify priorities, culture, and implications.

The roadmap can (and should) be viewed with a relatively high level of confidence in the short-term, medium level of confidence in the mid-term, and directional guidance (low level of confidence in specific details) for the long-term.

5.1.2 The Operational Pillar

The Operational Pillar is the execution of the strategy and roadmap. This pillar makes the strategy real by integrating capabilities and processes into business, technical, and security operations. This weaves together Zero Trust with the existing organizational and business context, binding it into concrete capabilities and components that can be built and operated.

Because Zero Trust introduces changes to existing operations, think about it like changing the engine or seats while flying the plane. Organizations have to run and grow the business while executing the Zero Trust Roadmap, typically while simultaneously integrating (and harmonizing) with and executing a digital business transformation and a cloud technology transformation.

The Operational Pillar takes the Zero Trust Reference Model and applies organizational, business, regulatory, and security environments, constraints, and limitations to translate them into an operational Zero Trust solution architecture. It applies the Zero Trust Roadmap to the organization's technical estate, culture, regulatory and risk context, and Process and Governance Framework, and translates those initiatives and other elements into actionable updates to security components that are applied to the various business and technical elements in the organization.

This allows the organization to execute the roadmap while establishing the governance framework and solution architecture, to create an organizational evolution towards Zero Trust maturity.

The Zero Trust Operational Pillar is composed of business capabilities, processes, and functions, as well as the technical estate that implements it. Business functions can be a combination of the people, organizational structures, business capabilities, business processes, and the business services provided.

Illustratively, in an insurance company, there exists a "Provider Network Management" composed of an organizational unit, supporting institutional processes and staff, business processes, underlying technical components, and security and regulatory controls. It will likely involve a mix of legacy (e.g., Java n-tier and mainframe) and newer cloud platforms with microservices forming its technical estate. The Zero Trust implications for this may include creating Zero Trust security zones, a data-centric framework for key data elements – provider ID, patient personally identifiable information, etc. A Zero Trust centric adaptive access control framework allows supporting the ecosystem in which the Provider Network Management function belongs with numerous channels and components. The SOC supports this by prioritizing monitoring and response resources for business-critical assets identified by business leaders.

What makes the Operational Pillar for Zero Trust different is that attributes that drive the implementation of a Zero Trust Roadmap conform with the Zero Trust Commandments and Reference Model. This creates consistency with both security and risk imperatives as well as the impacted business elements – processes, functions, regulatory environment, business ecosystem, business environment, and the existing technical estate. Zero Trust initiatives also tend to influence how business is done, particularly the technology, risk, and security domains.

The resulting Zero Trust Solution Architecture and the updates to business capabilities, functions and processes, and the technical estate are typically cross-cutting and not bound to individual components or functions.

Additional details on executing the Operational Pillar will be covered in the eventual Zero Trust Practitioners Guide.

5.1.3 The Operating Model Pillar

Zero Trust initiatives are enterprise-wide in nature so they must be aligned to the operating model and processes of the organization. The Zero Trust Operating Model Pillar involves establishing organizational guardrails and governance, communicating, and landing a shared enterprise vision, setting up skills enhancement processes, integrating continuous learning into the organization's culture, and establishing clear roles, decision rights, portfolio governance, and fiscal governance.

For it to succeed, the Zero Trust Operating Model must be adapted to the organizational style of the organization – a governance model designed for a unified organization with a single Chief Executive Officer (CEO) and centralized IT processes will not work for a diversified organization with multiple independent business units with their own CEOs and local technical and security functions.

Trying to implement or develop a roadmap that does not take these factors into consideration usually leads to failure. The Zero Trust Operating model uses the 4-Quadrant Model depicted in to focus and tailor all the other components of the pillar – the governance framework, the guiding principles, commandments, etc.

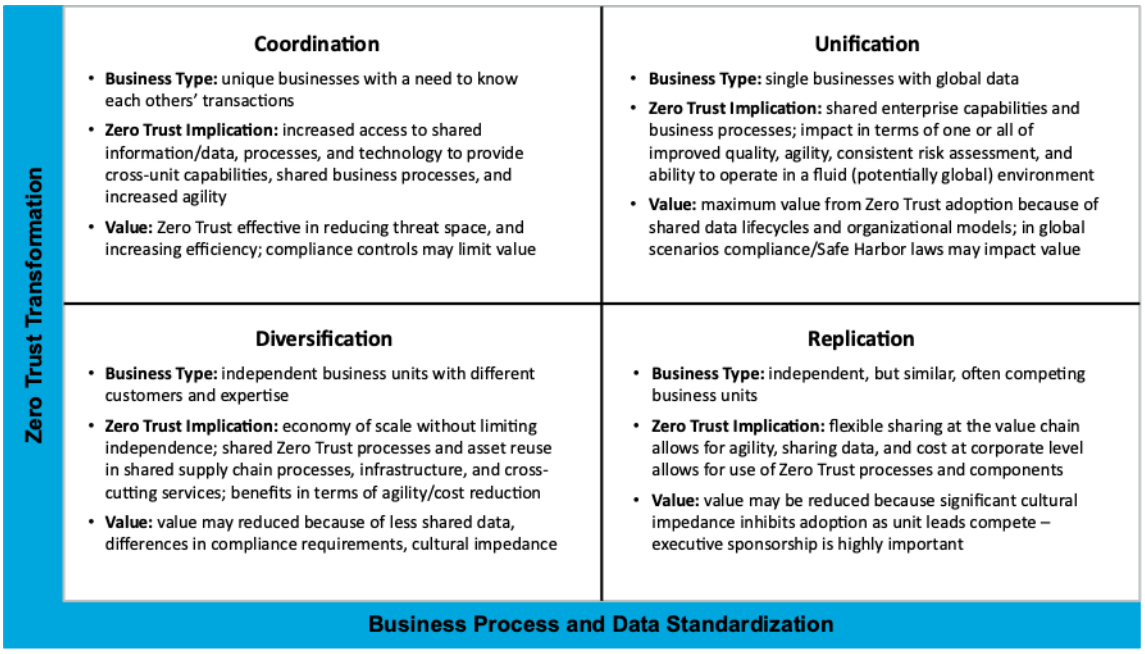

Figure 10: The Zero Trust Operating Model Pillar Quadrants

The Operating Model is based on the structure of the business and how it is organized and prioritized. The four quadrants are:

1. Coordination: unique businesses with a need to know each other's transactions.
2. Diversification: independent business units with different customers and expertise.
3. Unification: single businesses with global data.
4. Replication: independent, but similar, often competing business units.

The Zero Trust Practitioners Guide will tie together the various models to help organizations develop and implement their Zero Trust journey.

5.2 Zero Trust Information Security Management Models

The objective of an organization's Information Security Management System (ISMS) is to manage the information security risks to the organization's operations. There is typically a large gap between how Zero Trust is done and the realization of the functions (a combination of realized capabilities, people, process, and business process).

Zero Trust does not require or define a specific information security management approach and is compatible with standard definitions, including Open Information Security Management Maturity Model (O-ISM3) [C17B].

The characteristics of a Zero Trust ISMS are:

- Focuses on capabilities

  Zero Trust ISMS focuses on managing capabilities and outcomes composed of people, process, and technologies, rather than on the classic approach of managing technical components.

- Enables collaboration

  Zero Trust ISMS is structured to encourage collaboration and process integration across security teams, IT teams, and business teams.

- Integrates with organizational risk management

  Zero Trust ISMS risk functions should be integrated with the organization's risk management framework, risk register, and supporting processes to ensure seamless management of security risk. Illustratively, the ISMS should facilitate the creation and maintenance of an organization-wide Zero Trust security risk governance council and align security risk prioritization to the output of this council.

- Includes posture management

  Zero Trust includes a dedicated operational function for posture management focused on identify/protect to complement the detect/respond/recovery focus of the incident response and security operations. Zero Trust ISMS must support the human and governance (people, process, decision rights) aspects of Zero Trust ISMS.

- Focuses on agility across all functions

  Zero Trust supports the rapid changes in the business, technology, and security environments. Illustratively, policy updates frequency can be as short as two-week sprints in larger organizations at the leading edge of cloud adoption.

- Adopts risk-based internal standards

  Internal standards focus on mitigation of the risks faced by the organization, which is an extension of the traditional role that is focused on managing multiple regulatory compliance standards.

Key Zero Trust functions for ISMS functions are:

- Manage risk

  Focused on integrating with organizational risk management functions, considering both negative and positive implications of risk, striving to quantify risk, and using risk and intelligence to improve internal security standards (beyond just meeting compliance); see Section 5.3 for more detail.

- Manage compliance

  Focused on increasing speed and agility of reporting compliance to get to an "audit on demand state" that increases business agility to enter new markets and address new regulatory standards in existing markets.

- Manage policy

  Focused on increasing speed and agility of policy updates (particularly around control procedures) to keep up with changes to security risk and technical environments.

- Manage access

  Focused on shifting to managing an adaptive access approach that blends together identity and network access technology into a risk based model that applies across internal employees, partners, customers, and other account types.

- Manage operations – focused on two complementary functions that collectively cover the full identify, protect, detect, respond, and recover lifecycle:

  — Manage security posture: focused on establishing or improving a *posture management* function that integrates IT and business processes to continuously improve the ability to prevent incidents

  — Manage security incidents: focused on establishing or improving a *security operations* capability that finds and removes attacker access (from detections as they enter or by proactively hunting for attackers that evaded detection)

- Manage collaboration

  Focused on ensuring security functions collaborate with each other and other business units in a continuous learning and continuous improvement Zero Trust environment. This includes collection and dissemination of security intelligence – ensuring all stakeholders are informed about security incidents and learnings that they can use to reduce organizational risk.

The organization's ISMS should be tailored to the mission, needs and objectives, security requirements, processes, and the size and structure of the organization. Each company's ISMS is expected to change over time.

5.2.1 Zero Trust Security Collaboration and Information Security Management

Zero Trust drives agility, enabling the organization to rapidly respond to a continuous stream of external context (attacks, insights, risks, best practices, etc.). Figure 11 illustrates how security functions collaborate with each other in a continuous learning and continuous improvement model that increases security agility.

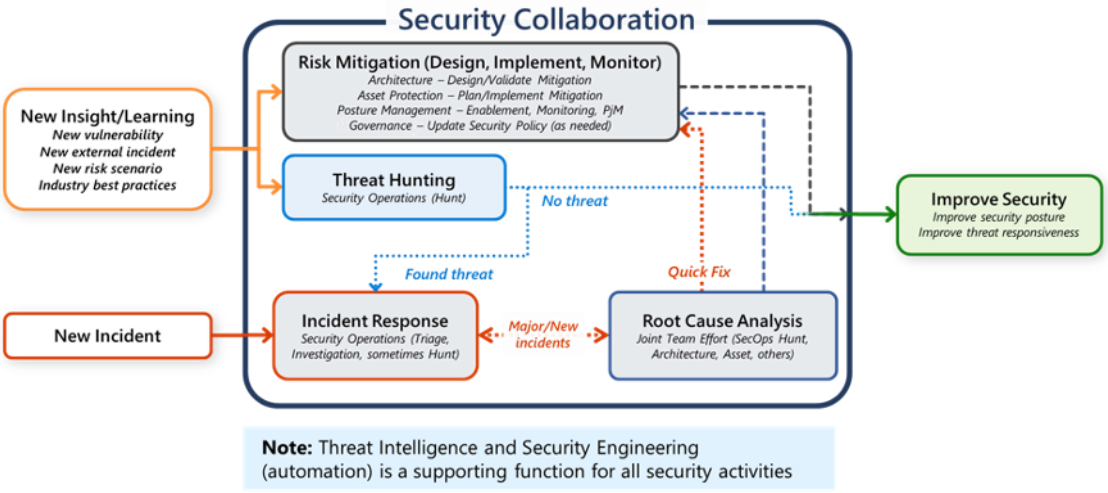

Figure 11: Security Function Collaboration Illustration

Any "New Incident" is managed by the Security Operations team, who performs an "Incident Response".

For major or new/novel incidents, a joint team effort should perform a "Root Cause Analysis" to identify how to best mitigate risk (by identifying quick fixes for immediate effect or other mitigations that require more analysis).

"Risk Mitigation" also involves multiple stakeholders with:

- Architecture or engineering creating and validating a design
- Asset protection teams planning and implementing the mitigation
- Posture management providing support, enablement, and monitoring (as well as some project management as needed)
- Governance teams updating the security policy (as needed)

A "New Insight/Learning" can take multiple forms including a new vulnerability (such as Log4j™), a new external incident (such as SolariGate), a new loss scenario (such as extortion or ransomware), or a new industry best practice. These may require mitigating the risk, proactively looking for a compromise that was previously missed ("Threat Hunting"), or both. Any threats that are found with threat hunting (e.g., attackers that previously evaded standard detections) will follow Incident Response processes (defined as Rapid Incident Response under Asset-Centric Security Operations). Note that the definition of the TRM is addressed in Chapter 5.

These actions will improve security by continuously integrating learnings that help the organization adapt to the external environment.

Information security management establishes a structure based on risk and controls and the manner of executing them. In short, it uses risk and core drivers – security, business, risk, technology – to determine the core governance framework required to operate the organization, especially where these areas work together to provide the capability.

Therefore, Zero Trust information security management emphasizes using risk and the other drivers to establish the structure (information security system) to manage a ZTA and strategy (including the Roadmap).

5.2.2 Manage Policy

Policy Management is one component of the ISM System. It provides policies that define a security controls framework used to manage security control requirement. These controls are developed using the combination of business, technology, regulatory controls, and security controls that form the body of controls. From those controls, policies can be developed and become standards in an organization.

The primary function of the policy management system is translating risk in the risk register into clear standards and requirements and into actionable control procedures that technical teams can implement to mitigate the risks.

Figure 12 describes this process.

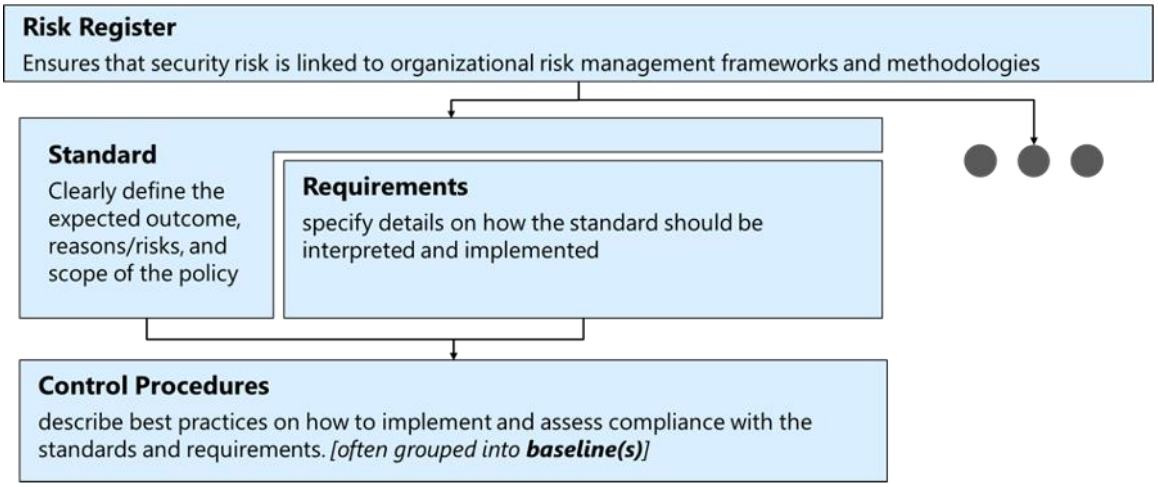

Figure 12: Policy Elements

The work of managing policy primarily comes from the ongoing maintenance and implementation of information security documentation, particularly the control standards. The first step in managing change to security controls designed to mitigate a particular risk is to model the threat surface and determine the associated controls, policies, and procedures.

Changes to the organizational "Risk Register" occur when:

- Change is initiated by updating security control requirements
- There are improvements to existing controls typically through introduction of new or improved technology, such as that associated with Zero Trust

Illustratively, the business addition of a new capability for vendor integration might result in the need to support streaming as a channel, with multiple endpoints. Multiple protocols might be involved, as well as integrations with different platforms. This now results in a threat surface area that might vary based on the stream, its integration point and technology, etc.

Security policy management for Zero Trust must be Agile and continuously improved to ensure it can keep up with changes to cloud platforms, business requirements, regulatory drivers, technology change, and security threats and capabilities. Policy updates may be done using regular sprints (or a similar process) where teams meet at a practicable cadence to discuss, write, and update policy to ensure that security keeps pace with business changes – some organizations may find it feasible to meet every few weeks, while others may meet every few months. Note also that different policy levels will need changes at different rates.

Managers of organizations' computing infrastructure have two key activities:

- Continuously improve the security infrastructure components
- Operate hosting systems including cloud services in compliance with security policy

Managers responsible for software development, including purchased software, need to:

- Integrate their systems with security infrastructure services
- Ensure the robustness of their application by applying a secure development process

All organizations must make decisions about relevant organizational risk. This requires documenting and consistently executing the processes behind these decisions. Figure 13 depicts an example of various governance functions within an organizational that are relevant in helping an organization identify and prioritize organizational risks and business investment to mitigate them.

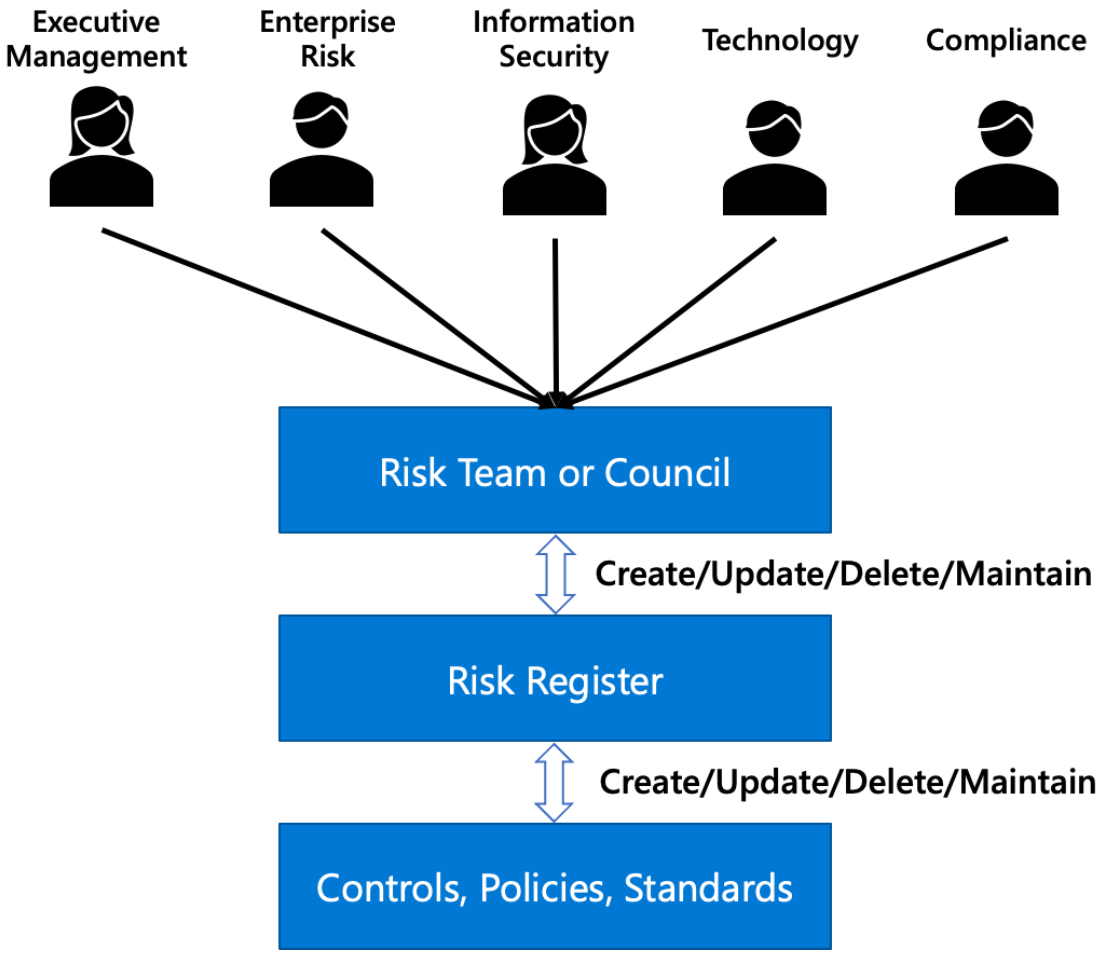

Figure 13: Risk and Policy Management Process

Organization type and size will impact the formality of having established risk and policies teams or councils – Small and Medium-Sized Businesses (SMBs) may have the same individual representing multiple business functions, while larger organizations may have a formally defined group tasked with individual responsibilities.

5.2.3 Manage Incidents

The incident management process monitors activities of the organization and investigates and resolves incidents of threats (threat events) to the organization's assets as they are detected.

The Threat Response Management subprocess depicted in Figure 14 is from *NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide* [NIST 2012] that is the basis of incident management at many organizations.

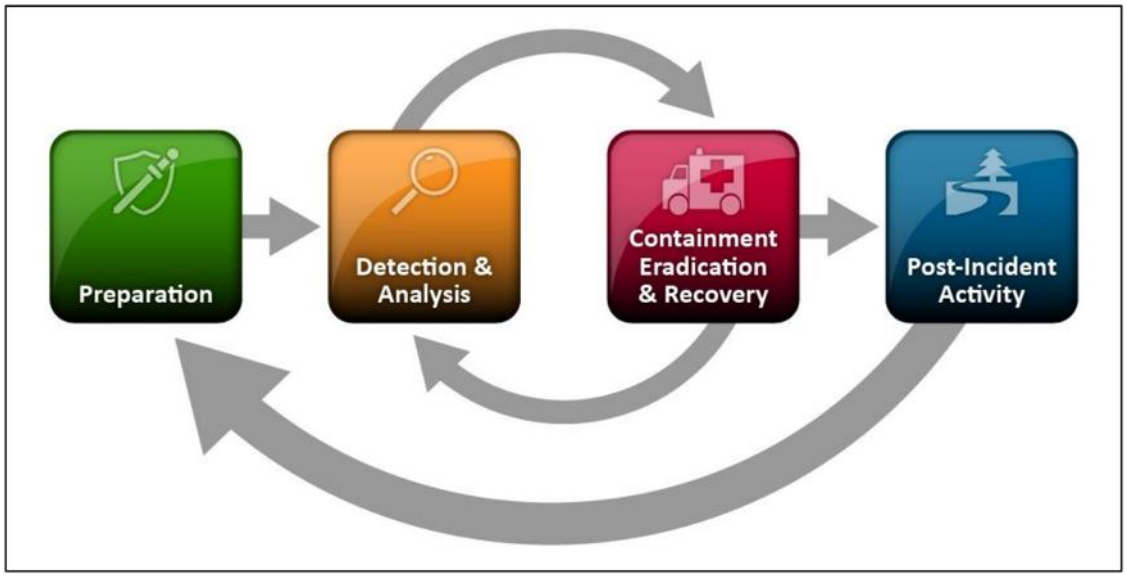

Figure 14: Threat Management Response Subprocess [Source: NIST SP 800-61 Rev. 2]

Key focus areas of Zero Trust are:

- MTTR incidents as the key metric to reduce organizational risk by reducing attacker dwell time

  — MTTA an incident is also a key leading indicator

- Continuous collaboration with threat intelligence, posture management, asset access, and other teams to continuously improve all functions

- Continuous integration with new assets and asset types in the organization

  In organizations with a DevSecOps organizational unit and function, IT Service Management (ITSM) will often act as the source of incidents and will be involved in these steps as the steward of these assets, similar to how IT operations teams currently do for infrastructure assets.

- Increased focus on proactive activities *via* the threat hunting function

Threat analysis, response planning, and community communications are performed by the Manage Incidents function. Recovery Management capabilities are performed by the Manage IT Infrastructure Security function.

These details illustrate the difference between Manage Incidents, which is in a constant ready and reacting state, and Manage IT Infrastructure Security, which operates to standard IT operations processes.

Figure 11 illustrates how the function integrates with other functions.

5.2.4 Posture Management for IT Infrastructure Security

Posture Management addresses two key capabilities to provide the mechanism to avoid incidents:

- The ability to proactively address security risk
- The ability to establish a continuous monitoring and governance capability

The design/build and run operate aspects of Posture Management are covered in Section 6.2.6 and Section 6.4.6. From an information security management perspective, IT infrastructures processes must be applied to operate and manage change for security components. Most change follows planned change cycles, incorporating requirements from security initiatives. Some changes arise as urgent changes funded and approved by Manage Risk as required to respond to infrastructure vulnerabilities identified by Manage Assessments or Manage Incidents.

In practice, the IT, the DevOps, and Information Systems Security (InfoSec) organizations work jointly to ensure that organizational functions such as Patch Management are conducted seamlessly.

Figure 15 shows how the Manage IT Infrastructure Security scope includes several Asset Protection Management capabilities and is influenced by the Security Policy Management Capability and Security Initiatives Management.

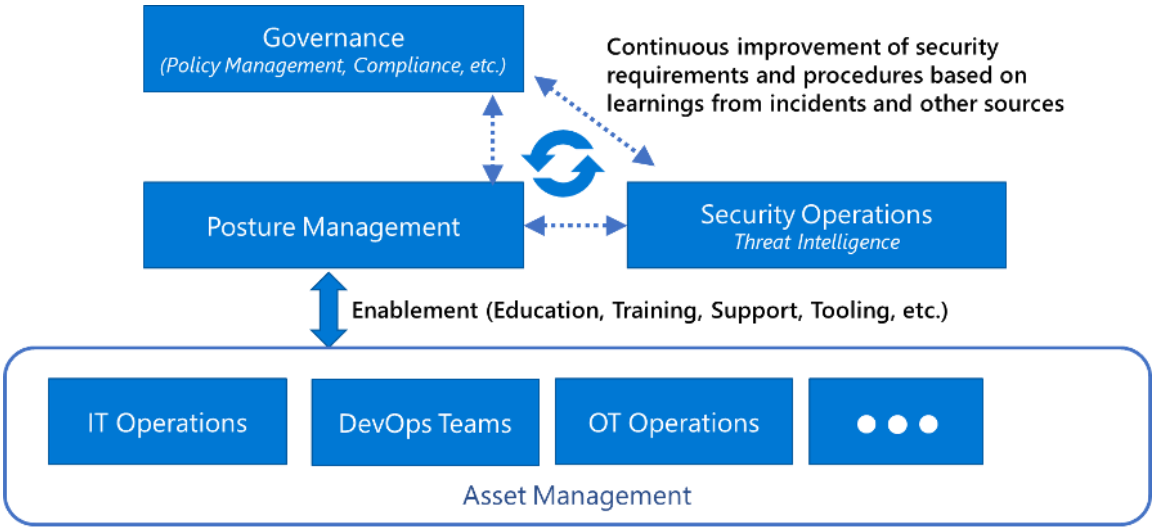

Figure 15: Posture Management

5.2.5 Manage Asset Access

Managing Asset Access needs to address both system and data assets. Authentication, authorization, and administration are the security elements that together enable an organization to control access.

Zero Trust brings capabilities such as Adaptive Access Control and System and Data Asset Protection that need to be considered.

From an information security management perspective, the Manage Asset Access function for system assets should include:

- The risk assessment and associated controls and standards
- The Risk Council that supports this
- The IT Application and Operations, and Security organizational entities that develop and maintain the assets and determine the implementation of the policies and standards in the development of the assets
- In practice, making sure that clearly defined accountabilities are established, as well as automation as far as is possible in the maintaining of asset access throughout their lifecycle and function

  This is typically using a Responsible, Accountable, Consulted, Informed (RACI) or another decision rights model.
- A clear definition of the organizational structures associated, and the standard operating procedures is critical for success

From an information security management perspective, the Manage Asset Access Function for data assets should include:

- The establishment of a function and capability in the security organization to:
  - — Develop controls, policies and procedures, and standards under the guidance of the Risk Council
  - — Establish a working agreement and structure (such as Data Security Council) with the information architecture and data governance functions to ensure that there is a clear understanding of the lifecycle of the data element from provisioning to deprovisioning

    That there is a clear understanding of its business value, and its meaning, if relevant in an enterprise or other context.
  - — Establish clearly defined policies and procedures, controls, and standards so that the policies to determine access can be clearly defined and automated
- The establishment of controls, policies and procedures, and standards to ensure clearly defined guidance exists on what is to be done with respect to data elements with regard to data protection
- The engagement and awareness of where the data is, and its movement, from a data loss prevention perspective across the lifecycle of the data

5.2.6 Manage Integrations and Data Exchange

In the digital era, organizations must define the flow and governance of data over various communication channels. In these scenarios, a number of stakeholders may be involved in managing the security assurances for this Data Exchange. The Information Security Management Model must help to define:

- The controls, policies, procedures, and standards to be followed in the case of the different communication channels. This should include all aspects of the Confidentiality, Integrity, and Availability (CIA) triangle

  Governance and guidance on what must be logged should be taken into account and provided. The Data Protection function should work with engineering and operations to make sure that repeatable processes are established.

- This should cover all stages in lifecycle of data from creation to destruction, including all updating, copying, sharing, moving, and other modification of data

- In the event that techniques such as tokenization are followed, the Security Organization should provide the governance and leadership to ensure implementation

5.3 Risk Management Model

Risk addresses potential loss, but effectively managing risk is a necessary component of business growth. Zero Trust is focused on enabling business decisions and goals, so it must look at risk and opportunity in the way that the business does – as balancing reducing potential loss at a reasonable cost against potential future gain. Zero Trust focuses on accurate and efficient risk estimates that can be used by business leaders at different levels. Because the future is always partially unknowable and business, technology, and security risk factors are continuously changing, Zero Trust risk management focuses heavily on continuous improvement of risk management as well.

Per ISO Guide 73:2009, risk management refers to the "coordinated activities to direct and control an organization with regard to risk" [ISO 73:2009]. A risk assessment is the "overall process of risk identification, risk analysis, and risk evaluation", and risk analysis refers to the "process to comprehend the nature of risk and determine the level of risk". These are summarized in the model shown in Figure 16.

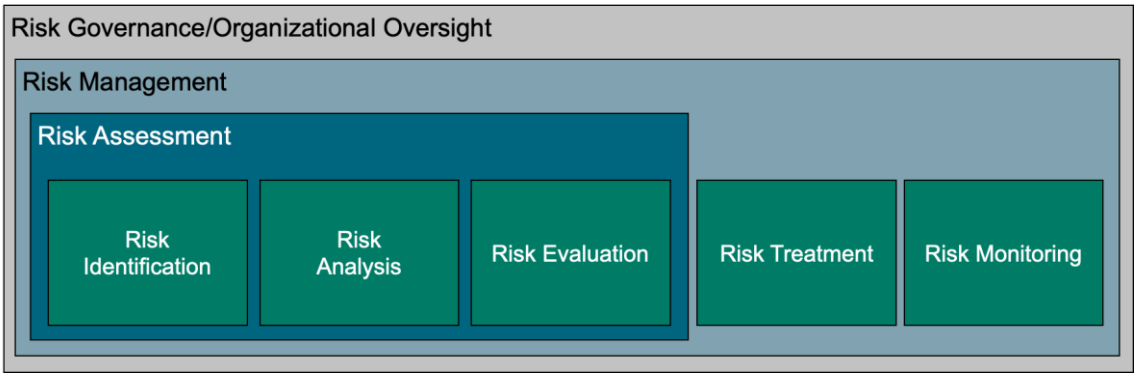

Figure 16: Risk Analysis in Context [Source: C20B]

Cybersecurity risk is fundamentally an organization-wide risk and must be managed as such. Cybersecurity risk shall be assessed and managed across the organization, and individual system owners must be held responsible for their role in managing risk to the organization. This is analogous to the risk of a fire in a factory – any fire can cause the whole building to burn down, regardless of where it starts. The owner of one piece of equipment cannot simply accept the risk of starting a fire that can damage the whole factory, though this is often how cybersecurity risk accountable is inadvertently structured.

5.3.1 Risk Analysis Model

The Open FAIR Body of Knowledge defines risk as the probable frequency and probable magnitude of future loss (also known as "loss exposure") that a Primary Stakeholder will bear within some defined time period [C20B]. Risk is measured by making forward-looking estimates of the probable frequency and the probable magnitude of a loss should it occur, and it is measured and managed from the perspective of the Primary Stakeholder, the party who bears the economic loss of the adverse events. To further refine risk and its components, the complete risk taxonomy develops the two sub-factors of risk: Loss Event Frequency and Loss Magnitude, as shown in the model in Figure 17.

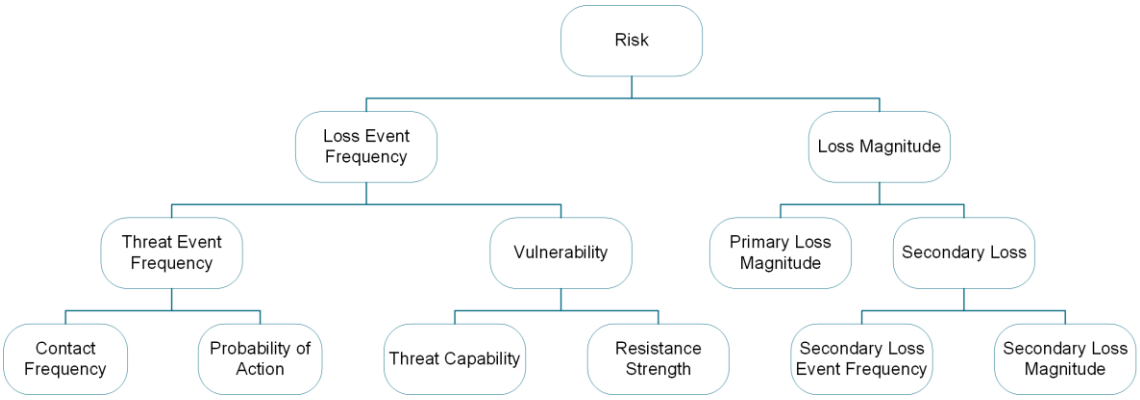

Figure 17: High-Level Risk Taxonomy Abstractions [Source: C20B]

5.3.2 Loss Scenario and Controls Model

While the risk analyst is responsible for helping the organization understand "How much risk do we have?", risk managers and decision-makers must answer different questions: "How does current-state risk compare to tolerance, and what, if anything, should be done to reduce probable future loss from a given Loss Scenario?". Tolerance for loss is sometimes referred to as risk appetite.

Doing something about risk consists of implementing controls that either reduce the Loss Event Frequency (reduce the likelihood of the Loss Scenario occurring) or reduce the Loss Magnitude of the Loss Event once it has occurred (mitigate the severity of the loss).

Figure 18 shows the decomposition of the Loss Scenario with the Open FAIR Controls and Categories as well as the NIST CSF color scheme.

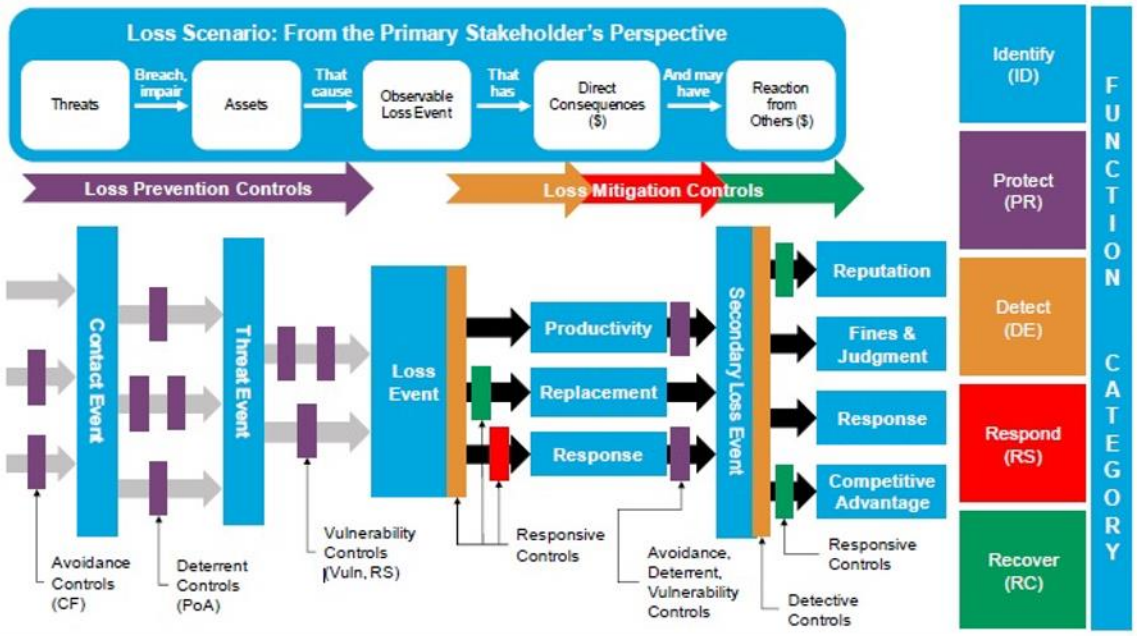

Figure 18: Decomposing an Open FAIR Loss Scenario, including the Open FAIR Control Categories and the NIST CSF Five Functions [Source: C20B]

6 Zero Trust Technology Reference Model

This Chapter introduces readers to the Technical Reference Model that defines the capabilities required for Zero Trust and realizes them into technology components. The capabilities define the outcomes (what Zero Trust is) and the ABBs define how to build it.

This section will enable leaders and practitioners to build implementation plans and implement the model for their organization by describing how to build Zero Trust capabilities and solutions that are adapted to your organization's unique business model and technical estate – most, if not all, organizations will need to tailor Zero Trust priorities and elements to their individual situations and requirements.

Figure 19 illustrates the process of realizing a capability-centric architecture – starting with defining required capabilities from the standard, determining ABBs required to deliver it, mapping these ABBs to associated standards, and then planning architectures and specific solutions.

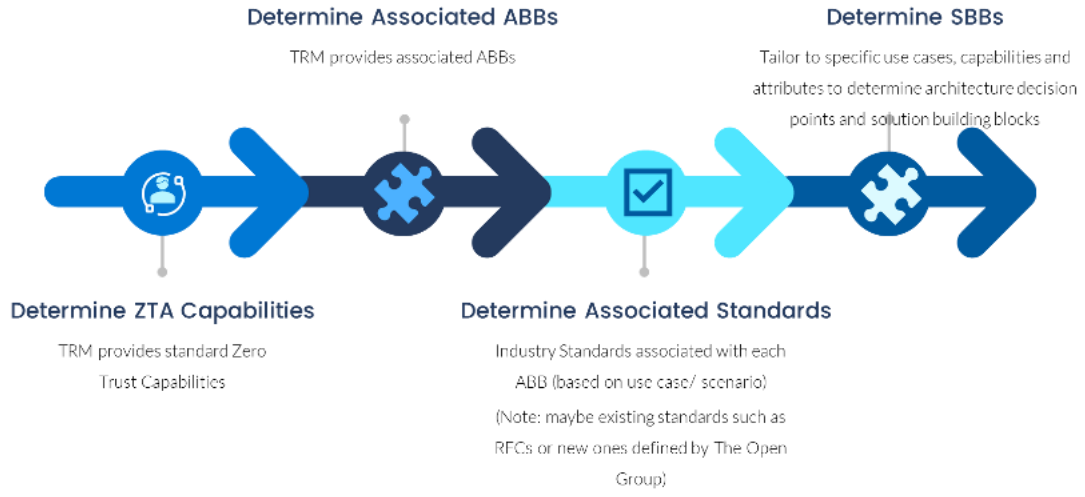

Figure 19: Mapping Capabilities to Solutions

This section covers two ways of viewing Zero Trust:

- A capability view of all high-level capabilities of the Zero Trust Architecture (ZTA)

  Dependent L2 and L3 capabilities may be identified, and in which case, they are denoted as L2 or L3 capabilities

- An ABB view that shows all the core components for ZTAs

  These ABBs are the logical architectural building blocks which realize the capabilities associated with designing, building, and operating ZTAs

Figure 20 illustrates the different parts of the Technical Reference Model.

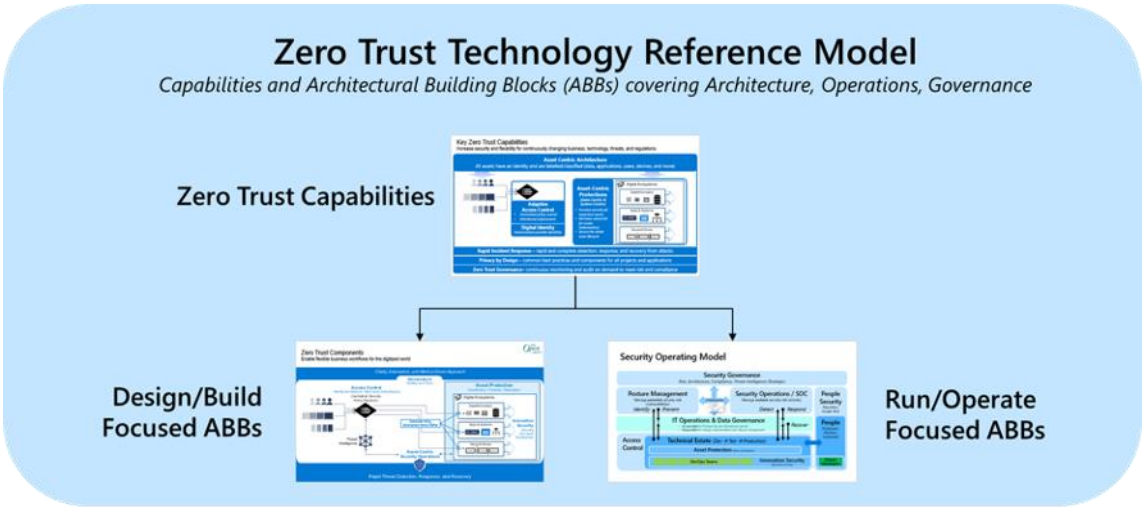

Figure 20: Capabilities, ABBs, and the Technical Reference Model

These views help business leaders and users, technology leaders and practitioners, and security and leaders see Zero Trust from their points of view and how it applies to their roles.

ZTAs are characterized by:

- Reduced threat surface area and complexity
- Reduced blast radius

They are also asset-centric, as opposed to traditional *network-centric* architectures. Assets in a digital era context can be classified into two groups – data assets and system assets. System assets manipulate the data (APIs (microservices), applications, systems, etc.). Examples of modern-day threats for the two asset classes include data breaches and ransomware attacks, respectively.

Note: Throughout Chapter 5, two main colors are used to distinguish between relevant concepts: blue is utilized for Capabilities, and green is utilized for ABBs.

6.1 Capabilities, ABBs, and SBBs and a Metamodel for Deriving Architectural Decisions

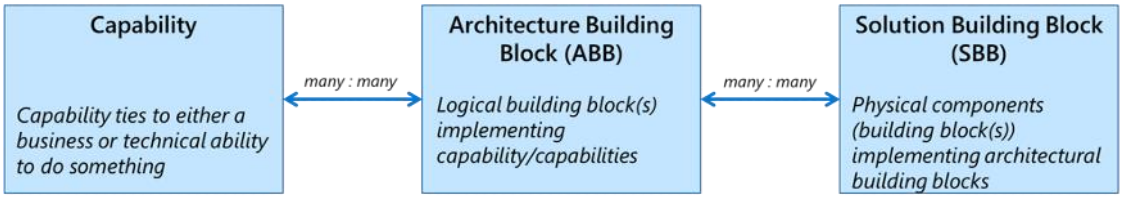

Figure 21: Capability, ABB, and SBB Relationships

As Figure 21 shows, capabilities enable doing something. In the context of the reference model, this refers to technical capabilities, such as the ability to do access control, or log accesses. ABBs are those logical components that implement (logically) those capabilities. Finally, SBBs are the physical components that are how these ABBs are realized. ABBs allow visualizing the architecture in terms of logical blocks. SBBs encompass reusing, purchasing, accessing (as in

Software as a Service (SaaS) solutions) or building the component. Note that the order of deciding what to use or pick may vary based on the enterprise, tooling available, etc.

Tooling available from vendors often provides multiple functions, allowing organizations to rapidly implement multiple SBBs and/or ABBs with a single product (or suite of products).

6.1.1 The Zero Trust Metamodel (Adapted from the Service Oriented Architecture (SOA) Reference Architecture Standard [C119])

Figure 22 shows the Zero Trust Metamodel.

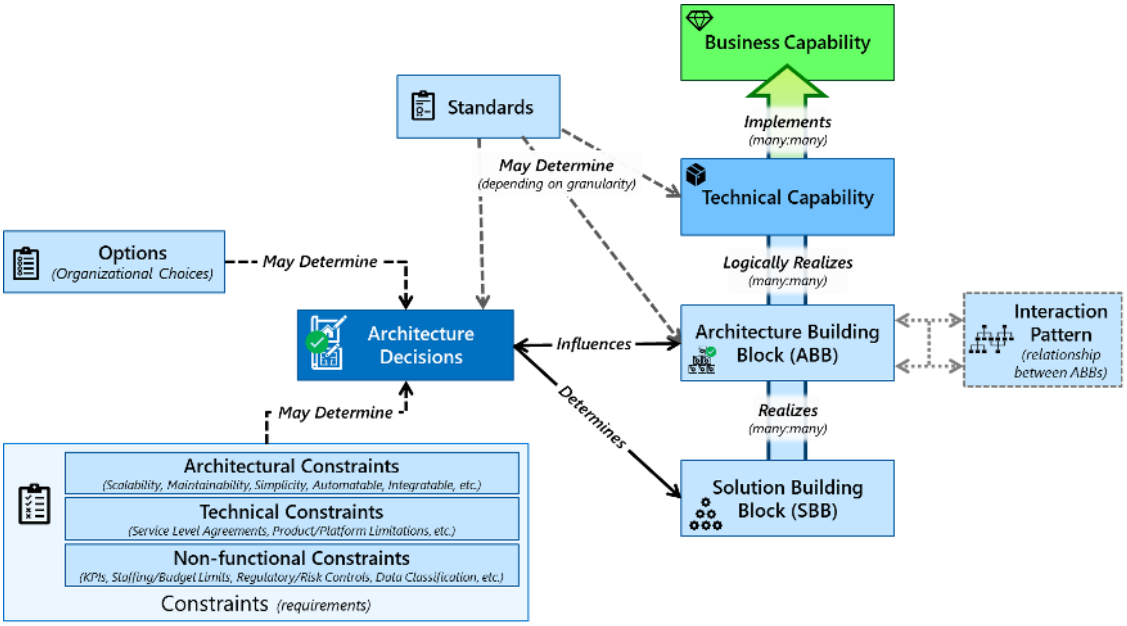

Figure 22: Zero Trust Metamodel with full set of Relationships

Figure 23 depicts the Zero Trust Metamodel in UML format.

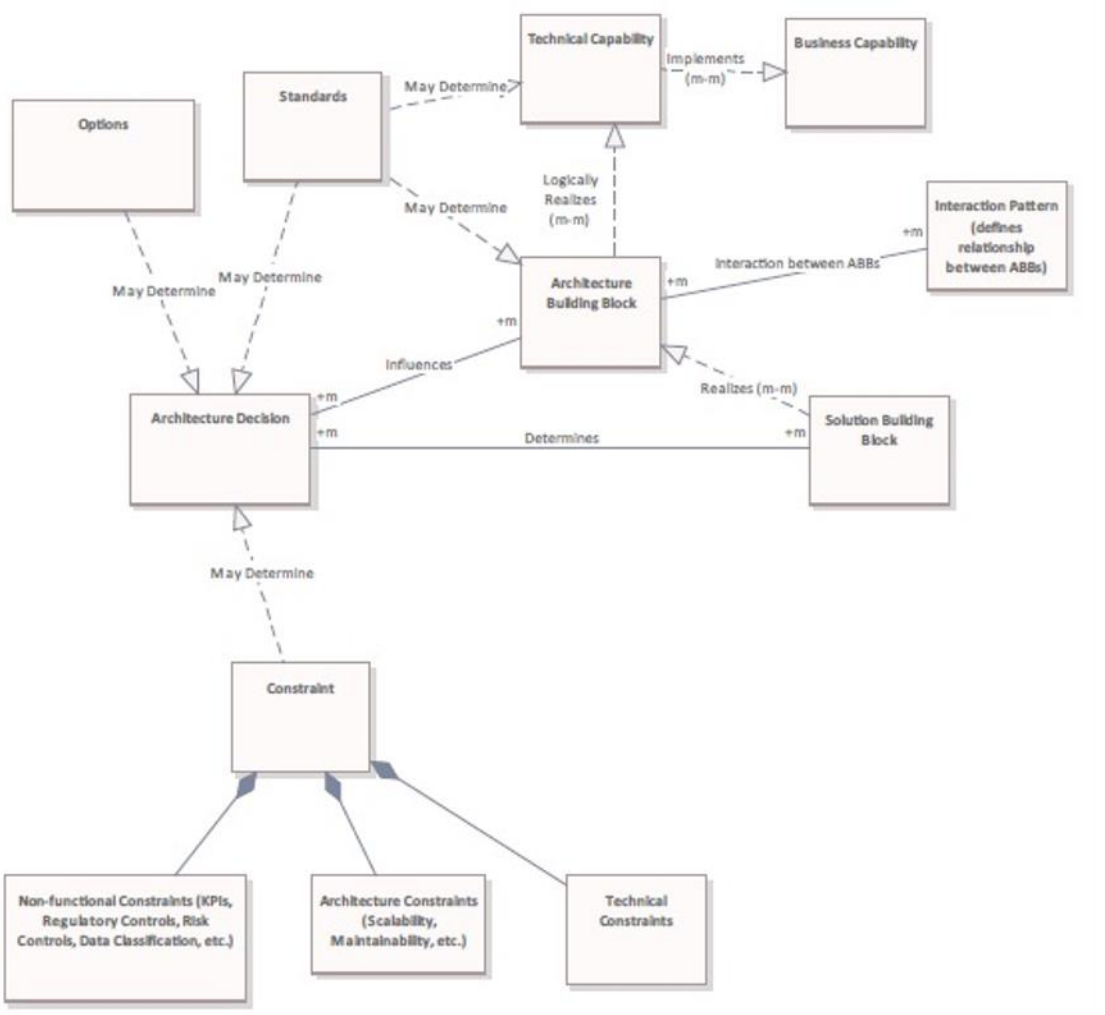

Figure 23: Zero Trust Meta Model in UML Format

Figure 23 shows the following elements:

- Capability: An ability that an organization, person, or system possesses to deliver a product or service

  A capability represents a requirement or category of requirements that fulfill a strongly cohesive set of needs. This cohesive set of needs or functionality is summarized by name given to the capability. In the context of the reference model, a capability refers to a technical ability. Capabilities are hierarchically ordered as Level 1 (L1) (highest, most abstract level), and composed of Level 2 (L2) Capabilities, which may be further decomposed into Level 3 (L3) Capabilities and so on.

- Architecture Building Block (ABB): An architectural component that specifies the required SBBs at a more logical (or supplier-independent) level[11]

[11] Refer to Section 4.9 of the TOGAF® Standard, 10th Edition [C220].

- Level 1 ABB (L1): An abstraction of a grouping of a cohesive set of lower level ABBs, architectural decisions, interactions among ABBs, and interactions among lower level ABBs, that support a set of related capabilities

  By definition L1 ABBs tend to be compositional in nature. Interactions and relationships between L1 ABBs are defined by "Options".

- Options: A collection of possible choices available in each Level 1 (L1) ABB that impact other artifacts of a L1 ABB

  Options are the basis for architectural decisions within and between L1 ABBs, and have concrete standards, protocols, and potentially solutions associated with them. Options are often determined by the environment that exists in the technical estate and help determine what decision will then follow. Illustratively, an option might be that the environment uses a particular public cloud product or SaaS product to support one or more Capabilities and ABBs. There may be an option to purchase a new platform, build a custom one, or reuse some existing component. Along with the application of the different constraints, the Options help form an architectural decision.

- Non-Functional Constraints (*aka* Non-Functional Requirements): Illustrative non-functional constraints such as the number of users or APIs to be supported, etc.

  Regulatory controls fall in these constraints. For example, Payment Card Industry (PCI) may define the constraints for Data Tokenization in a particular manner, or there might be controls determined by NIST for a US government agency.

- Architectural Constraints: Architectural constraints usually refer to architectural quality attributes, such as scalability, redundancy, etc.

- Technical Constraints: Technical Constraints usually refer to technical boundaries set by the technology environment that Architectural Decision is being made in.; for example, there might be some legacy stacks which preclude or alternatively mandate the use of a particular integration and encryption standard

- Standards: Documents that define the interactions and expectations for Technical Capabilities, ABBs, and SBBs

  Based on the granularity, standards may define the Technical Capabilities and ABBs, or as in the case of more granular standards, form more detailed definitions and boundaries for them.

- Architectural Decision: A decision derived from the options, non-functional, and architectural constraints, and standards

  Architectural Decisions are used to determine which ABBs are to be associated with which capabilities and which ABBs are associated with which SBBs. Architects (including security, enterprise, and solution architects) should use this framework to make architectural decisions.

- Interaction Pattern: Diagrams, patterns, pattern languages, and interaction protocols that define the relationship between ABBs

Note: This model has been adapted from The Open Group SOA Reference Architecture, with some modifications.

6.2 Capability View

For this Zero Trust model to be useful to the organization, it must provide consistent outcomes to the organization over time. These outcomes are provided by a set of durable capabilities that remain constant, even as the technologies that enable them to evolve over time.

For example, the ability to determine identity for assets in a Zero Trust ecosystem is critical for implementing adaptive asset control. Hence the ability to have a unique, reliable, digital identity would be a Zero Trust capability. Similarly, the ability to create a secure token *in lieu* of the actual sensitive data is foundational for some techniques for data centric security.

Figure 24 illustrates key Zero Trust capabilities that differentiate a Zero Trust approach from a classic security model.

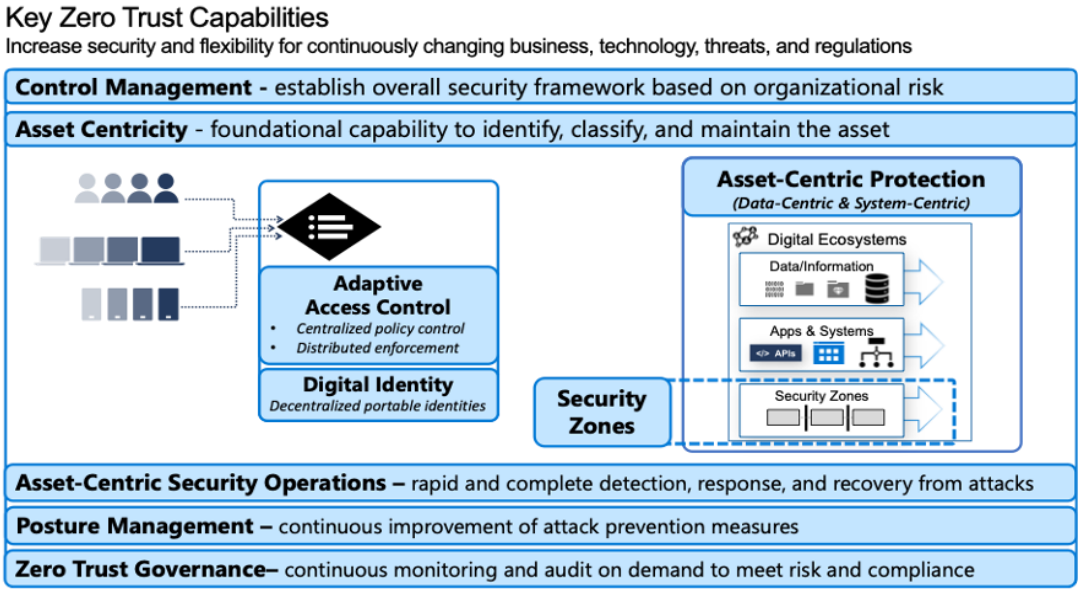

Figure 24: Key Zero Trust Capabilities

These key Zero Trust capabilities are listed below and will be described in more detail in the subsequent subsections:

- Asset-Centricity
- Adaptive Access Control
- Digital Identity
- Asset-Centric Protection
- Asset-Centric Security Operations
- Posture Management
- Zero Trust Governance
- Security Zones
- Controls Management

6.2.1 Asset-Centricity Capability

Asset Centricity provides the ability for organizations to identify, classify, and maintain the asset. It is foundational to other Zero Trust capabilities.

Table 1 lists each Asset Centricity capability and which ABBs support it.

Table 1: Asset-Centricity Capabilities and Supporting and ABBs

Capability Number	Capability	Level	ABB
AC-1	Asset-Centricity	1	Asset-Centricity Platform (ABB ACP1.0).
AC-1.1	Digital Identity Binding	2	Identity Wrapper (ABB ACP-1.1).
AC-1.2	Asset Management	2	Asset Repository (ABB ACP-1.2).
AC-1.2.1	Asset Classification	3	Asset Taxonomy (ABB ACP-1.3).
AC-1.2.2	Asset Capture	3	Asset Discovery Engine (ABB ACP-1.4).
AC-1.2.3	Asset Metadata Storage	3	Asset Repository (ABB ACP-1.2.3).
AC-1.2.4	Asset Lifecycle Management	3	Asset Lifecyle Manager (ABB ACP-1.10).
AC-1.3	Asset Integrity Protection	2	Infrastructure as Code (ABB ACP-1.9). Source Code Management Engine (ABB ACP-1.5). Continuous Integration (CI) / Continuous Delivery (CD) Engine (ABB ACP-1.16).
AC-1.3.1	Patch Management	3	Asset Patch Management Manager (ABB ACP-1.6).
AC-1.3.2	Configuration Management	3	Configuration and Account Management ABB (ABB ACP-1.13).
AC-1.3.3	Asset Operational Integrity Process Management	3	Policy and Controls engine (ABB ACP-1.7). Policy Compliance audit tool (ABB ACP-1.8).

Capability Number	Capability	Level	ABB
AC-1.3.4	Asset Supply Chain Integrity Management	3	Software Bill of Materials (SBOM) Manager (ABB ACP-1.11). Supply Chain Security Risk Manager (ABB ACP-1.12).
AC-1.3.5	Asset Integrity Policy Management	3	Policy and Controls engine (ABB ACP-1.7). Policy Compliance audit tool (ABB ACP-1.8).
AC-1.3.6	Asset Vulnerability Management	3	Common Vulnerabilities and Exposures (CVE) Repository (ABB ACP-1.14). CVE Manager (ABB ACP-1.15).
AC-1.3.6.1	Vulnerability Monitoring	4	Continuous Vulnerability Scanner (ABB ACP-1.17). Internal Vulnerability Scanner (ABB ACP-1.17.1). External Vulnerability Scanner (ABB ACP-1.17.2). External Attack Surface Management (ABB SPMP-1.1.1).
AC-1.3.6.2	Vulnerability Remediation	4	Vulnerability Remediation Process (ABB ACP-1.18).
AC-1.3.6.3	Vulnerability Prevention	4	Vulnerability Prevention Process (ABB ACP-1.29).

The Asset Centricity capability includes the following capabilities:

- Asset-Centricity (AC-1) – provides the ability for organizations to identify, classify, and maintain security of assets, it is foundational to other Zero Trust capabilities
  - — Digital Identity Binding (Identify) (AC-1.1) – provides the ability to assign individual identities to assets, including data, applications, endpoints, etc., in a verifiable manner
  - — Asset Management (AC-1.2) – provides the ability to classify, capture assets and their metadata in the technical domain and store that information
    - Asset Classification (AC-1.2.1) – provides the ability to divide the protected resources in the digital ecosystem into assets and asset classes, based on business value
    - Asset Capture (AC-1.2.2*)* – provides the ability to capture asset metadata from the technical estate of the enterprise

This capability allows for the scanning and determination of what individual assets are there in the technical estate, uniquely qualifying them, classifying them, associating them with any metadata that they have, and either periodically or on an event-basis:

- On addition, add this metadata to a repository of asset metadata
- On deletion, delete this asset metadata from the repository
- Update the stored metadata in the repository

- Asset Metadata Storage (AC-1.2.3) – provides the ability to store and manage asset metadata
- Asset Lifecycle Management (AC-1.2.4) – provides the ability to manage the lifecycle of the metadata of assets across the lifecycle of assets from provisioning to deprovisioning

— Asset Integrity Protection (maintain) (AC-1.3) – provides the ability to ensure that the assets in the technical estate are properly maintained

This includes the following sub-capabilities:

- Patch Management (AC-1.3.1) – provides the ability to apply patches to all assets
- Configuration Management (AC-1.3.2) – provides the ability to monitor and ensure configurations are maintained following recommended security configurations
- Asset Operational Integrity Process Management (AC-1.3.3) – provides the ability to monitor and follow secure operational practices
- Asset Supply Chain Integrity Management (AC-1.3.4) – provides the ability to validate software design/implementation security (including supply chain components)
- Asset Integrity Policy Management (AC-1.3.5) – provides the ability to monitor, create, modify, and delete, and apply security policy to all assets in your technical estate for all other Zero Trust capabilities

  It also allows easy change of those policies and the addition of new consumers or classes of consumers. This fundamentally enables security agility and organizational agility.
- Asset Vulnerability Management (AC-1.3.6) – provides the ability to manage all vulnerabilities to assets in the technical estate. These can be broken up into:
  - Vulnerability Monitoring (AC-1.3.6.1) – provides the ability to monitor the status of all vulnerabilities
  - Vulnerability Remediation (AC-1.3.6.2) – provides the ability to remediate all vulnerabilities
  - Vulnerability Prevention (AC-1.3.6.3) – provides the ability to provide preventive measures for all vulnerabilities

The asset vulnerabilities management capability covers all vulnerabilities including (but not limited to) the following:

- Functional (software) vulnerabilities that increase organizational risk from vulnerabilities in software design or implementation

  This typically takes the form of CVEs that represent vulnerabilities in software authored by an external source and vulnerabilities in software your own teams developed. This is instantiated when security patches and updates for CVEs are not applied, or development teams introduce them during development (often because they do not apply secure development best practices, such as those detailed in Open Worldwide Application Security Project (OWASP) Top 10 and other guidance)

- Configuration vulnerabilities that increase organizational risk from misconfigurations of systems that enable attackers to more easily access or abuse systems

  This typically takes the form of monitoring the current configurations against the recommended security configuration from manufacturers, government agencies providing security guidance, or credible independent organizations like the Center for Internet Security (CIS)

- Operational vulnerabilities that increase organizational risk in operational processes and practices from bad operational practices

  The excessive use of service accounts and a lack of their management are an example. Illustratively, posture management would monitor for risky usage of privileged administrator accounts such as:

  — Bypassing the Privileged Identity (PID) / Privileged Access Management (PAM) system by using built-in administrator/root accounts to get around security controls

  — Using privileged accounts on lower trust user devices and workstations instead of privileged access workstations (which are secured at a higher level for these accounts)

6.2.2 Adaptive Access Control Capability

Adaptive Access Control provides the ability to implement consistent access policy enforcement across any type of asset (resource).

Adaptive Access Control involves the ability to identify a consumer (subject), support authentication and authorization, and implement access decisions at an individual asset level that is informed by security risk context. Table 2 lists adaptive access control capabilities and supporting ABBs.

Table 2: Adaptive Access Control Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
AAC-1	Adaptive Access Control	1	Adaptive Access Control Platform (ABB ACP-1).

Capability Number	Capability	Level	ABB
AAC-1.1	Authentication (Known)	2	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2	Trust Validation (Trusted)	2	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.1	Subject Security Status	3	Adaptive Policy Decision Point (AAC-1.2). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.1.1	Subject Security Status Determination	4	Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.1.2	Subject Security Status Management (Create, Update, Delete)	4	Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.2	Policy Decisioning	3	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2).
AAC-1.2.2.1	Policy Enforcement (used by Authentication and Authorization)	4	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3).
AAC-1.2.2.2	Policy Management (Add, Delete, Create)	4	Adaptive Policy Manager (ABB AAC-1.4).

Capability Number	Capability	Level	ABB
AAC-1.2.2.3	Asset Entitlement Assignment	4	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.2.4	Adaptive Policy Determination For Subjects	4	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.2.2.5	Adaptive Policy Determination for Sessions	4	
AAC-1.3	Authorization (Allowed)	2	Adaptive Policy Information Point (ABB AAC-1.1). Adaptive Policy Decision Point (ABB AAC-1.2). Adaptive Policy Enforcement Point (ABB AAC-1.3). Adaptive Policy Manager (ABB AAC-1.4).
AAC-1.4	Policy And Identity Storage	2	Adaptive Policy Information Point (ABB AAC-1.1). Identity Provider (ABB AAC-1.5).

Note: Consumers are referred to as the subject, and the resource being accessed is referred to as the asset. In practice both are assets, but in the context of access control, one asset is acting in the role of a consumer (subject), and the other asset as a resource (object) being accessed/consumed (often to provide a service to the consumer).

The Adaptive Access Control capability includes the following capabilities:

- Adaptive Access Control (AAC-1) – provides the ability to implement consistent access policy enforcement across any type of asset (resource)
- Authentication (known) (AAC-1.1) – provides the ability to validate the identity of a subject, often in the form of an account in an identity system

- Trust Validation (trusted) (AAC-1.2) – provides the ability to measure trustworthiness of subjects and enforce the appropriate access policy on their access requests

  This ensures that subjects can only access valuable assets after providing proof that their account is under the control of the actual subject (and not an attacker or impersonator)

  For example, a user may be able to automatically access low value assets (e.g., local cafeteria menu) if they are at an elevated likelihood of potential compromise (such as unusual geographic location for that user that does not match previous behavior patterns). This same user in the same status should not be able to access high value intellectual property (like proprietary engineering designs) until the likelihood of account compromise has been reduced. This change in security status could take the form of a strong authentication method such as presenting biometric proof to the user's managed and trusted device.

- Subject security status (AAC-1.2.1) – provides the ability to categorize subjects (consumers) by how likely it is that the subject's account or credentials are currently under the control of a malicious actor

  Defining this security status using consistent, defined levels (such as a high/medium/low likelihood that the account/credentials are compromised) enables consistent and automatic policy enforcement in the face of dynamically changing threats and user behaviors

- Subject security status determination (AAC-1.2.1.1) – provides the ability to determine the security status of a subject based on various data sources and signals that indicated the likelihood that the account or credentials of the subject has been compromised by one or more malicious actors

- Subject security status management (create, updated, delete) (AAC-1.2.1.2) – provides the ability to develop and maintain policies associated with subject security status

- Policy decisioning (AAC-1.2.2) – provides the ability to determine whether the subject's account and session meets security policy for accessing the resource:

  — Policy enforcement (used by authentication and authorization) (AAC-1.2.2.1) – provides the ability to enforce security policy before allowing access to assets

  — Policy management (add, delete, create) (AAC-1.2.2.2) – provides the ability to develop and maintain policies that meet the organization's risk tolerance, capabilities, and other factors

  — Asset entitlement assignment (AAC-1.2.2.3) – provides the ability to grant or deny access to groups of assets (often by security levels or security zones)

  — Adaptive policy determination for subjects (AAC-1.2.2.4) – provides the ability to integrate security status factors for the subject into policy decisioning

    This could include assessing factors such as:

    - Whether the subject's account has been compromised by attackers
    - Whether the subject's credentials are known to be under the control of attackers
    - Whether the subject is currently authorized to use their account

— Adaptive policy determination for sessions (AAC-1.2.2.5) – provides the ability to integrate dynamic current context about the session in policy decisioning

This could include assessing factors such as:

- Whether human subjects have used strong phish-resistant multi-factor authentication
- Whether the subject's access request matches normal behavior patterns and locations
- Whether the subject's device is configured securely and is running an Endpoint Detection and Response (EDR) that reports no malware infections on the device, and so on

- Authorization (allowed) (AAC-1.3) – provides the ability to provide granular permissions the assets, often with a Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC) approach
- Policy and identity storage and management (AAC-1.4) – provides the ability to have the repository where identity is stored with associated entitlements (the Identity Provider (IDP)) and the storage of policies

6.2.2.1 Dependent Capabilities Reused by the Adaptive Access Control L1 Capability

The Adaptive Access Control capability reuses the Digital Identity Binding and Asset Management capabilities to support subject and asset identification, classification, and management.

Data classification is used to determine one of the policies used in determining risk levels to develop policies to apply to get access rights to resources and determine credential requirements of the subject.

Table 3 lists each reused capability for Adaptive Access Control and which ABBs support it.

Table 3: Reused Capabilities for Adaptive Access Control

Capability	Level	Design / Operational
Digital Identity (DI-1)	1	N/A
Digital Identity Binding (AC-1.1)	2	N/A
Asset Management (AC-1.2)	2	N/A
Data Classification (ACP-1.1)	2	N/A

Adaptive Access Control expands the traditional two-stage process of authentication (know) and authorization (allowed) into a three-part process that introduces explicit validation.

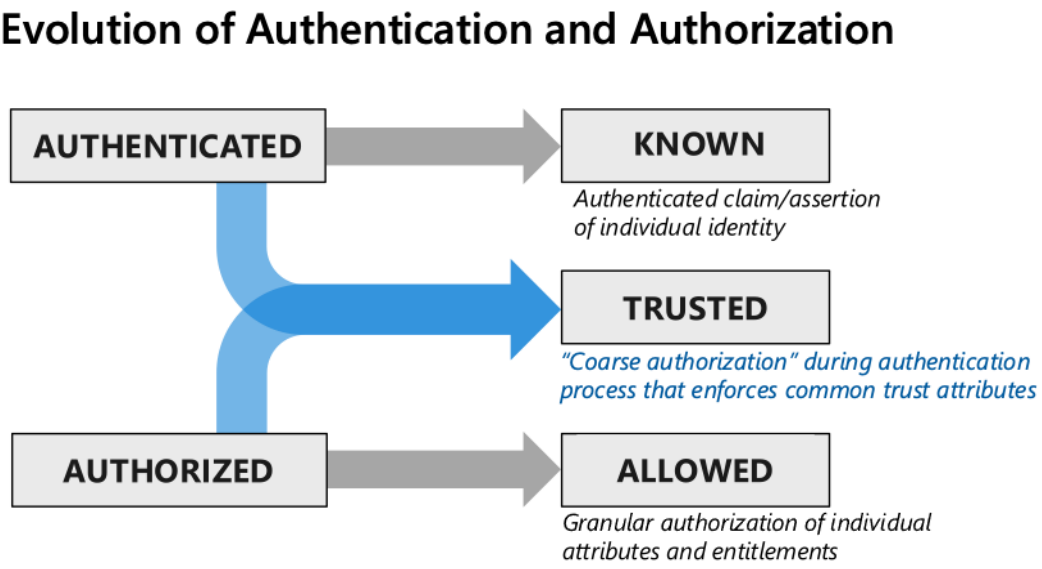

Figure 25: Evolution of Authenticated and Authorized to Known, Trusted, Allowed

This provides separation and explicit definition of the outcomes of access control:

- Known (Authentication – AAC-1.1) **–** the subject is who they claim to be
- Trusted (Trust Validation – AAC-1.2) – the circumstances and risk factors of the access request (and ongoing access session) are within risk tolerances/acceptability for the asset being accessed
- Allowed (Authorization – AAC-1.3) **–** the subject is granted the appropriate permissions and entitlements to the assets

Error! Reference source not found. shows that this evolution is comparable to how airport security has evolved to meet increased threat levels where a minimum level of security is consistently applied across all passengers beyond simply validating someone's identity (e.g., their government identification) and the tickets and entitlements they have bought.

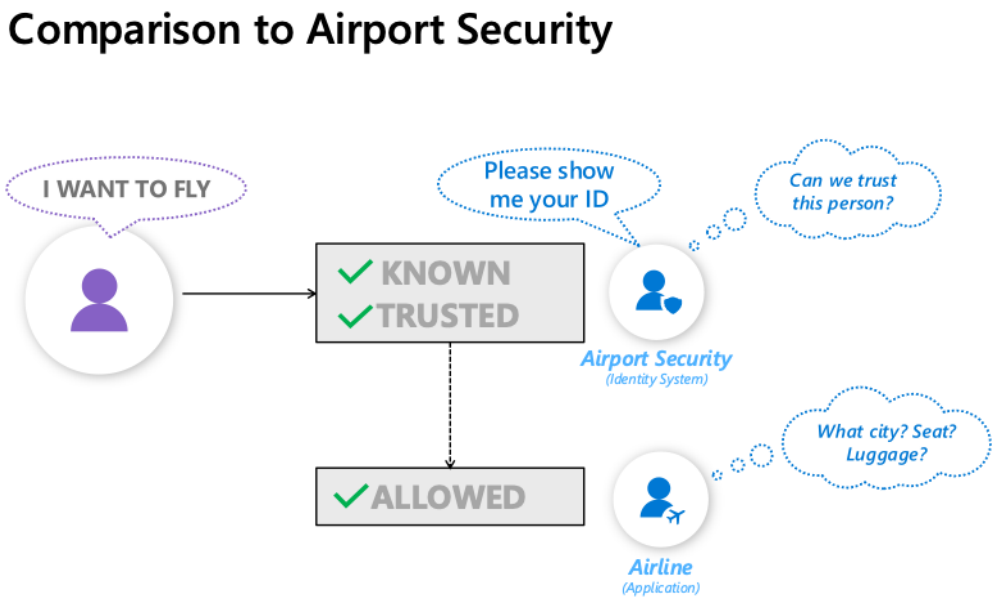

Figure 26: Analogy of Airport Security for Known, Trusted, Allowed

Assets need to be able to support digital identity (supported by the overarching Asset Centricity Capability), as well as entitlements. The authorization capability needs to be able to associate the claims on the asset by a subject granted to it by an authorization provider, which obtains that information from an asset repository. The association and enforcement of claims involves policies, and there needs to be capabilities that define the policies, the enforcement of the policies, where they are stored, and where the policy enforcement decision is taken. An adaptive access control capability will also include the ability to support Agile modification of these assets (the adaptive capability, often in the modern context involving techniques such as Machine Learning (ML)), and the auditability and administration of these assets.

In the Digital Era, the number of participants in the ecosystem, including subjects, assets, and the policies governing the accessing of the assets by the subject, tends to grow exponentially and evolve rapidly. Therefore, the Zero Trust context requires the ability to support the authentication and authorization relationship in an Agile manner to support growing ecosystems.

Adaptive Access Control also provides the ability to protect assets in an Agile manner, factoring in multiple telemetric factors (location, business process, etc.), consumer, provided credentials (and their classes), and resource (data) classification. Thus, this capability involves the creation of comprehensive, rapidly evolving, and agile access control policies that might involve rapid change in subject, asset, or the environment in which these reside, or other business, security, regulatory, or other drivers.

The main drivers behind Adaptive Access Control capabilities are:

- Business requirements

  Organizations adapt to the shifting market conditions with partnerships, mergers, divestitures, and acquisitions, and Adaptive Access Control incorporates any individual business role changes as people move between employee, supplier, competitor, and other roles.

- Automation, reconciliation, verifiable changes, and monitoring and audit of these changes are enabled by Adaptive Access Control

- Technical estate

  The technical estate is in a state of continuous flux in the Digital Era. Organizations are undergoing Digital Transformation, adopting cloud, IOT, and other technologies, incorporating new players in their digital ecosystem (technical estate). Providers must rapidly evolve to support this evolving technical estate. In this environment, for example, assets are rapidly spun up and down on cloud platforms to meet elastic demand, and new development quickly introduces new applications and services. Adaptive access control provides the mechanism to deal with changing relationships.

- Security environment

  Organizations face constant change with new threat actors, new attack techniques, new tools that make sophisticated techniques available to more attackers, and new defensive measures. The ability to make static decisions and include dynamic factors based on evolving threat analysis are supported by adaptive access control.

- Regulatory environment

  Organizations face constantly changing and mandatory requirements, especially as they enter new channels and lines of business. Furthermore, regulations may be rapidly evolving or lagging a changing business environment. Organizations need to be able to change risk levels, and access control policies at a very rapid rate. Adaptive Access Control provides the capability to support this. More sophisticated implementations might use intelligent, AI driven approaches to achieve this.

6.2.3 Digital Identity Capability

Digital Identity provides the ability to have a set of validated digital attributes and credentials for the digital world, like a person's identity for the real world, associated with an asset.

Digital Identity is a key part of the ability to support agility in a Zero Trust Digital Enterprise. This capability allows assets to support portable identity, allowing ZTAs to support the flux that exists in relationships between organizations in the digital ecosystem in a seamless manner, without creating a continuous set of new identities, and thus a continuous set of updates to policies and other aspects of the ZTA.

Digital Identities support more Agile, data-centric establishment of trust, of the portability, and of the interoperability of identity using non-repudiable attributes and credentials. Examples of modern digital identity are the Fast Identity Online (FIDO) standard and the evolution of national sovereign identity.[12] Table 4 lists each Digital Identity capability and which ABBs support it.

[12] Refer to: https://www.oecd-ilibrary.org/sites/2b1a96d6-en/index.html?itemId=/content/component/2b1a96d6-en.

Table 4: Digital Identity Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
DI-1	Digital Identity	1	Digital Identity Platform (ABB DIP-1).
DI-1.1	Identity Definition	2	Digital Identity Definition Engine (ABB DIP-1.1).
DI-1.2	Identity Management	2	Digital Identity Lifecycle Manager (ABB DIP-1.2). Digital Identity Manager (ABB DIP-1.3).
DI-1.3	Identity Access	2	Identity Wrapper (ABB ACP-1.1).
DI-1.3.1	Access Verifiability	3	Digital Identity Manager (ABB DIP-1.3).
DI-1.4	Access Monitoring	2	Digital Identity Manager (ABB DIP-1.3).
DI-1.5	Digital Identity Access Consent	2	Digital Identity Consent Manager (ABB DIP-1.4).
DI-1.6	Digital Identity Access Consent Management (Create, Update, Delete, Monitor)	2	Digital Identity Consent Manager (ABB DIP-1.4).
DI-1.7	Digital Identity Persistence (Long-lived)	2	Digital Identity Repository (ABB DIP-1.1).

The Digital Identity capability includes the following capabilities:

- Digital Identity (DI-1) – Provides the ability to have a set of validated digital attributes and credentials for the digital world, like a person's identity for the real world, associated with an asset

  — Identity definition (DI-1.1)

  Provides the ability to define an identity using attributes that are well-known and accepted, usually by some regulatory authority or industry body. Note that this is complemented by the Digital Identity Binding capability that associates an identified Digital Identity with an asset, using the Identity Definition capability to define the Digital Identity.

  — Identity management (DI-1.2)

  Provides the ability to support the creation, update and deletion of identities.

— Identity access (DI-1.3)

Provides the ability to access identities to owners of the identities, lawfully entitled entities as prescribed by sovereign laws, and other stakeholders as allowed by the owner under the law.

- Access verifiability (DI-1.3.1)

  Provides the ability to verify access to the identity in a non-repudiable and auditable manner.

- Access monitoring (DI-1.4)

  Provides the ability to monitor access to ensure integrity of the identity.

- Digital identity access consent (DI-1.5)

  Provides the ability to support consent for identity access from governing or owning parties following legal controls. Consent for access should be tracked, and auditable.

- Digital identity access consent management (create, update, delete, monitor) (DI-1.6)

  Provides the ability to manage consent records.

- Digital identity persistence (Long-lived) (DI-1.7)

  Provides the ability to retain identity in a secure manner for a long period of time. Identities in the case of people can be life-long, while others can exist for the duration of the life of the system asset. Ensuring durable, long-lived persistence of the ID is one of the requirements for a trusted digital identity capability.

6.2.3.1 Dependent Capabilities Reused by the Digital Identity L1 Capability

All capabilities in the Asset-Centricity Capability may be reused to implement or support the capabilities for Digital Identity.

6.2.4 Asset-Centric Protection Capability

Asset-Centric Protection provides the ability to protect the various kinds of assets, at any time, and at any place, in an environment of assumed breach. Table 5 lists each Asset-Centric Protection capability and which ABBs support it.

Table 5: Asset-Centric Protection Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
ACP-1	Asset-Centric Protection	1	Asset Centric Protection Platform (ABB ACPP-1).
ACP-1.1	Data Centric Protection	2	Data Protection Platform (ABB ACPP-1.2).

Capability Number	Capability	Level	ABB
ACP-1.1.1	Data Classification	3	Data Lifecycle Governance Repository (ABB ACPP-1.1.1.1). Data Lifecycle Governance Engine (ABB ACPP-1.1.1.2).
ACP-1.1.2	Data Lifecycle Capture	3	Data Lifecycle Engine (ABB ACPP-1.1.1).
ACP-1.1.3	Data Discovery	3	Data Lifecycle Governance Engine (ABB ACPP-1.1.1.2). Data Lifecycle Governance Repository (ABB ACPP-1.1.1.1).
ACP-1.1.4	Data Encryption at Rest	3	Data Tokenization Engine (ABB ACPP-1.2.3). Token Vault (ABB ACPP-1.2.2). Data Anonymization Engine (ABB ACPP-1.2.1). Data Encryption Service (ABB ACPP-1.2.4).
ACP-1.1.5	Data Encryption in Transit	3	Data Tokenization Engine (ABB ACPP-1.2.3). Token Vault (ABB ACPP-1.2.2). Data Anonymization Engine (ABB ACPP-1.2.1). Data Encryption Service (ABB ACPP-1.2.4).
ACP-1.1.6	Data Encryption in Use	3	Data Tokenization Engine (ABB ACPP-1.2.3). Token Vault (ABB ACPP-1.2.2). Data Anonymization Engine (ABB ACPP-1.2.1). Data Encryption Service (ABB ACPP-1.2.4).
ACP-1.1.7	Data Provenance	3	Data Lifecycle Engine (ABB ACPP-1.1.1). Lifecycle Governance Repository (ABB ACPP-1.1.1.1) and composed ABBs.

Capability Number	Capability	Level	ABB
ACP-1.1.8	Data Protection by Elimination	3	Data Lifecycle Engine (ABB ACPP-1.1.1) and composed ABBs. Data Discovery (ABB ACP-1.1.3) (reused).
ACP-1.1.9	Data Protection by Tokenization	3	Token Vault (ABB ACPP-1.2.3). Data Tokenization Engine (ABB ACPP-1.2.4).
ACP-1.1.10	Data Protection by Obfuscation (hashing)	3	Data Obfuscation Engine (ABB ACP-1.2.5).
ACP-1.1.11	Data Protection by Anonymization	3	Data Anonymization Engine (ABB ACP-1.2.1).
ACP-1.2	System Asset Centric Protection	2	Asset Availability Protection Platform (ABB ACP-1.3.2).
ACP-1.2.1	System Asset Rate-limiting	3	API Gateway (ABB ACPP-1.3.1.1).
ACP-1.2.3	System Asset access Throttling	3	Asset Availability Protection Platform (ABB ACP-1.3.2). API Gateway (ABB ACP-1.3.2.1).

The Asset-Centric Protection capability includes the following capabilities:

- Asset-Centric Protection (ACP-1) – Provides the ability to protect various kinds of assets, at any time, and at any place, in an environment of assumed breach
  - — Data Centric Protection (ACP-1.1) – Provides the ability to protect data at rest, in transit, and in use, across the lifecycle of the data asset
    - Data classification (ACP-1.1.1) – Provides the ability to classify data assets based on policies that can be derived from regulatory controls, enterprise threat, and risk assessments or a combination of all three

      This risk classification is usually a combination of regulatory controls (such as the definition of Electronic Protected Health Information (ePHI) in HIPAA) as well as a further assignment based on perceived organizational risk determined by the organizational risk team and business stakeholders. Note that “classification” may refer to formal levels of trust or sensitivity of contents (e.g., “Top Secret” or “Classified”) or may be defined by the organization.
    - Data lifecycle capture (ACP-1.1.2) – Provides the ability to capture the lifecycle of data assets

- Data discovery (ACP-1.1.3) – Provides the ability to discover data assets, especially based on their classification across the technical estate
- Data encryption at rest (ACP-1.1.4) – Provides the ability to ensure that data assets are encrypted at rest if required by their classification
- Data encryption in transit (ACP-1.1.5) – Provides the ability to encrypt in transit if the assets are required to do so based on policy controls
- Data encryption in use (ACP-1.1.6) – Provides the ability to encrypt in use if the assets are required to do so based on policy controls

  Examples are format preserving encryption, hardware encryption, and homomorphic encryption.
- Data provenance (ACP-1.1.7) – Provides the ability to ensure traceability and transparency of data use, access, and transformation
- Data protection by elimination (ACP-1.1.8) – Provides the ability to reduce risk to the organization from the breach and theft or access to sensitive data by elimination of the data and replacement with an alternative business process to support the functionality where the data was used
- Data protection by tokenization (ACP-1.1.9) – Provides the ability to replace the data element of high business value with an alternative with lower or no business value to an attacker

  Techniques such as Format Preserving Encryption may be used to support tokenization, with the ability to create different tokens for the same data element. This can be used to separate out the data into different "zone" based on the token, supporting various consumer groupings.
- Data protection by obfuscation (hashing) (ACP-1.1.10) – Provides the ability to replace high value data with a hashed data element that is not reversible back to the original data element
- Data protection by anonymization (ACP-1.1.11) – Provides the ability to replace high value data by anonymizing the data using techniques such as T-Closeness or k-anonymity

— System Asset Centric Protection (ACP-1.2) – Provides the ability to support availability protection of a system asset

- System asset rate-limiting (ACP-1.2.1) – Provides the ability to protect API assets by limiting the access rate from subjects to control denial of service to other consumers
- System asset access throttling (ACP-1.2.3) – Provides the ability to limit the number of requests supported by a particular asset

  For example, this prevents impact on other assets in a shared environment.

6.2.4.1 Dependent Capabilities Reused by the Asset Centric Protection L1 Capability

The Adaptive Access Control capability reuses the Digital Identity Binding (AC-1.1) and other Asset Centricity (AC-1) capabilities to support subject and asset identification, classification, and management. These are required to enable the asset to be identified and availability protected.

Data Classification may be used to both statically and dynamically determine threat protection levels for data assets. Thus, different data classes may be moved into different security zones, and assets be subject to different level of protection based on data classification, intelligent threat monitoring and dynamic risk management.

6.2.4.2 A Deeper Drive into Asset-Centric Protection Concepts

Regardless of the vector used, monetization model, or motivation, most threat actors focus on gaining control of assets in an attack. A ZTA divides the technical estate into data and system assets, and the security professional and the associated team must consider both data assets and system assets in their protection design. Asset-Centric Protection is that capability that addresses both data assets and system assets (these are the assets that manipulate that data), using Security Zones, Adaptive Access Control, and Digital Identity.

Asset Centric Protection can be divided into protection of the two kinds of assets – data and system assets.

- Data-Centric Protection – this capability focuses on the security of the data that matters most to the organization

  Data-centric protection enables identifying and focusing resources and security investment on higher-value assets through their full lifecycle. It also enables identifying which assets increase security risk without creating business value (e.g., extra copies of PII in databases) that may be retired or tokenized. Finally, this capability allows organizations to create flexible data protection architectures that can evolve over time, taking into consideration the entire lifecycle of the data asset. This includes assessing the risk associated with the data element and its use, the regulatory, business, technical, and security implications, and the associated policies that must be created to ensure appropriate protection and posture management. This will include data-flow analysis for data elements.

  Illustratively, for credit card numbers, the lifecycle starts from the time the number is originated and provisioned, through different states (period that it is valid, is suspended, lost, retention for regulatory/compliance purposes), to deprovisioning. Finally, these would lead to a set of policies that determine the data protection regime for credit card numbers and their use for an organization and its digital ecosystem. These policies would be based on organizational risk appetite, regulations (e.g., Payment Card Industry (PCI)), and other controls.

- System-Centric Protection – this capability focuses security on the assets that operate on the data or on underlying business process, and in particular their availability

  This capability uses the following capabilities Asset Centricity, Digital Identity, Adaptive Access Control, Asset Centric Protection, and Security Zones. Core Zero Trust concepts apply – assets are considered in terms of value and secured in Security Zones. As expanded on in the section on Security Zones, this allows protecting assets based on value, to address operational blast radius and compartmentalize risk, and be able to operate in an environment of assumed breach.

This capability provides the ability to protect attacks that threaten the operation on the data in traditional "in-band" processes, as well as the "out of band" scenarios (disrupting network traffic, OT protocols, analog communications, etc.) that are specific to the assets (e.g., the process equivalent of data at rest/in transit).

System-Centric Protection provides the ability to maintain asset availability at any time, in any place, including during an active attack. In the context of Zero Trust, this involves isolating the asset or assets in the event of a breach and compartmentalizing its impact. It also includes the capability to support fencing, throttling, rate-limiting, and other capabilities used to traditionally protect the asset in the event of an attack on availability (such as a Distributed Denial of Service (DDoS) attack).

Note that:

- The security responsibility for availability is focused on the intentional disruption of services, whereas standard IT and other processes handle scenarios from natural causes, human error, equipment failures, etc.

  The remediation and scenarios may overlap between these two, but this is where Zero Trust security focuses.

- Zero Trust is focused on all types of attack scenarios (account takeover, data corruption, app deletion/corruption, etc.), not just network-driven scenarios

6.2.5 Asset-Centric Security Operations Capability

Asset-Centric Security Operations provide the ability to pro-actively detect, respond, and recover from threats in an asset-centric, Zero Trust manner.

ZTAs require the ability to mitigate realized risk by limiting the time that adversaries have access to business assets (attacker "dwell time") with security operations. This is a natural corollary of assuming compromise – the threat actors are assumed to gain access to assets, so the operational security capabilities must be built to rapidly evict them. Table 6 lists each Asset Centric Security Operations capability and which ABBs support it.

Table 6: Asset-Centric Security Operations Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
ACSO-1	Asset-Centric Security Operations	1	Asset-Centric Security Operations Platform (ABB ACSOP-1).
ACSO-1.1	Rapid Incident Response	2	Asset-Centric Security Operations Platform (ABB ACSOP-1).
ACSO-1.2	Incident Management	2	Case Management (ABB ACSOP-1.2).
ACSO-1.2.1	Case Management	3	Case Management (ABB ACSOP-1.2).

Capability Number	Capability	Level	ABB
ACSO-1.2.2	Major Incident Management	3	Major Incident Management (ABB ACSOP-1.3).
ACSO-1.3	SecOps Business Intelligence	2	SecOps Business Intelligence Platform (ABB ACSOP-1.5).
ACSO-1.4	Threat Hunting and Detection Tuning	2	Threat Hunting (ABB ACSOP-1.6).
ACSO-1.4.1	Threat Hunting	3	Threat Hunting (ABB ACSOP-1.6).
ACSO-1.4.2	Detection Tuning	3	Detection Tuning (ABB ACSOP-1.10).
ACSO-1.4.3	Purple Teaming	3	Purple Teaming (ABB ACSOP-1.10.1).
ACSO-1.4.3.1	Red Teaming	4	Red Teaming (ABB ACSOP-1.10.1.1).
ACSO-1.5	Threat Intelligence	2	Threat Intelligence Platform (ABB ACSOP-1.11).
ACSO-1.6	Asset-type specific attack detection	2	Extended Detection and Response (XDR) (ABB ACSOP-1.1).
ACSO-1.7	Security Information and Event Management (SIEM)	2	SIEM (ABB ACSOP-1.7).
ACSO-1.7.1	Security Data Lake Capability	3	Security Data Lake (ABB ACSOP-1.7.1).
ACSO-1.8	SOAR	2	SOAR (ABB ACSOP-1.4).
ACSO-1.9	Advanced Security Analytics	2	Intelligent Anomaly Detection (ABB ACSOP-1.8). Intelligent Behavior Analytics (ABB ACSOP-1.9).
ACSO-1.10	Integrated Threat Intelligence Feeds	2	XDR (ABB ACSOP-1.1). SIEM (ABB ACSOP-1.7).
ACSO-1.11	SecOps Custom Development	2	SecOps Custom Development Tools (ABB ACSOP-1.12).

The Asset Centric Security Operations capability includes the following capabilities:

- Asset-Centric Security Operations (ACSO-1) – Provides the ability to rapidly reduce risk to the organization by reducing how much time attackers have access to business assets (e.g., attacker dwell time)
  - — Rapid Incident Response (ACSO-1.1) – Provides rapid incident response across the lifecycle of detecting threats, investigate incidents, remove adversary access, and coordinating with asset owners to recover full functionality of any damaged assets
  - — Incident Management (ACSO-1.2) – Provides the ability to effectively manage and coordinate the lifecycle of a security incident
    - Case management (ACSO-1.2.1) – Provides the ability to manage and track current security incidents and search/correlate historical incidents
    - Major incident management (ACSO-1.2.2) – Provides the ability to manage and coordinate activities related to a major incident across technical teams, legal teams, organizational leaders, and other stakeholders

      A major incident is an attack that can inflict significant damage on the organization's assets and operations, up to and including material damage. Major incidents are typically triggered when an attacker has gained access to administrative privileges to multiple or all business critical systems.
  - — SecOps Business Intelligence (ACSO-1.3) – Provides insights on the business workflows of the SOC to monitor process status and health and enable prioritization of work for continuous improvement
  - — Threat Hunting and Detection Tuning (ACSO-1.4) – Provides the ability to continuously improve detection of attackers accessing to the organization's assets (attempted and successful)
    - Threat hunting (ACSO-1.4.1) – Provides the ability to identify attackers who have previously gained access to the organization without being detected
    - Detection tuning (ACSO-1.4.2) – Provides the ability to continuously improve detection of attacker access to the organization's assets
    - Purple teaming (ACSO-1.4.3) – Provides the ability to rapidly improve the knowledge and defenses of the organization with joint activities including both red teams (simulated attackers) and blue teams (defenders)
      - Red teaming (ACSO-1.4.3.1) – Provides the ability to simulate persistent attackers to find weaknesses in the organization's detections and preventive controls

        Note: It is critical that this function's goal is based on the improvement of the organization's defenses (*via* purple teaming or other interactions with defenders) and not "successfully attacking" the organization.

— Threat Intelligence (ACSO-1.5) – Provides security insights to security operations functions, other security and IT functions, and other organizational functions

This includes analysis and insights for current and past attacks on the organization, attacks on other external organizations, and other security insights and context from external organizations and sources.

— Asset-Type Specific Attack Detection (ACSO-1.6) – Provides the ability to detect and respond to attacks on assets quickly and efficiently with asset type-specific insights on threats, technical behavior detection, normal baseline behavior and anomalies

— SIEM Capability (ACSO-1.7) – Provides the ability to correlate and analyze events, alerts, and other data across any source in the organization to inform detections, investigations, threat hunting, remediations, and other security operations functions

- Security Data Lake Capability (ACSO-1.7.1) – Provides the ability to store and query a large amount of security operations data for an extended period

  This provides a complete record for compliance purposes as well as historical records for various security operations functions including threat hunting, threat intelligence, and others.

— SOAR Capability (ACSO-1.8) – Provides the ability to automate manual tasks and orchestrate actions across multiple systems to reduce human error and increase speed of response, hunting, and other security operations functions

— Advanced Security Analytics (ACSO-1.9) - Provides the ability to parse large volumes of data using ML and identify anomalies using behavioral analytics

— Integrated Threat Intelligence Feeds (ACSO-1.10) – Provides the ability to provide context on attacks and learnings from other organizations to security operations functions by integrating it automatically into technical capabilities

— SecOps Custom Development (ACSO-1.11) – Provides the ability to create custom tools to enhance and automate investigation, hunting, integration and other SecOps functions as well as integrate SecOps tools with other tools for DevOps, Asset Repository (ACP-1.2), and others

6.2.5.1 Dependent Capabilities reused by the Asset-Centric Security Operations L1 Capability

The Asset-Centric Security Operations Capability reuses the following L1 capabilities: Asset Centricity, Asset-Centric Protection, Security Zones, and Posture Management. It is assumed that some or all of the underlying L2 or lower capabilities of these L1 capabilities may be reused.

6.2.5.2 A Deeper Dive into Asset-Centric Security Operations Capability Concepts

Asset-Centric Security Operations differ from classic security operations in the following ways:

- Asset-type specific tooling is designed to provide high quality alerts and investigation experience, as well as proactive hunting capabilities reduces the number of false positive alerts that cause analyst fatigue, improving overall security operations efficiency

  This takes the form of EDR or XDR (ACSOP-1.1) tooling that gathers asset-specific insights (e.g., memory and process trees from endpoints). This is often used in conjunction with a SIEM) (ACSOP-1.7) tool and shifts some scenarios from the SIEM.

- A SOAR Capability (ACSO-1.8) enables automating the response process

  This further increases SecOps efficiency and reduces fatigue and burnout of human analysts. SOAR implementations (SOAR ABBs (ACSOP-1.4)) can take the form of fully automated processes (often vendor provided) and orchestration capabilities that allow automate of response processes and tasks across multiple SecOps tools. To keep up with changes in threats and platforms, SOAR capabilities must be continuously refined and updated.

- Advanced analytics allow identifying anomalies in the collected data and analyzing which anomalies are likely to be attacks

  This includes ML and behavioral analytics that help identify attacks that may otherwise be overlooked (false negative detections) and help avoid human analysts from being wasted chasing false alarms (false positive detections).

- Proactive functions include threat hunting and red/purple teams

  In addition to reactive processes to respond to incidents, SecOps must also proactively assume that attackers have evaded standard detections and hunt for them. To grow maturity of these functions and team skills, SecOps must spar with simulated attackers (red teams) and collaborate with them for mutual learning and growth (purple teams).

- Managing increasing complexity and speed allows Asset-Centric Security Operations Platforms to focus on reducing complexity for the human investigators as complexity continues to increase

  Analysts must contain the blast radius for any given attack as attackers grow in sophistication, technology platforms continuously change, and business critical asset definitions evolve. These operations must continuously adapt to these changes and integrate threat intelligence in near real-time as it comes in.

6.2.6 Posture Management Capability

Posture Management provides the ability to monitor and improve the security posture (security status) of the organization.

Security posture refers to an organization's overall cybersecurity strength and how well it can predict, prevent, and respond to ever-changing cyber threats.

This capability is critical to ensure that the organization understands and is actively reducing potential risk to the organization.

This concept has been understood for some time: NIST 800-128 defines security posture as "the security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. Synonymous with security status".

Zero Trust requires a dedicated posture management capability because the concept of a "safe network" is explicitly invalidated, so this cannot be used as a compensating control instead of managing security posture across assets. Zero Trust also updates posture management to provide on-demand assessment of security posture across all asset types (*versus* a traditional focus on network and operating system posture) as depicted in Figure 27.

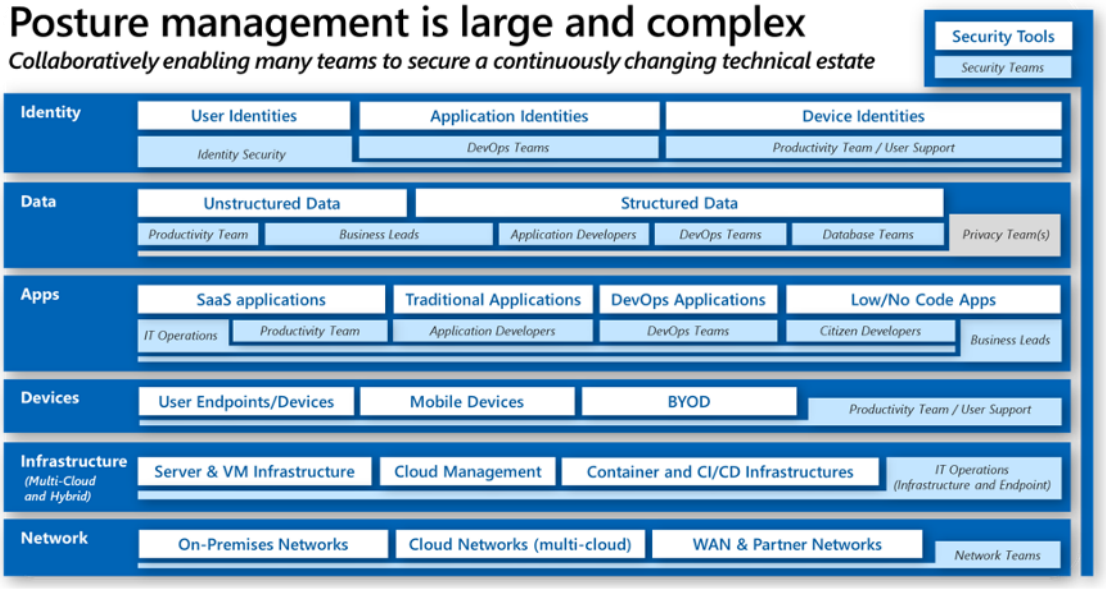

Figure 27: Posture Management Scope

Zero Trust posture management also focuses on continuously updating posture definition and prioritization of controls as threats, security capabilities, platforms/services, and business priorities change.

Zero Trust Posture management explicitly expands the definition of what constitutes a vulnerability from a functional flaw in software design or implementation into any type of function, configuration, or operational vulnerability that allows an attacker to obtain or increase access to the organization's assets. These different types of vulnerabilities are depicted in Figure 28.

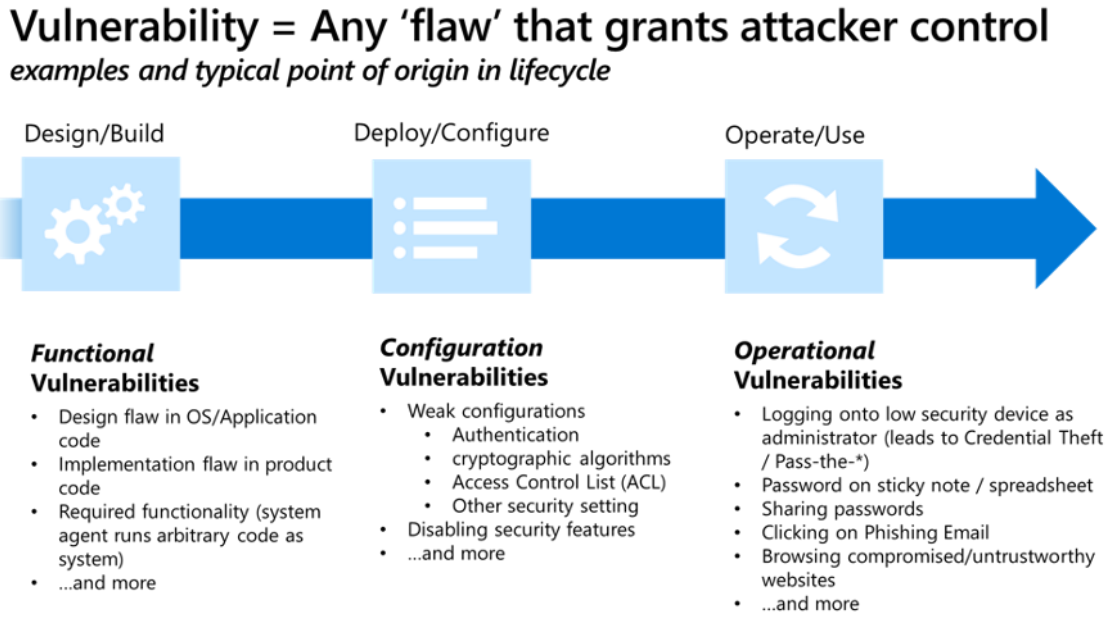

Figure 28: Different Types of Vulnerabilities that can Grant Attacker Control of Assets

Vulnerability Management Capabilities are covered under the Asset Centricity Capability: Asset Vulnerability Management (AC-1.3.6), including Vulnerability Monitoring (AC-1.3.6.1), Vulnerability Remediation (AC-1.3.6.2) and Vulnerability Prevention (AC-1.3.6.3).

Posture management is an operational function focused on identify/prevent operations and complements traditional SOC functions that focus primarily on detect/respond/recover operations. Posture management typically evolves from traditional vulnerability management, growing from monitoring and reporting software vulnerabilities (often only operating systems) into a full-fledged operational function. It works as the supporting function to enable the asset integrity protection capability. Table 7 lists each Security Posture Management capability and which ABBs support it.

Table 7: Security Posture Management Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
SPM-1	Security Posture Management	1	Security Posture Management Platform (ABB SPMP-1).
SPM-1.1	Continuous Assessment of Posture	2	Continuous Security Posture Management Platform (ABB SPMP-1.1).
SPM-1.1.1	Continuous Monitoring	3	Continuous Security Posture Management Platform (ABB SPMP-1.1).
SPM-1.2	Prioritization of Weaknesses and Vulnerabilities	2	No ABB required.
SPM-1.2.1	Threat Intelligence Integration	3	Threat Intelligence Platform (ABB ACSOP-1.11).
SPM-1.2.2	Business Intelligence Integration	3	No ABB required.
SPM-1.3	Rapid Remediation of Vulnerabilities	2	Asset-Centricity Platform (ABB ACP-1).
SPM-1.4	Continuous Improvement of Process and Technology	2	No ABB required.

Capability Number	Capability	Level	ABB
SPM-1.5	Threat and Vulnerability Management (TVM)	2	Internal Vulnerability Scanning Tool (ABB SPMP-1.1.1). Continuous Vulnerability scanner (ABB ACP-1.17). Vulnerability Remediation Process (ABB ACP-1.18). Vulnerability Prevention Process (ABB ACP-1.19).
SPM-1.6	Security Posture Management	2	Continuous Security Posture Management Platform (ABB SPMP-1.1).
SPM-1.7	EASM	2	External Attack Surface Management Tool (outside-in scanning) (ABB SPMP-1.1.2). Monitoring of Application/API posture (ABB SPMP-1.1.3).
SPM-1.7.1	Application and API Security Validation	3	Application penetration testing (ABB SPMP-1.1.2).
SPM-1.8	Asset Posture Management Expertise	2	No ABB required.
SPM-1.9	Asset Posture Management Advocacy	2	Continuous Security Posture Management Platform (ABB SPMP-1.1).
SPM-1.10	Intelligent Posture Management	2	No ABB required.

The Security Posture Management capability includes the following capabilities:

- Security Posture Management (SPM-1) – Provides the to monitor and improve the security posture (security status) of the organization
  - — Continuous Assessment of Posture (SPM-1.1) – Provides the ability to assess the security posture of the organization to inform organizational risk assessments and decisions
    - Continuous Monitoring (SPM-1.1.1) – Provides the ability to support continuous monitoring across the technical estate

      Data-centric protection reduces complexity which can help calibrate what is monitored and to what extent.

— Prioritization of Weaknesses and Vulnerabilities (SPM-1.2) – Provides the ability to prioritize which vulnerabilities to mitigate first so that security, IT, and other resources are allocated to the most important tasks first. This helps avoid resources being wasted on lower priority tasks while leaving organizational risk elevated

  - Threat intelligence integration (SPM-1.2.1) – Provides the ability to inform the prioritization based on threat context such as which vulnerabilities and vulnerability types are being actively exploited the most and having the most impact on other organizations
  - Business intelligence integration (SPM-1.2.2) – Provides the ability to inform the prioritization on which assets are most critical to the business (e.g., they are business critical data and systems or support/host them)

— Rapid Remediation of Vulnerabilities (SPM-1.3) – Provides the ability to rapidly apply asset-centric protections (AC 1.3, ACP-1) in response to discovered vulnerabilities

— Continuous Improvement of Process and Technology (SPM-1.4) – Provides the ability to reduce risk by avoiding future iterations of vulnerabilities or quickly resolving them with changes to processes and technology

— TVM (SPM-1.5) – Provides the ability to scan assets for software vulnerabilities and integrate those insights into various security functions including governance, compliance, security operations, and others

  This helps discover and prioritize vulnerabilities (sometimes using threat intelligence) to mitigate and informs prioritization of security operations incident investigations. This reuses the Asset Centricity capabilities of vulnerability management: Asset Vulnerability Management (AC-1.3.6) including Vulnerability Monitoring (AC-1.3.6.1), Vulnerability Remediation (AC-1.3.6.2), Vulnerability Prevention (AC-1.3.6.3).

— Security Posture Management (SPM-1.6) – Provides the ability to gain an inside-in perspective on asset security posture

  This helps provide a view across many assets in the technical estate to help discover and prioritize vulnerabilities to mitigate.

— EASM (SPM-1.7) – Provides the ability to gain an outside-in perspective on asset security posture

  This mimics what an attacker sees from the outside of the organization to help discover and prioritize vulnerabilities to mitigate.

— Asset Posture Management Expertise (SPM-1.8) – Provides the ability to enables asset managers in IT Operations, DevOps, and others to effectively apply security controls

  This helps address asset-specific security issues by providing security expertise, education, tooling, and other support to these teams who often lack native security experience and skills.

— Asset Posture Management Advocacy (SPM-1.9) – Provides the ability to help in the establishment and implementation of security controls while understanding the posture management challenges

It also enables architects, leaders, auditors, policy authors, and regulators, to advocate for the establishment of security controls and balance delivery and uptime goals with the enterprise security posture.

— Intelligent Posture Management (SPM-1.10) – Provides the ability to ensure that enterprise posture management standards are maintained at an appropriate level, incorporating regulatory controls, organization risk and threat assessment, and the associated asset-driven posture

This partnership is especially important in the Digital Era, where security threats often evolve much faster than regulatory requirements (often in hours/days *versus* multiple years for regulations).

6.2.6.1 Dependent Capabilities Reused by the Posture Management L1 Capability

The Posture Management capability reuses the following L1 Capabilities: Asset Centricity, Asset Centric Protection, and Security Zones. It is assumed that some or all of the underlying L2 or lower capabilities of these L1 capabilities may be reused.

6.2.7 Zero Trust Governance Capability

Zero Trust Governance in the Digital Era provides the ability to establish decision rights, audit and compliance, and guardrails in implementation.

Governance also includes the goals, principles, policies that constitute these guardrails and the education and training required to make this actionable. Table 8 lists each Zero Trust Governance capability and which ABBs support it.

Table 8: Zero Trust Governance Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
ZTG-1	Zero Trust Governance	1	Zero Trust Governance Platform (ABB ZTGP-1).
ZTG-1.1	Audit on Demand	2	Audit on Demand Engine (ABB ZTGP-1.1).
ZTG-1.2	Privacy by Design	2	Privacy by Design Engine (ABB ZTGP-1.3).
ZTG-1.3	Asset Protection Governance	2	Asset Protection Governance Manager (ABB ZTGP-1.4). Posture Management Governance Manager (ABB ZTGP-1.5).
ZTG-1.4	Zero Trust Organizational Structure	2	Zero Trust Organizational Structure (ABB ZTGP-1.6).

Capability Number	Capability	Level	ABB
ZTG-1.5	Zero Trust Organizational Processes	2	Zero Trust Organizational Process Manager (ABB ZTGP-1.7).
ZTG-1.6	Zero Trust Continuous Learning	2	Zero Trust Continuous Learning Platform (ABB ZTGP-1.8).
ZTG-1.7	Zero Trust Strategic Governance	2	Zero Trust Strategic Governance Manager (ABB ZTGP-1.10).
ZTG-1.8	Innovation Security for Professional Development	2	Security Enablement for Professional Development (ABB ZTGP-1.11).
ZTG-1.9	Innovation Security for Citizen Development	2	Security Enablement for Citizen Development (ABB ZTGP-1.12).

The Zero Trust Governance capability includes the following capabilities:

- Zero Trust Governance (ZTG-1) – Provides the ability to drive consistent security outcomes by establishing and enforcing decision rights, audit and compliance, and implementation guardrails

  — Audit on Demand (ZTG-1.1) – Provides the ability to generate audit reports and data on demand to meet the compliance requirements in which a Digital Enterprise operates

  As a key Zero Trust capability in the Zero Trust context, this enables an organization to reduce the friction that compliance often causes, and in doing so, enables business agility. This reuses the SPM-1.1.1 Continuous Monitoring L3 Capability.

  - Audit reporting capability (ZTG-1.1.1) – Provides the ability to support compliance reports (leveraging the Audit on Demand Capability) and security baseline reports (an organizational security standard to support security controls based on regulatory and other controls)
  - Compliance requirement alignment capability (ZTG-1.1.2) – Provides the ability to assess the technical estate to compliance requirements

    This supports the ability to conduct continuous audits and provide a dynamic view on the organization's compliance controls status.
  - Regulatory rules compliance rules capability (ZTG-1.1.3) – Provides the ability to assess and associate compliance rules and develop associated reports

— Privacy by Design (ZTG-1.2) – Provides the ability to provide processes, solutions, and patterns to enable the organization to consistently meet privacy requirements across various workloads and business capabilities

This reuses the ACP-1.1.1 Data Classification Capability in order to determine privacy.

— Asset Protection Governance (ZTG-1.3) – Provides the ability to use the over-arching goals, principles, and policies, coupled with regulatory, security, technical, and business controls to define the actual policies used to govern asset protection

— Zero Trust Organizational Structure (ZTG-1.4) – Provides the ability to enable organizational structural units and changes to existing structures to support the Zero Trust capabilities

Illustratively, data-centric asset protections involve the closer engagement between data/information architecture and the information security organization to ensure data governance includes information security aspects

— Zero Trust Organizational Processes (ZTG-1.5) – Provides the ability to establish new processes or update existing ones to ensure the implementation of Zero Trust Governance

— Zero Trust Continuous Learning (ZTG-1.6) – Provides the ability to incorporate new and evolving techniques such as gamification, new communication protocols, and credential-oriented learning to establish a continuous learning culture

— Zero Trust Strategic Governance (ZTG-1.7) – Provides the ability to plan information security strategy around Zero Trust Commandments

It involves a "whole of organization" security architecture approach and monitoring threats that have manifested, as well as threats that might occur, based on the organization's business operations, risk, compliance, and technical estate.

In keeping with Zero Trust Commandments, this approach will pursue the establishment of roadmaps and capabilities that address these strategic needs in an asset-centric manner, with the assumption of assumed breach and reduced blast radius. Finally, the Zero Trust Commandments shall be used as guardrails to help drive this vision.

— Innovation Security for Professional Development (ZTG-1.8) – Provides the ability for professional developers to integrate security practices into the development of applications

— Innovation Security for Citizen Development (ZTG-1.9) – Provides the ability for citizen developers to integrate security practices into the development of low-code and no-code applications

6.2.7.1 *Dependent Capabilities Reused by the Zero Trust Governance L1 Capability*

The Zero Trust Governance Capability reuses the Continuous Monitoring (SPM-1.1.1), Asset Centricity (AC-1), and Data Classification (ACP-1.1.1) Capabilities.

6.2.8 Security Zones Capability

Security Zones provide the ability to group assets together that have similar business value or security requirements.

Security Zones define secured parts of the technical estate based on various factors. They are distinguished by:

- Protection of sets of assets of a particular business value, up to a granularity of one (network-of-one)
- Control of the direction of the data flow (ingress/egress/routing)
- Protection of the data flowing through each zone
- Data-centric protection of the data flowing through each zone (e.g., tokenization, data obfuscation by one-way hashing, data elimination)
- Control of access to the zone by applying least privilege and restricting the access to a limited set of accounts, allowing zones to be architected as required by use case; the access controls for this may include network, identity, application, data, and other types of access controls
- Control of access by adaptive access control, allowing for multiple policies to be applied to the access to the endpoints or zones
- Monitoring of the flow and access of data, both in real-time and through trending

Security zones simplify security design, build, and operation by providing the same or similar security controls to this grouping of assets. Table 9 lists each Security Zones capability and which ABBs support it.

Table 9: Security Zones Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
SZ-1	Security Zones	1	Security Zones Platform (ABB SZP-1).
SZ-1.1	Asset Grouping and Protection	2	Identity, Endpoint, and Application based Security zone controls (ABB SZP-1.1). Data-Centric Security zone controls (ABB SZP-1.2). Network-Centric Security zone controls (ABB SZP-1.3). SecOps based zone controls (ABB SZP-1.4).

Capability Number	Capability	Level	ABB
SZ-1.2	Data Flow Direction Control	2	Identity, Endpoint, and Application based Security zone controls (ABB SZP-1.1). Data-Centric Security zone controls (ABB SZP-1.2). SecOps based zone controls (ABB SZP-1.4).
SZ-1.3	Limited Access	2	Identity, Endpoint, and Application based Security zone controls (ABB SZP-1.1). Data-Centric Security zone controls (ABB SZP-1.2). Network-Centric Security zone controls (ABB SZP-1.3).
SZ-1.4	Monitoring of Data Flow	2	Identity, Endpoint, and Application based Security zone controls (ABB SZP-1.1). Data-Centric Security zone controls (ABB SZP-1.2). SecOps based zone controls (ABB SZP-1.4).
SZ-1.5	Data Protection at Rest, Use, and in Transit Across a Security Zone	2	Identity, Endpoint, and Application based Security zone controls (ABB SZP-1.1). Data-Centric Security zone controls (ABB SZP-1.2).
SZ-1.6	Data Centric Protection of Data	2	Data-Centric Security zone controls (ABB SZP-1.2).

The Security Zones Protection capability includes the following capabilities:

- Security Zones (SZ-1) – Provides the ability to protect assets efficiently by grouping them together and applying common controls
  - — Asset Grouping and Protection (SZ-1.1) – Provides the ability to group assets together with similar business value or security requirements to provide consistent protections with less effort
  - — Data Flow Direction Control (SZ-1.2) – Provides the ability to control the flow of data within a security zone
  - — Limited Access (SZ-1.3) – Provides the ability to restrict and monitor access to a security zone to specific groupings of subjects (accounts) based on the principle of least privilege

— Monitoring of Data Flow (SZ-1.4) – Provides the ability to monitor data flow across the security zone for attack vectors based on data flow, both in real-time and through trend-analysis, based on the business value of the assets

— Data Protection at Rest, Use, and in Transit Across a Security Zone (SZ-1.5) – Provides the ability to support consistent protection of assets within a zone, so that all instances of that assets within the zone have the same level of data-centric protection, based on the business value of the assets

Examples can be elimination of a data-element within a zone or the use of tokenization using different key to have different tokens for different zones. This is a dependent capability, reusing the L2 Data-Centric protection capability from the overall L1 Asset-Centric Protection capability.

— Data Centric Protection of Data (SZ-1.6) – Provides the ability to protect data within a security zone based on data-centric approaches such as tokenization (where each zone might have different keys), obfuscation using one-way hash, data elimination, etc. This is a dependent capability, reusing the Data Centric capability from Asset-Centric Protection

6.2.8.1 Dependent Capabilities Reused by the Security Zones L1 Capability

- Security Zones reuses all the capabilities of Asset Centricity

  Protecting assets requires being able to identify and protect them.

- Security Zones reuses all the capabilities of Adaptive Access Control

  Protecting security zones requires being able to protect access based on various attributes.

- Security Zones reuses all the capabilities of Asset-Centric Protection

  — Example 1 – based on the particular security zone that the system asset is located in, the security posture can evolve with new levels of asset-centric protection

  — Example 2 – data classification schemes are critical to determining how to group the data in a particular security zone

  Based on the organization's security posture, how different classes of data protected at different stages in their lifecycle, and at different locations, etc., can be determined, and data encryption schemes applied.

Note: In Table 9, the L2 capabilities associated with the L1 capabilities are assumed to be included.

6.2.8.2 A Deeper Dive into Security Zones Capability Concepts

Note that the overall security partitioning in ZTAs can be considered to be a combination of security zones as defined, division of data based on tokenization, and the setup of secure segments based on the access controls implemented by using adaptive access control.

Zero Trust security sones incorporate support for key Zero Trust capabilities and characteristics. Thus, data-centricity can drive the development of data-centric zones, using, for example, different keys for different token "zones", forming one kind of security zone. This may be seen in the financial sector. These are network agnostic and allow organizations to reduce blast radius and increase agility.

There is also the concept of "network of one", which effectively treats each asset as its own "micro" network and allows for identity, access privileges, policy decisions, and enforcement to all occur at the level of the individual asset. This supports the Zero Trust attributes of agility and adaptability.

Illustratively, these "security zones" or "micro-segments" (networks-of-one) can be grouped into Security Zones, with traditional concepts of network segmentation, tiering, etc. (e.g., segmenting, using firewalls, the application, and data tier). Alternatively, as in the case of container orchestration and container architectures in cloud and virtualized platforms, they can be grouped into "pods" or microsegments fronted by "API Gateways" or "Service Meshes," with each "pod" being its own security zone. In OT environments, identity wrappers along with security zones can allow for "compartmentalizing" and protecting both analog and digital assets. In cloud architectures they may be managed through security groups and configurations limited by the cloud provider. Finally, these can be combined with the data-centric approaches to create new security zone models.

This capability supports blast-radius reduction, as well as complexity reduction and operational delivery management. Modern concepts such as "Infrastructure as Code" can be used to maintain and manage modern security zones, and provide both visibility, auditability, governance, and runtime operational support for modern assets.

For example, in the context of hybrid cloud environments, this is usually a combination of network/API gateway definitions, as well as access control and routing configurations driven by the platform architecture, coupled with data-centric controls. In a hybrid cloud environment, an environment may be setup using account controls and router and API gateway configurations to control the routing of data, while based on business drivers, a data tokenization environment splitting data into different token groups based on multiple factors can be set up. The first one forms the basis for data routing, while the second one forms the basis for data sharing. The first one uses adaptive access control to provide agility, allowing organizations to add and remove system assets and configure the relations between them, while the second one uses data tokenization to share data across different stakeholders such as internal APIs/capabilities, or to clients, partners, or vendors.

6.2.9 Control Management Capability

The Control Management capability provides the ability to establish and document an overall organizational framework of regulatory and security controls[13] (sometimes called "risk" controls) and then utilize it to ensure organizations meet compliance and information security requirements based on regulatory and business risk value estimation. This also allows the organization to confirm whether the controls currently in place are adequate for new and emerging threats, the answer to which is informed by enterprise risk estimation. Table 10 lists each Controls Management capability and which ABBs support it.

Table 10: Controls Management Capabilities and Supporting ABBs

Capability Number	Capability	Level	ABB
CM-1	Controls Management	1	Control Management Platform (ABB CMP-1).

[13] This standard does not identify or recommend a security control framework; the organization may choose to create its own or to utilize an existing security control framework and make adaptions as required.

Capability Number	Capability	Level	ABB
CM-1.1	Control Classification	2	Controls Repository (ABB CMP-1.1).
CM-1.2	Control Maintenance	2	Controls Manager (ABB CMP-1.2). Controls Engine (ABB CMP-1.3). Controls Integration Services (CMP-1.4).
CM-1.3	Control Audit	2	Controls Reporting Manager (CMP-1.5).

The Control Management capability includes the following capabilities:

- Control Management (CM-1) – Provides the ability to establish a regime of controls to help manage risk for the technical estate based on the security posture and threat posture of the organization
  - — Control Classification (CM-1.1) – Provides the ability to identify and describe risks and ensure alignment with any legal regulations that might exist
  - — Control Maintenance (CM-1.2) – Provides the ability to add, delete, and update controls in a verifiable and auditable manner
  - — Control Audit (CM-1.3) – Provides the ability to expose controls for compliance and audit purposes

6.2.9.1 Dependent Capabilities Reused by the Control Management L1 Capability

The Control Management capability reuses all the capabilities of Asset Centricity.

6.3 Architectural Building Block View

ABBs are logical components that implement a capability. In practice, there may be one or more ABBs realizing a particular capability; one ABB may use or implement more than one capability (i.e., ABBs and capabilities have a many-to-many relationship). Just like capabilities, some ABBs maybe reuse or compose other ABBs. Finally, as capabilities are reused; similarly, the ABBs implementing them may be reused in implementing the ABB for another capability. For example, the Asset Repository ABB belongs or is owned by the Asset Centric L1 capability, but as some of the Asset-Centric capabilities L2 capabilities such as Digital Identity Binding are reused in realizing other capabilities (for example, the Adaptive Asset Control), their associated ABBs are reused.

The Zero Trust Technology Reference Model applies these cross-cutting ABBs (security in general is a cross-cutting concern) across IT, OT, and IoT environments in an organization’s technical estate (which is comprised of all technical components in the organization).

These ABBs represent the architectural components that support the key capabilities associated with a Zero Trust reference architecture. They also often correlate directly to the security disciplines within a security program using a Zero Trust strategy. Discrete Zero Trust security modernization initiatives also often focus on modernizing all (or part of) an ABB.

Note: In the case of all ABBs in this document, the L2 and lower-level ABBs are subject to evolution and change in subsequent versions of this document. Sections to be provided in the next Snapshot version will also make the ABBs more tangible. In particular, each lower-level ABB will be associated with scenarios, and standards for its implementation (e.g., TLS-1.xx for the implementation of security for data in transit) will be defined.

The ABBs are arranged in two groups – those used for designing and building Zero Trust solution architectures, and those for running and operating Zero Trust solution architectures. In some cases, such as Posture Management, there may be ABBs for both the Design/Build group and the Run/Operate group. These ABBs are different and address different capabilities.

6.4 Zero Trust ABBs

This sub-section presents a high-level overview of core Zero Trust ABBs (building on existing ABBs where relevant). Note that these ABBs might not be unique to Zero Trust. However, they are required elements used to compose and establish a ZTA.

These ABBs support the Zero Trust components depicted in Figure 29.

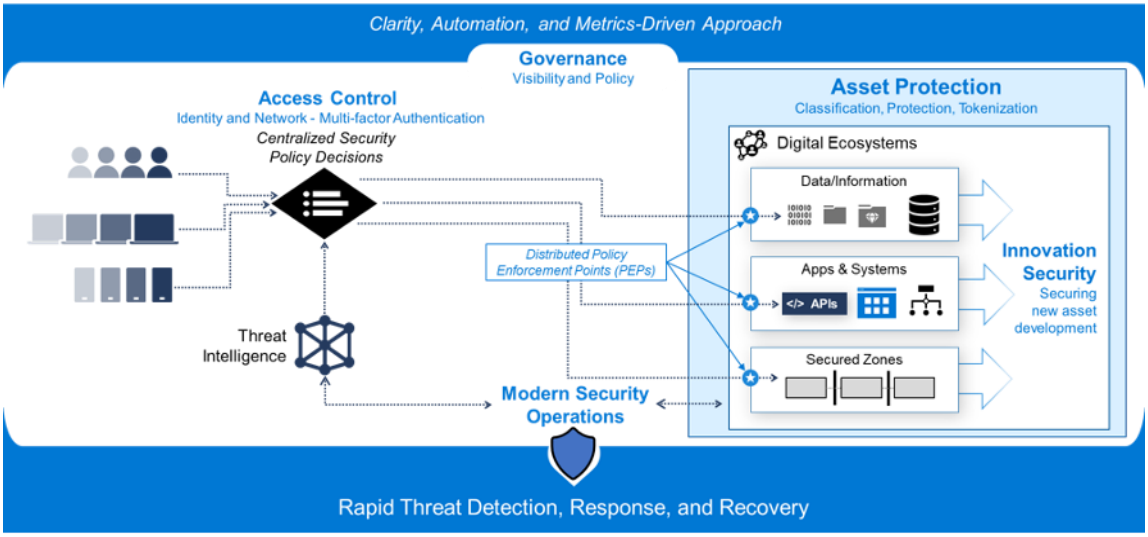

Figure 29: The Zero Trust Technology Reference Model - Design/Build View

As the ABBs are realized into SBBs and functional components (and sometimes teams) within the organization, they will need to interact with each other, with other teams and functions, with all the various assets in the technical estate, and with key stakeholders in IT Operations, DevOps Teams, citizen developers, and other people within the organization. These core ABB categories are depicted in Figure 30.

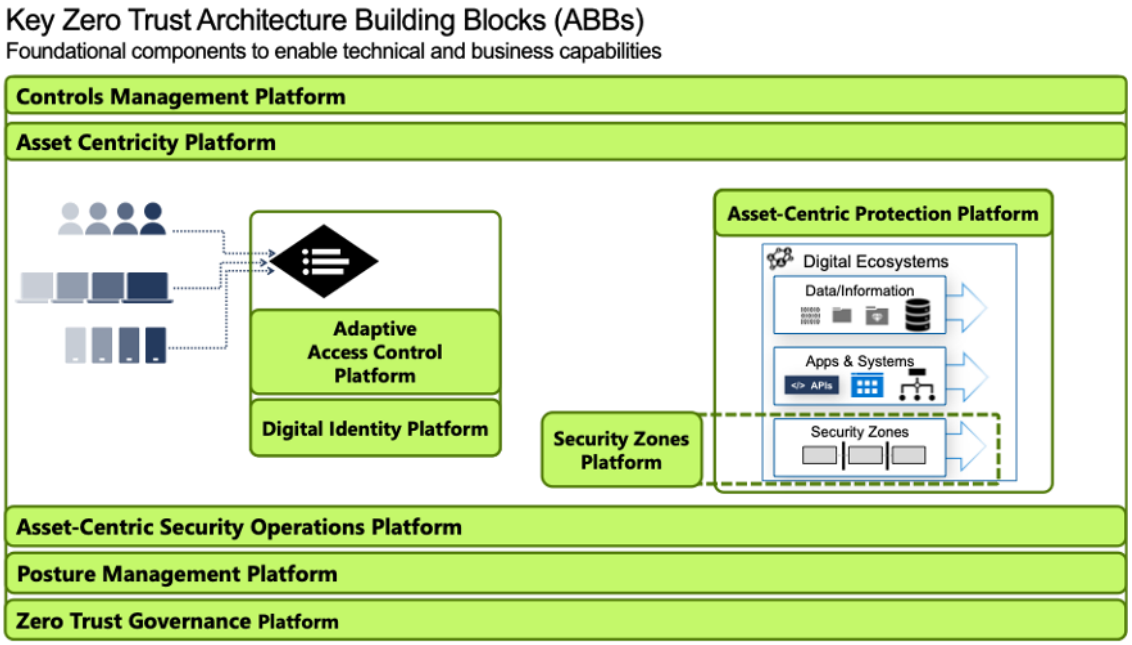

Figure 30: The Zero Trust ABBs

Figure 31 provides a high-level overview of these relationships and common interactions in an operational Zero Trust environment as supported by ABBs and SBBs:

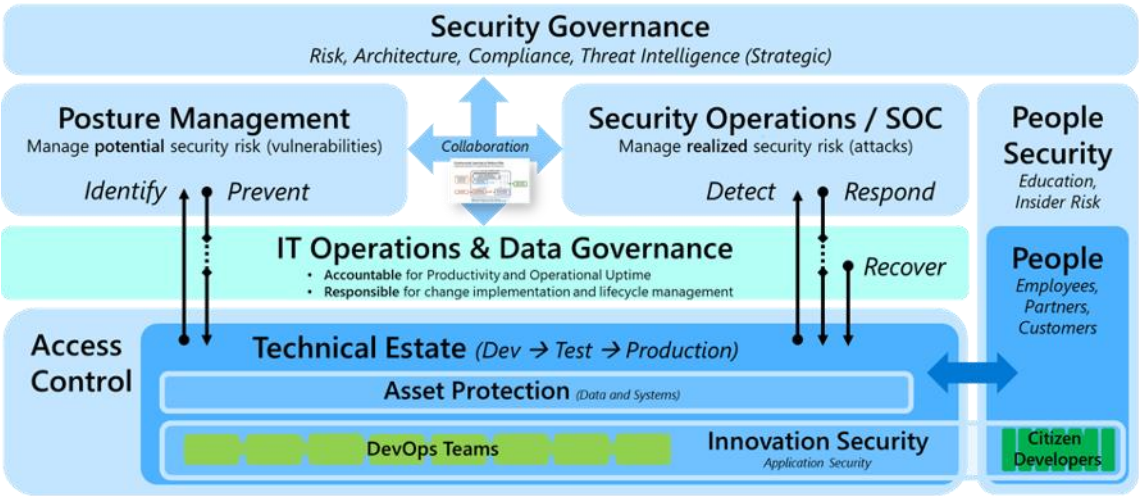

Figure 31: Zero Trust Operating Environment

The NIST Cybersecurity Framework Functions of Identify, Protect, Detect, Respond, and Recover illustrate the "overlay" nature of security teams. Security teams are able to read information and context from the environment (identify/detect) freely, but work through asset owners/managers (IT Operations) for any operations that change the environment (Prevent, Respond, Recover).

6.4.1 Asset-Centricity Platform ABBs

The Asset-Centricity Platform implements the Asset-Centricity capability. Table 11 lists each Asset Centricity Platform capability and which ABBs support it.

Table 11: Asset Centricity Platform ABBs

ABB Number	ABB	Level	Capability
ACP-1	Asset-Centricity Platform	1	Asset Centricity (AC-1).
ACP-1.1	Identity Wrapper	2	Digital Identity Binding (AC-1.1).
ACP-1.2	Asset Repository	2	Asset Management (AC-1.2).
ACP-1.3	Asset Taxonomy	2	Asset Classification (AC-1.2.1).
ACP-1.4	Asset Discovery Engine	2	Asset Capture (AC-1.2.2).
ACP-1.5	Source Code Management Engine	2	Asset Integrity Protection (AC-1.3).
ACP-1.6	Asset Patch Management Manager	2	Patch Management (AC-1.3.1).
ACP-1.7	Policy and Controls Engine	2	Asset Operational Integrity Process Management (AC-1.3.3). Asset Integrity Policy Management (AC-1.3.5).
ACP-1.8	Policy Compliance Audit Tool	2	Asset Operational Integrity Process Management (AC-1.3.3). Asset Integrity Policy Management (AC-1.3.5).
ACP-1.9	Infrastructure as Code	2	Asset Integrity Protection (Maintain) (AC-1.3).
ACP-1.10	Asset Lifecycle Manager	2	Asset Lifecyle Management (AC-1.2.4).
ACP-1.11	SBOM Manager	2	Asset Supply Chain Integrity Management (AC-1.3.4).
ACP-1.12	Supply Chain Security Risk Manager	2	Asset Supply Chain Integrity Management (AC-1.3.4).

ABB Number	ABB	Level	Capability
ACP-1.13	Configuration and Account Management ABB	2	Configuration Management (AC-1.3.2).
ACP-1.14	CVE Repository	2	Asset Vulnerability Management (AC-1.3.6).
ACP-1.15	CVE Manager	2	Asset Vulnerability Management (AC-1.3.6).
ACP-1.16	CI/CD Engine	2	Asset Integrity Protection.
ACP-1.16.1	Automated Code Scanning (ACP-1.16.1)	3	Asset Integrity Protection.
ACP-1.17	Continuous Vulnerability Scanner	2	Vulnerability Monitoring (AC-1.3.6.1).
ACP-1.17.1	Internal Vulnerability Scanner	3	Vulnerability Monitoring (AC-1.3.6.1).
ACP-1.17.2	External Vulnerability Scanner	3	Vulnerability Monitoring (AC-1.3.6.1).
ACP-1.18	Vulnerability Remediation Process	2	Vulnerability Remediation (AC-1.3.6.2).
ACP-1.19	Vulnerability Prevention Process	2	Vulnerability Prevention (AC-1.3.6.3).
ACP-1.20	Supply Chain Dependency Management	2	Asset Supply Chain Integrity Management (AC-1.3.4).

The Asset-Centricity Platform is composed of the following ABBs:

- Asset-Centricity Platform (ABB ACP-1) – Foundational ability to identify, classify, and maintain security for all types of assets:
  - — Identity Wrapper (ABB ACP-1.1) – Enables all assets to support identity and the associated access control
  - — Asset Repository (ABB ACP-1.2) – Stores cataloged and classified assets
  - — Asset Taxonomy (ABB ACP-1.3) – Supports asset classification (classify) and provides a framework and guidance for labelling assets consistently across the technical estate (with business priorities and risk signals)

— Asset Discovery Engine (ABB ACP-1.4) – Provides asset discovery and labelling across the technical estate

— Source Code Management Engine (ABB ACP-1.5) – Supports the integrity of assets, supporting the verifiability and auditability of application code in assets.

— Asset Patch Management Manager (ABB ACP-1.6) – Supports traversal of the asset repository and automated update of patches in an auditable manor

— Policy and Controls engine (ABB ACP-1.7) – Stores and maintains policies and Standard Operating Procedures (SOPs), maintaining an audit trail of changes

— Policy Compliance audit tool (ABB ACP-1.8) – Supports a controls process to capture and ensure that the policies are followed

— Infrastructure as Code (ABB ACP-1.9) – Ensures that assets are verifiable and auditable

— Asset Lifecycle Manager (ABB ACP-1.10) – Supports tracking the lifecycle of an asset during the design and build process, through provisioning to deprovisioning (retirement) of the asset

— SBOM Manager (ABB ACP-1.11) – Supports the ingestion, creation, maintenance, export, and governance of SBOMs

— Supply Chain Security Risk Manager (ABB ACP-1.12) – Manages all the capabilities required to manage Supply Chain Risk

  These capabilities will be detailed in later sections, but illustrative sources of supply chain security capabilities are the requirements detailed in the Open Trusted Technology Provider™ Standard (O-TTPS)[14].

— Configuration and Account Management ABB (ABB ACP-1.13) – Supports the auditable management of configuration items, and accounts such as service accounts

— CVE Repository (ABB ACP-1.14) – Contains the relevant CVE controls for the organization (which may be internal or using and industry standard CVE repository such as the MITRE CVE list function)[15]

— CVE Manager (ABB ACP-1.15) – Manages the import and export of CVEs, assessment, alerting, and support of controls for CVE management and compliance

— CI/CD Engine (ABB ACP-1.16) – Manages the insertion of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) into the SDLC. These are shifted-left as far as is possible so that vulnerabilities are caught early

  Both SAST and DAST may end up with false positives and tooling and processes need to plan for that. Interactive Application Solution Testing (IAST) and Runtime Application Self Protection (RASP) are not included in this because that is a runtime capability really covered by the Zero Trust Security Operations Center Capability and associated ABBs. However, controls can be placed into the CI/CD process to ensure the insertion of situational awareness into the application code and the ability to

[14] Refer to: https://ottps-cert.opengroup.org/ottps-standard.
[15] Refer to: https://www.cve.org/.

proactively respond to attacks built into the CI/CD process to ensure that it is in the application code.

- Automated Code Scanning (ABB ACP-1.16.1) – Is used by the CI/CD engines to support SAST and DAST

— Continuous Vulnerability scanner (ABB ACP-1.17) – Supports the ability to continuously scan and detect vulnerabilities in the technical estate

This allows organizations to leverage vulnerability the remediation process to proactively to remediate vulnerabilities, with an idea to limit the duration of exposure and to apply blast radius prevention measures to isolate the assets in the technical estate that have been impacted to prevent a breach. Vulnerability scanning can include internal and external vulnerability scanning to enable complete coverage of the technical estate. In cloud environments and Zero Trust oriented technical estates in general, internal scanning is very important as it addresses the perimeter-less requirement and works towards proactively establishing remediation. Also, in general, in a Zero Trust context, agent-based scanning techniques apply as network based scanning techniques cannot be outside a network perimeter – as can happen in a remote work scenario:

- Internal Vulnerability Scanner (ABB ACP-1.17.1) – Uses typically agent-based tools to scan for and monitor vulnerabilities on a continuous basis for vulnerabilities on all assets in the technical estate
- External vulnerability scanner (ABB ACP-1.17.2) – Monitors the external threat surface of the enterprise

— Vulnerability Remediation Process (ABB ACP-1.18) – Applies mitigations to address the vulnerability risk through manual actions, semi-automated actions, or fully automated actions

A vulnerability scan alert from a continuous scanning engine can trigger an automated remediation process.

— Vulnerability Prevention Process (ABB ACP-1.19) – Is a process that assess the threat posture for the technical estate of the organization for a variety of vulnerabilities, and triggers vulnerability remediation processes (ABB ACP-1.18)

— Supply Chain Dependency Management (ABB ACP-1.20) – Assesses and supports asset dependencies during the build process, as well as resulting impact to the security posture

6.4.2 Adaptive Access Control Platform ABBs

The Adaptive Access Control Platforms ABBs provide and secure access to the full diverse set of resources in the technical estate.

They do so by supporting the Adaptive Access Control capability and its composed lower level capabilities of policy decisioning and enforcement. In a Zero Trust context, policy decisioning must be centralized and consistent, and access policies must be Agile and adaptive to accommodate rapid changes in business, technology, and security. Table 12 lists each Adaptive Access Control capability and which ABBs support it.

Table 12: Adaptive Access Control ABBs

ABB Number	ABB	Level	Capability
AAC-1	Adaptive Access Control Platform	1	Adaptive Access Control (AAC-1).
AAC-1.1	Adaptive Policy Information Point (PIP)	2	Policy and Identity Storage (AAC-1.4).
AAC-1.2	Adaptive Policy Decision Point (PDP)	2	Policy Decisioning (AAC-1.2.2).
AAC-1.3	Adaptive Policy Enforcement Point (PEP)	2	Policy Enforcement (AAC-1.2.2.1).
AAC-1.4	Adaptive Policy Manager	2	Policy and Identity Storage and Management (AAC-1.4). Policy Decisioning (AAC-1.2.2). Policy Enforcement (AAC-1.2.2.1). Policy Management (AAC-1.2.2.2). Asset Entitlement Assignment (AAC-1.2.2.3). Subject Security Status (AAC-1.2.1). Subject Security Status Determination (AAC-1.2.1.1). Subject Security Status Management (AAC-1.2.1.2).
AAC-1.5	IDP	2	Authentication (AAC-1.1). Trust Validation (AAC-1.2). Authorization (Allowed) (AAC-1.3).

The Adaptive Access Control Platform is primarily composed of the following ABBs:

- Adaptive Access Control Platform (ABB AAC-1) – Provides a policy engine and signals that apply real time evaluation and application of organizational policy to access requests across all types of asset (resource):
  - — Adaptive PIP (ABB AAC-1.1) – Is a repository of policies and support all aspects of policy management

— Adaptive PDP (ABB AAC-1.2) – Makes access decisions at the time of access request based on consistent policy and dynamic data including threat intelligence, access context, and more

This ABB makes resource access decisions based on the organizational policy and the relative security risk of the subject and their session.

This policy engine should assess policy and grant access, deny access, or provide an inline remediation mechanism. This inline remediation mechanism allows the subject to present additional proof that they are the actual subject and have exclusive control of their account (e.g., an attacker does not have access to the account or credentials). This proof could come in the form of the subject presenting their biometric or Personal Identification Number (PIN) to the user's managed and trusted device.

The policy should be informed by context from multiple sources including:

- Behavior analytics of the subject to identify anomalies in behavior patterns
- Security integrity of device or host being used by subject to request access (if available)
- Access policies for the organization, such as requiring high security devices to access specific assets, asset-specific policies thresholds, geo-location restrictions, and more
- Pre-determined access authorizations such as RBAC and ABAC
- Threat intelligence feeds and data to provide risk context from current threats:

— Adaptive PEP (ABB AAC-1.3) – Enforces access control policies on the assets based on the policy decision made by the PDP

A PDP may be integrated with a PEP to enforce policy by granting or withholding authentication tokens.

— Adaptive Policy Manager (ABB AAC-1.4) – Provides the ability to support Agile changes and updates to policy due to changes in business drivers or threats, with as much automation as possible

It supports modern techniques such as AI and other mechanisms to keep updating and evaluating risk and policy options and supports the entry of new participants through the addition of a new channel, line of business, mergers and acquisitions, or organizational chart changes.

— IDP (ABB AAC-1.5) – Stores and allows management of accounts, groups, relationships, asset objects, and other data related to subjects and assets

The IDP issues, manages, and validates electronic credentials for subjects (human, device, and workload/service) and issues assertions or claims derived from those credentials. This may be configured as a single centralized IDP or a synchronized set of providers. An IDP often has an internal RBAC model and may also provide coarse authorization for resources.

6.4.2.1 A Deeper Dive into Adaptive Access Control ABB Concepts

Policy decisioning is done using L2 policy decision point and policy enforcement point ABBs. The policy decision point ABB can be centralized or federated but must be managed consistently. The policy enforcement points are applied at the asset level.

Supporting centralizing by using either a central ABB or a federated synchronized model to achieve centralization allows the organization to seamlessly support provisioning and deprovisioning of assets. It also enables manageability, adaptability, and agility. Even in federated scenarios, having a centralized and consistent ability to establish identity and enforce policies provides the ability to support easy changes and updates.

Policy enforcement at an asset level allows decoupling assets from consumers/users of those assets which are often associated with things that change frequently, such as organizational structure and roles. Illustratively, an asset (say a microservice, an IT system, or an IOT device) can be used within the context of an enterprise, but its owner (say an organization) might go through a merger and acquisition, or be sold, or undergo an organization chart change in a restructuring initiative, or have its consumers change as new partners and sales channels bring new classes of consumers. Organizations can no longer wait long periods of time to implement these changes. The ability to enforce these capabilities at the asset level ensures that the asset is not coupled to such structures, and the policy decisioning ABB merely adds, deletes, or modifies policies determining the relationship between assets and consumers.

An Adaptive Policy Decision Point ABB supports the ability to make intelligent decisions on policy updates in order to automate the policy management process. This allows management of the increasing complexity and volume of access control policies. Adaptive decisioning may involve sophisticated ML approaches or simplistic decision trees. This helps incorporation of threat intelligence and enforcement of a dynamic policy, to enable blast radius protection when an attack is discovered, or proactively when it is expected due to threat intelligence.

6.4.2.2 Reused ABBs Associated to Other L1 ABBs

The Asset Centricity and Digital Identity Platforms are reused to support identification of assets and establishing digital identity in order for the Adaptive Access Control ABBs to be able to operate on the assets.

6.4.3 Digital Identity Platform ABBs

This group of ABBs (Table 13) is leveraged by the L1 Adaptive Access Control capability, and it implements the L1 Digital Identity capability. This provides the flexibility for people and other entities to have portable identities that can be consumed by different organizations, helping to deal with rapidly evolving business and technology structures. This is sometimes referred to as Decentralized Identity (DID) or self-sovereign identity.

Table 13: Digital Identity ABBs

ABB Number	ABB	Level	Capability Number
DIP-1	Digital Identity Platform	1	Digital Identity (DI-1).
DIP-1.1	Digital Identity Repository	2	Identity Management (DI-1.2). Digital Identity Persistence (Long-lived) (DI-1.7).

ABB Number	ABB	Level	Capability Number
ACP-1.1	Identity Wrapper (reused from Asset Centricity Platform)	2	Identity Access (DI-1.2).
DIP-1.2	Digital Identity Lifecycle Manager	2	Digital Identity Management (DI-1.2).
DIP-1.3	Digital Identity Manager	2	Identity Management (DI-1.2). Access Monitoring (DI-1.4). Access Verifiability (DI-1.3.1). Digital ID Consent (DI-1.5).
DIP-1.4	Digital Identity Consent Manager	2	Digital Identity Access Consent (DI-1.5). Digital Identity Access Consent Management (DI-1.6).
DIP-1.5	Digital Identity Definition Engine	2	Identity Definition (DI-1.1).

The Digital Identity Platform is composed of the following ABBs:

- Digital Identity Platform (ABB DIP-1) – Enables managing access to the organization's resources by clients, customers, citizens, and other external identities. This allows for support of sovereign, portable, or external/individual identities that the organization does not manage:
  - — Digital Identity Repository (ABB DIP-1.1) – Defines the link among credentials, principals, and assets
  - — Identity Wrapper (ABB ACP-1.1) – Reused from the Asset-Centricity Platform
  - — Digital Identity Lifecycle Manager (ABB DIP-1.2) – Manages the provisioning, deprovisioning, and lifecycle management of Digital Identities
  - — Digital Identity Manager (ABB DIP-1.3) – Manages the access to Digital Identities and invokes the other ABBs to support the Digital Identity Platform as well as the Identity Definition (DI-1.1) capability
  - — Digital Identity Access Consent Manager (ABB DIP-1.4) – Supports the Digital Identity Access Consent (DI-1.5) and Digital Identity Access Consent Management (DI-1.6) capabilities

    It will often be reused by and composed within the Digital Identity Manager (ABB DIP-1.3) and Digital Identity Lifecycle Manager (ABB DIP-1.2) ABBs.
  - — Digital Identity Definition Engine (ABB DIP-1.5) – Supports the Digital Identity Definition Capability (DI-1.1)

6.4.3.1 Reused ABBs Associated to other L1 ABBs

The Digital Identity Platform reuses the Asset Centricity Platform ABBs.

6.4.4 Asset-Centric Protection Platform ABBs

These ABBs (Table 14) provide for the application of security policy to the protection of various technical assets including data assets and system assets.

Asset protection regimes are dependent on the asset being protected. In general, in the Zero Trust context, asset protection of data assets involves protection of both data in use, at rest, and in flight and the lifecycle of data including the different states that it may be in and its provisioning and deprovisioning.

The use of this ABB has the following characteristics in a Zero Trust context:

- The application of asset protection is characterized by being performed by teams who regularly apply these controls on these assets (IT Operations, Data Owners, DevOps teams, etc.), helping ensure consistency across diverse types of assets

  The establishment of guardrails/governance for this is a part of the establishment of the asset protection ABB.

- Security control implementation is close to those who own the assets, empowering asset owners and ensuring that governance and controls are applied

- The Asset-Centric Protection Platform also forms the bridge to engage IT infrastructure and DevOps teams and provide an auditable means of control and implementation

- Data governance is responsible for data lifecycle governance of data assets, ensuring that data-centric incorporates all stages in an asset's lifecycle including retention, provisioning, deprovisioning, compliance and legal requirements, classification, and other concerns

  This function also addresses any data access concerns, and integration into the business use of the data, and the implications of any Zero Trust approaches on the business and the data.

Table 14: Asset-Centric Protection ABBs

ABB Number	ABB	Level	Capability
ACPP-1	Asset-Centric Protection Platform	1	Asset-Centric Protection (ACP-1).
ACPP-1.1	Data Asset Protection Platform	2	Data-Centric Protection (ACP-1.1).
ACPP-1.1.1	Data Lifecycle Engine	3	Data Classification (ACP-1.1.1). Data Lifecycle Capture (ACP-1.1.2). Data Discovery (ACP-1.1.3).

ABB Number	ABB	Level	Capability
ACPP-1.1.1.1	Data Lifecycle Governance Repository	4	
ACPP-1.1.1.2	Data Lifecycle Governance Engine	4	Data Classification (ACP-1.1.1). Data Discovery (ACP-1.1.2). Data Lifecycle Capture (ACP-1.1.3).
ACPP-1.2	Data Protection Platform	2	Data Centric Protection (ACP-1.1).
ACPP-1.2.1	Data Anonymization Engine	3	Data Centric Protection (ACP-1.1).
ACPP-1.2.2	Token Vault	3	Data Centric Protection (ACP-1.1).
ACPP-1.2.3	Data Tokenization Engine	3	Data Centric Protection (ACP-1.1).
ACPP-1.2.4	Data Encryption Service	3	Data Centric Protection (ACP-1.1).
ACP-1.2.5	Data Obfuscation Engine	3	Data Centric Protection (ACP-1.1).
ACPP-1.3	System Asset Protection Platform	2	System Asset Centric Protection (ACP-1.2).
ACPP-1.3.1	Asset Availability Protection Platform	3	System Asset Centric Protection (ACP-1.2).
ACPP-1.3.1.1	API Gateway	4	System Asset Rate-limiting (ACP-1.2.1). System Asset access Throttling (ACP-1.2.3).

Asset-Centric Protection Platform is primarily composed of ABBs focused on Data-Centric Asset Protection and System-Centric Asset Protection.

- Asset-Centric Protection Platform (ABB ACPP-1) – Enables the organization to discover, protect, and monitor the security of system and data assets at any time, and at any place
  - — Data Asset Protection Platform (ABB ACPP-1.1) – Includes the following ABBs, in the context of Zero Trust, that provide the ability to support:
    - Data Lifecycle Engine (ABB ACPP-1.1.1) – Builds a catalog of data assets and their lifecycles, maintains it, and makes it available for queries/reporting

This includes tracking of security criteria such as data classification, data protection controls (e.g., encryption levels), data protection mechanisms (e.g., tokenization, obfuscation, masking), data lifecycle (e.g., provisioning, deprovisioning, and protections in different states), audit and compliance controls, and controls associated with the data in different states of the lifecycle. This might be broken up into a Data Lifecycle Governance repository and engine.

- Data Lifecycle Governance Repository (ABB ACPP-1.1.1.1) – Contains Data Assets, their lifecycle states, data sensitivity and business value in that state, associated data classification and controls
- Data Lifecycle Governance Engine (ABB ACPP-1.1.1.2) – Updates and manages the state of the data asset based on changes that might occur to assigned business value and changing threats and risk levels

— Data Protection Platform (ABB ACPP-1.2) – Implements the L2 data assets protection capability for the L1 Asset-Centric Protection capability by encrypting sensitive files and managing keys to access them and through Data Tokenization Service/Engine and data anonymity engines to provide capabilities, such as K- and T- anonymity

Some ABBs that this might be decomposed to include:

- Data Anonymization Engine (ABB ACPP-1.2.1) – Anonymizes data based on a combination of regulatory, risk and other attributes
- Token Vault (ABB ACPP-1.2.2) – Manages data tokens (data elements that substitute for sensitive data, eliminating or reducing the value for malicious actors)
- Data Tokenization Engine (ABB ACPP-1.2.3) – Manages the creation, and lifecycle management of tokens
- Data Encryption Service (ABB ACPP-1.2.4) – Encrypts data based on regulatory, risk, and security controls
- Data Obfuscation Engine (ABB ACPP-1.2.5) – Supports a standards and regulation compliant one-way hash function that converts a high value data element to a low or no value data element. The new data element cannot be reverted to the original high value data element

— System Asset Protection Platform (ABB ACPP-1.3) – Includes the following ABBs, in the context of Zero Trust, that provide the ability to support:

- Asset Repository (ABB ACP-1.2) (reused) – Reused from the Asset-Centricity Platform; contains meta-information about assets including classification, risk, BC/DR controls, Distributed Denial-of-Service (DDOS) controls, Supply Chain, presence in DevOps (for example is the asset a part of an infrastructure as a service, and managed and audited in that manner), etc.
- Adaptive Access Control Platform (ABB AAC-1) (reused) – Reused from Adaptive Access Control Platform; provides a policy engine and signals that apply real time evaluation and application of organizational policy to access requests across all types of asset (resource)

- Asset Availability Protection Platform (ABB ACPP-1.3.1)– Refers to the ABBs incorporating the support for the L2 system asset protection capability, including:
  - API Gateway (ABB ACP 1.3.1.1) – Implements rate-limiting and throttling
  - Security Zones Platform (ABB SZP-1) (reused) – Enables the organization to discretely protect groups of highly sensitive, highly valuable, or highly fragile assets with common controls and processes
  - Asset Centric Security Operations Platform (ABB ACSOP-1) (reused) – Enables rapid detection, response, and recovery from security incidents with a coordinated system of people, process, and technology

6.4.4.1 Reused ABBs Associated to Other Capabilities

1. Security Zones Platform.
2. Asset-Centricity Platform.
3. Adaptive Access Control Platform.
4. Asset-Centricity Security Operations Platform.
5. Rapid Incident Response Engine from the Asset-Centric Security Operations Platform.

6.4.5 Asset-Centric Security Operations Platform ABBs

Security Operations (Centers) provide an operational function that focuses on mitigating realized risk (in the form of active attacks). Rapid incident response minimizes the blast radius and impact of an attack. This is the basic minimum foundation of security operations – ensuring that attackers who are found are evicted from access.

Zero Trust broadens the role of security operations to the full technical estate beyond the firewall and focuses on partnership and integration with IT Operations and DevOps teams. Zero Trust also introduces a proactive approach that includes threat hunting, continuous improvement and automation, and red and purple team operations.

Zero Trust security operations focuses on all elements of the CIA triad including “availability” to avoid and quickly recover from interruption of business-critical services through ransomware, extortion, and other disruptive attacks.

This group of ABBs (Table 15) supports security operations in an asset-centric manner.

Table 15: Asset-Centric Security Operations ABBs

ABB Number	ABB	Level	Capability
ACSOP-1	Asset-Centric Security Operations Platform	1	Asset-Centric Security Operations (ACSO-1). Rapid Incident Response (ACSO-1.1).
ACSOP-1.1	XDR	2	Asset-Type Specific Attack Detection (ACSO-1.6). Integrated Threat Intelligence Feeds (ACSO-1.10).
ACSOP-1.2	Case Management	2	Case Management (ACSO-1.2.1). Incident Management (ACSO-1.2).
ACSOP-1.3	Major Incident Management	2	Major Incident Management (ACSO-1.2.2).
ACSOP-1.4	SOAR	2	SOAR (ACSO-1.8).
ACSOP-1.5	SecOps Business Intelligence Platform	2	SecOps Business Intelligence (ACSO-1.3).
ACSOP-1.6	Threat Hunting	2	Threat Hunting and Detection Tuning (ACSO-1.4). Threat Hunting (ACSO-1.4.1).
ACSOP-1.7	SIEM	2	SIEM (ACSO-1.7). Integrated Threat Intelligence Feeds (ACSO-1.10).
ACSOP-1.7.1	Security Data Lake	3	Security Data Lake Capability (ACSO-1.7.1).
ACSOP-1.8	Intelligent Anomaly Detection	2	Advanced Security Analytics (ACSO-1.9).
ACSOP-1.9	Intelligent Behavior Analytics	2	Advanced Security Analytics (ACSO-1.9).
ACSOP-1.10	Detection Tuning	2	Detection Tuning (ACSO-1.4.2).
ACSOP-1.10.1	Purple Teaming	3	Purple Teaming (ACSO-1.4.3).
ACSOP-1.10.1.1	Red Teaming	4	Red Teaming (ACSO-1.4.3.1).

ABB Number	ABB	Level	Capability
ACSOP-1.11	Threat Intelligence Platform	2	Threat Intelligence (ACSO-1.5).
ACSOP-1.12	SecOps Custom Development Tools	2	SecOps Custom Development (ACSO-1.11).

The Asset-Centric Security Operations Platform includes the following ABBs:

- Asset-Centric Security Operations Platform (ABB ACSOP-1) – Enables rapid detection, response, and recovery from security incidents with a coordinated system of people, process, and technology

  — XDR (ABB ACSOP-1.1) – Provides high quality threat detection (and enhanced investigation experience) for individual asset types such as endpoint, identity, storage, email, databases, network, Enterprise Resource Planning (ERP) systems, OT and IoT devices, etc.)

  This provides detections for common threats without requiring building queries manually, and often allows for custom queries and advanced hunting.

  — Case Management (ABB ACSOP-1.2) – Acts as an incident response engine to coordinate rapidly across tools and teams

  This enables tracking of current security incidents (status, history, relationship to other cases, associated threat intelligence, and other context) and provides a historical record to support threat research for current incidents, threat hunting, and other activities. This also provides the core dataset for SecOps Business Intelligence Platform (ABB ACSOP-1.5), supports Major Incident Management (ABB ACSOP-1.3), supports integration with the Asset Repository (ABB ACP-1.2), supports and integrates with Governance and DevOps/DevSecOps processes, tools, and teams.

  — Major Incident Management (ABB ACSOP-1.3) – Utilizes standard processes and tooling to rapidly and efficiently manage the risk of major incidents

  This enables security analysts to efficiently get support from peers in an “all hands on deck” situation. This also enables analysts to provide other teams (communications teams, legal teams, organizational leaders, and others) incident information they require while minimizing impact on rapidly resolving the incident. Attack Simulation Exercises (ABB ZTGP-1.9) help improve these processes and people’s readiness to follow them.

  — SOAR (ABB ACSOP-1.4) – Enables the response process and facilitates incident analysis and response using automated digital models

  — SecOps Business Intelligence Platform (ABB ACSOP-1.5) – Enables visibility on the business and process health of the SOC by providing analytics and reporting

  This helps track standard metrics like MTTR and MTTA as well as perform custom reporting on particular case types, particular root causes, etc. to assess the potential impact of shifting security investments.

  — Threat Hunting (ABB ACSOP-1.6) – Enables searching for adversaries that have already gained access to organization’s assets without being detected

This ABB focuses on reducing risk to the organization by reducing the time that attackers have access to business assets after a successful attack. This function is required to detect and evict adversaries that are skilled or lucky enough to evade standard detections. Threat hunting is still largely a manual capability relying on deep human expertise, though it is increasingly leveraging ML and AI Advanced Security Analytics (ABB ACSO-1.9), and SOAR (ABB ACSOP-1.4).

— SIEM (ABB ACSOP-1.7) – Detects threats for scenarios and data sources which are not covered by the asset-centric Detection and Response tooling

It aids investigation by correlating across all tools and data, and it enables advanced detection and advanced hunting.

- Security Data Lake (ABB ACSOP-1.7.1) – Stores a large amount of security operations data across many sources in the organization (events, alerts, and other data) that can be queried for various purposes

— Intelligent Anomaly Detection (ABB ACSOP-1.8) – Identifies anomalies in the collected data using ML and other advanced analytics

— Intelligent Behavior Analytics (ABB ACSOP-1.9) – Identifies anomalies based on users and entities behavior (also known as User and Entity Behavior Analytics (UEBA))

— Detection Tuning (ABB ACSOP-1.10) – Enables and enhances detection of attackers across the lifecycle of an attack (often called an attack chain or kill chain) including attacker planning, entering, traversing, and executing objectives

The MITRE ATT&CK® framework may be used to measure completeness against current attack techniques.

- Purple Teaming (ABB ACSOP-1.10.1) – Enables rapid improvement of organizational defenses through a collaborative process between red teams (simulated attackers) and blue teams (defenders)

  Blue team defenders (security operations and other security roles) are able to rapidly gain rich insights into attacker thought processes and techniques to apply to their daily roles. Red teams are able to improve their skills and context to better simulate attacks and continuously push blue teams to improve their defenses (and get/stay ahead of real attackers).

  - Red Teaming (ABB ACSOP-1.10.1.1) – Improves preventive controls and detection, investigation, and hunting processes/tooling by simulating persistent attackers that constantly search for security weaknesses in the organization

    Note: It is critical that this function is goaled on improvement of the organization's defenses (*via* purple teaming or other interactions with defenders) and not "successfully attacking" the organization.

— Threat Intelligence Platform (ABB ACSOP-1.11) – Supports the L2 integrated threat intelligence capability and allows ensuring that the threat intelligence context is integrated into all security operations processes and tooling, including detection, incident response (investigation), and threat hunting

This ABB includes integration into the XDR (ABB ACSOP-1.1) and SIEM (ABB ACSOP-1.7) / SOAR (ACSOP-1.4).

— SecOps Custom Development Tools (ABB ACSOP-1.12) – Implement the SecOps Custom Development *(*ACSO-1.11) capability

6.4.5.1 Reused ABBs Associated to Other Capabilities

The Asset Centric Security Operations ABBs reuse the Asset Centricity Platform, and the Security Zones Platform.

6.4.5.2 A Deeper Dive into Asset-Centric Security Operations Concepts

The Asset-Centric Security Operations ABBs:

- Focus metrics and process success on time to remediate (as ultimate goal of rapidly removing attacker access to assets) and time to acknowledge (as a key early indicator of getting analysts started on an investigation)
- Require a high true positive rate for alert feeds to Tier 1, allowing them to be more effective and stop wasting time/energy/morale on false positives
  - — This requires a threat hunting team to avoid missing real incidents in the lower quality alert feeds, rather than a reactive approach to try and detect everything at Tier 1
  - — The process/practice can be assisted by an ABB that allows rating alert feeds with true positive rate
- Use increased automation and the integration of ML technologies to rapidly reason over large datasets to establish baselines and quickly spot anomalies from those baselines
- Leverage known attack frameworks such as the MITRE ATT&CK framework to measure their coverage and capabilities and continuously improve them.
- Integrate with IT capabilities and processes like ITSM and Configuration Management Database (CMDB)
- Integrate external providers like Managed Security Service Providers (MSSP) and Managed Detection and Response (MDR) vendors to supplement their SecOps programs
- Shift some scenarios from the traditional SIEM (ABB ACSOP-1.7) to the XDR ABB (ABB ACSOP-1.1), replacing the (slow) legacy way of moving numerous network detections/data off the egress point (firewall, IDS/IPS) and then processing in SIEM (heavily manual) and then remediating by blocking Ips at the firewall (and cleaning up endpoints)

6.4.6 Security Posture Management Platform

Posture management is an operational function that focuses on mitigating potential security vulnerabilities in partnership with operations teams in IT, OT, IoT, and DevOps teams. Posture management is a hallmark of ZTAs, enabling Digital Enterprises to operate proactively and to establish preventive controls that block future attacks from happening.

This Zero Trust function is a greatly expanded and integrated version of vulnerability scanning. Posture management enables a proactive, holistic security approach that allows the organization

to burn down the “technical debt” of weak security practices that have accumulated over 30-plus years of adopting computer technology.

Because the posture of a complex organization is often complex and difficult to discover with a single approach, posture management ABBs (Table 16) include both an inside-out and outside-in view.

Table 16: Security Posture Management ABBs

ABB Number	ABB	Level	Capability
SPMP-1	Security Posture Management Platform	1	Security Posture Management (SPM-1.1).
SPMP-1.1	Continuous Security Posture Management Platform	2	Continuous assessment of posture (SPM-1.1).
SPMP-1.1.1	External Attack Surface Management (Outside-in Scanning)	3	EASM (SPM-1.7).
SPMP-1.1.2	Application Penetration Testing	3	Application and API Security Validation (SPM-1.7.1).
SPMP-1.1.3	Monitoring of Application/API Posture	3	EASM (SPM1.7).

The Security Posture Management Platform includes some or all of the following ABBs:

- Security Posture Management Platform (ABB SPMP-1) – Enables the organization to discover and analyze the security posture of the organization and its exposure to attacks and risk

  — Continuous Security Posture Management Platform (ABB SPMP-1.1) – Enables visibility into various aspects of security posture across cloud (sometimes called cloud security posture management), on-premises, endpoints/devices, applications, network, identity, and more

  This often incorporates recommendations, best practices, and scoring as well as ML/AI technology. This also enables individual asset owners (such as DevOps teams, infrastructure teams, etc.) to monitor the status of their own assets so they can continuously improve their security posture.

  This ABB uses the internal vulnerability scanner (s) (ABB ACP-1.17.1) to monitor the security status of the organization’s posture such as a CSPM tool that continuously reports on and makes recommendations to improve security posture.

- External attack surface management tool (outside-in scanning) (ABB SPMP-1.1.1) – Uses external vulnerability scanners (ABB ACP-1.17.2) provided by vendors that monitor the security posture and attack surface of the organization from the internet (mimicking an attacker's view of the organization)

  Tools like EASM products monitor what the digital footprint of the organization looks like across their platforms, websites, brands, multiple cloud types and providers, on-premises datacenters, mobile, social, third parties, and more. This ABB supports the capabilities to scan, evaluate, and take decisions based on the scan results.

- Application penetration testing (ABB SPMP-1.1.2) – Enables evaluation of important applications and planning for remediation of vulnerabilities

- Monitoring of application/API posture (ABB SPMP-1.1.3) – Enables audit and scan teams to monitor Application (APP)/API posture

6.4.6.1 Reused ABBs Associated to Other Capabilities

This ABB reuses the Asset Centricity Platform and the Digital Identity Platform.

6.4.7 Zero Trust Governance Platform ABBs

This group of ABBs (Table 17) provides visibility and policy control over the entire technical estate.

Zero Trust Governance includes traditional risk, compliance, and policy functions, but they are more dynamic (e.g., two-week sprints for policy updates rather than updates occurring every few years).

Table 17: Zero Trust Governance ABBs

ABB Number	ABB	Level	Capability
ZTGP-1	Zero Trust Governance Platform	1	Zero Trust Governance (ZTG-1).
ZTGP-1.1	Audit on Demand Engine	2	Audit on Demand (ZTG-1.1).
ZTGP-1.1.1	Audit Reporting Manager	2	Audit on Demand (ZTG-1.1).
ZTGP-1.1.2	Risk Alignment Tool	3	Audit on Demand (ZTG-1.1).
ZTGP-1.1.3	Regulatory Rules Compliance Engine	3	Audit on Demand (ZTG-1.1).
ZTGP-1.3	Privacy by Design Engine	2	Privacy by Design (ZTG-1.2).

ABB Number	ABB	Level	Capability
ZTGP-1.4	Asset Protection Governance Manager	2	Asset Protection Governance (ZTG-1.3).
ZTGP-1.5	Posture Management Governance Manager	2	Asset Protection Governance (ZTG-1.3).
ZTGP-1.6	Zero Trust Organizational Structure	2	Zero Trust Organizational Structure (ZTG-1.4).
ZTGP-1.7	Zero Trust Organizational Process Manager	2	Zero Trust Organizational Processes (ZTG-1.5).
ZTGP-1.8	Zero Trust Continuous Learning Platform	2	Zero Trust Continuous Learning (ZTG-1.6).
ZTGP-1.9	Attack Simulation Exercises	2	Major Incident Management (ACSOP-1.3).
ZTGP-1.10	Zero Trust Strategic Governance Manager	2	Zero Trust Strategic Governance (ZTG-1.7).
ZTGP-1.10.1	Security Intelligence Engine	3	Governance (ZTG-1.7).
ZTGP-1.10.2	Security Architecture Repository and Tool	3	Governance (ZTG-1.7).
ZTGP-1.11	Security Enablement for Professional Development	2	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.1	Technical Enablement and Support	3	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.2	Developer Education and Training	3	Innovation Security for Professional Development (ZTG-1.8).

ABB Number	ABB	Level	Capability
ZTGP-1.11.2.1	Advocacy/Champions Program	4	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.3	Secure Coding Standards	3	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.4	Threat Modelling	3	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.5	Automated Code Scanning (reused ABB)	3	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.11.6	Dependency/Supply Chain Validation (reused)	3	Innovation Security for Professional Development (ZTG-1.8).
ZTGP-1.5	Posture Management Governance Manager	3	Audit on Demand (ZTG-1.1).
ZTGP-1.12	Security Enablement for Citizen Development	2	Innovation Security for Citizen Development (ZTG-1.9).
ZTGP-1.13	People Security	2	
ZTGP-1.14	Physical Security	2	

The Zero Trust Governance Platform involves the following ABBs:

- Zero Trust Governance Platform (ABB ZTGP-1) – Enables the organization to ensure consistent execution and enablement of security processes across the technical estate and organizational processes

  — Audit on Demand Engine (ABB ZTGP-1.1) – Allows for on-demand audit compliance, which is a major barrier to entry into new lines of business and technology domains

  This ABB collates the metrics into an immediate response, corelating the telemetry and information imported from the L2 continuous monitoring capability in a compliance perspective. It also composes the following:

  - Risk Alignment Tool (ABB ZTGP-1.1.1) – Aligns controls with regulatory controls

    Note that regulatory controls might be controls against regimes such as HIPAA or against governance regimes such as COSO™/ COBIT®

- Regulatory Rules Compliance Engine (ABB ZTGP-1.1.2) – Validates for compliance with accepted regulatory controls.

It also leverages a set of supporting ABBs including the Asset Repository ABB (ABB ACP-1.2) (and other Asset Centricity Platform (ABB ACP-1) composed ABBs), Threat Intelligence Platform ABB (ABB ACSOP-1.11) (including the supporting XDRs (ABB ACSOP-1.1), SIEMS (ABB ACSOP-1.7), etc. providing technical estate visibility leveraging the Asset Centricity Platform (ABB ACP-1), Access-Centric Architecture Platform (ACPP-1), Continuous Monitoring Engine (ZTGP-1.2) and other Zero Trust Governance Platform ABBs (ABB ZTGP-1).

— Continuous Monitoring Engine (ZTGP-1.2) – Includes pluggable telemetry mapped to security and compliance requirements

This ABB is composed of a metrics repository to capture metrics and a continuous monitoring export and publication ABB to support publishing and exporting the data to the Audit on Demand Engine ABB (ABB ZTGP-1.1)

— Privacy by Design Engine (ABB ZTGP-1.3) **–** Is supported by a set of ABBs that largely support the underlying L3 Capabilities

The criticality of privacy from a business risk and compliance perspective, driven by rapidly evolving regulations, geopolitical and business landscapes, tooling, and the manner in which data can be stored and accessed leads to a variety of ABBs.

The Privacy by Design Engine usually involves a cross-cutting ABB that allows ensuring that any usage of data is validated to follow privacy regulations, and there are supporting capabilities to ensure that any use of private data follows regulatory requirements. In particular, privacy by design supports the ability to do the requisite data protection, as well as appropriate regulatory reporting, and regulatory requirements support (e.g., for General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA)).

— Asset Protection Governance Manager (ABB ZTGP-1.4) – Allows organizations to track the policies being set up, ensure traceability, and audit the processes so that they are being followed

These ABBs may also be linked to compliance requirements and may be decomposed into include a policy manager, policy repository, and policy engine.

— Posture Management Governance Manager (ABB ZTGP-1.5) – Allows organizations to track the processes setup for posture management and audit the processes so that they are being followed

The Posture Management Governance Manager incorporates a process repository that documents processes and associated organizations and an audit repository that allows for monitoring compliance with the following of processes.

— Zero Trust Organizational Structure (ABB ZTGP-1.6) – Is a logical ABB and incorporates an organization repository that documents organizations, their capabilities, responsibilities, associated processes, and decision rights, as well as an audit repository that allows for monitoring compliance with the usage of the processes associated with the organization

— Zero Trust Organizational Process Manager (ABB ZTGP-1.7) – Incorporates a process repository that documents organizations, their capabilities, responsibilities, associated processes, and decision rights, as well as an audit repository which allows for monitoring compliance with the usage of the processes associated with the organization

- It may use a BPMN tool
- It is focused on security related processes

— Zero Trust Continuous Learning Platform (ABB ZTGP-1.8) – Includes the gamification engine and credential repository ABBs

The gamification engine is a highly configurable tool that may use AI to develop evolving levels of complexity to address specific criteria. The credential repository allows for the support of credentials as a mechanism to ensure a continuous learning culture.

— Attack Simulation Exercises (ABB ZTGP-1.9) – Includes conducting proactive simulation/practice exercises to continuously improve the organization's ability to respond effectively to major incidents

These exercises help identify gaps, overlaps, and other weaknesses in processes, skills, and tools that are used to respond to major incidents. The exercises also build muscle memory to speed up responses on real incidents – Major Incident Management (ABB ACSOP-1.3).

— Zero Trust Strategic Governance Manager (ABB ZTGP-1.10) – Informs security, IT, and business strategy using context from threat environment, technology, and business. This also provides clear documentation of vision and desired outcomes to provide consistency across teams. Component ABBs include:

- Security Intelligence Engine (ABB ZTGP-1.10.1) – Processes technical incidents into simple visual summaries that can inform business leaders, architects, and other stakeholders in the organization
- Security Architecture Repository and Tool (ABB ZTGP-1.10.2) – Provides an architecture repository and tool to document and store the security architecture

  It helps define a clear vision and end state across different teams and functions, and to continually work across teams to address divergence (harmonize or integrate).

— Security Enablement for Professional Development (ABB ZTGP-1.11) – Enables developers, other application/product team members, and others to get the skills, tools, and data required to apply security best practices

- Technical Enablement and Support (ABB ZTGP-1.11.1) – Enables developers to have access to application and DevOps security expertise to answer questions, request support, and other related activities
- Developer education and training (ABB ZTGP-1.11.2) – Enables developers to educate themselves on security via their preferred format (self-paced, formally structured, event-driven, etc.) through gamification and other engaging means

        - Advocacy/Champions program (ABB ZTGP-1.11.2.1) – Enables building of security knowledge and expertise within the professional development community

    - Secure Coding Standards (ABB ZTGP-1.11.3) – Define Minimum Viable Product (MVP) for security and continuous improvement of MVP. Also define standards for business-critical applications

    - Threat Modeling (ABB ZTGP-1.11.4) – Enables identification of application design and implementation vulnerabilities and identification/prioritization of mitigation for the most important risks

    - Automated Code Scanning (ABB ZTGP-1.11.5) – Reuses the CI/CD engines Automated Code Scanning (ABB ACP-1.16.1) ABB and uses SAST and Dynamic Application Security Testing **(**DAST)

    - Dependency/Supply chain validation (ABB ZTGP-1.11.6) – Reuses SBOM Manager (ABB ACP-1.11), Supply Chain Security Risk Manager (ABB ACP-1.12), Supply Chain Dependency Management (ABB ACP-1.20)

    - Monitoring of Application/API posture (ABB ZTGP-1.11.7) – Reuses from Posture Management - Monitoring of Application/API posture (ABB SPMP-1.1.3)

    - Application penetration testing (ABB ZTGP-1.11.8) – Reuses Application penetration testing (ABB SPMP-1.1.2)

— Security Enablement for Citizen Development (ABB ZTGP-1.12) – Enables citizen developers to safely build and share applications (securely handle data, connect applications, grant access to applications, and more)

— People Security (ABB ZTGP 1.13) – Manages risk from human actions including inadvertent errors (*via* user education and enablement) and malicious insiders

Zero Trust introduces this element to combat insider threats and to increase user engagement and enablement on security. This should use positive rewards and gamification to teach security knowledge, rather than a classic “phish and punish” type of punitive education.

— Physical Security (ABB ZTGP 1.14) – Provides measures to protect people, property, or information (including information systems) from unauthorized access

Although not specific or unique to Zero Trust, physical security considerations are required for completeness, including whether the physical system is protected from electronic attack, whether the electronic impact of assets on the physical world is addressed (e.g., IoT and OT), and whether the philosophy of Zero Trust is applied to physical designs.

6.4.7.1 A Deeper Dive into Zero Trust Governance Platform Concepts

Zero Trust drives agility, adaptability, continuous learning and improvement, and reduced complexity for a security architecture and program. Governance functions and policies are key to enabling that while enabling the organization to meet requirements for both internal business security assurances and external regulatory bodies.

In the context of Zero Trust, governance has both a monitoring and an enablement function to help diverse asset protection teams apply these standards. It also includes all aspects of the ZTA and incorporates goals, principles, policies, decision rights, and processes, as well as organizational structure, and it covers both operational aspects and culture, operating models, and DevSecOps.

Operational security governance provides key end-to-end services across security functions, including risk management and policy compliance. *Zero Trust introduces security architecture and threat intelligence as governance functions to drive informed decisions across systems*. Distinguishing attributes of governance in a Zero Trust context include decisions on data classification, data protection (including data tokenization), the establishment of security zones, asset classification, identity management controls, and the management of policy based adaptive access. How these capabilities interoperate and adapt to the operating environment, coupled with the operational security governance, form the core of Zero Trust Security Governance. *Continuous Monitoring* and *audit on demand* allows Zero Trust Governance to ensure that rapidly evolving compliance requirements can be met.

This ABB integrates security into development of new capabilities by professional developers (DevOps/DevSecOps teams) and Citizen Developers (low-code and no-code applications).

Figure 32 shows how Zero Trust shifts from a classic quality approval gate process that disrupts productivity and agility to an integrated approach where security elements fit smoothly into the Agile development process.

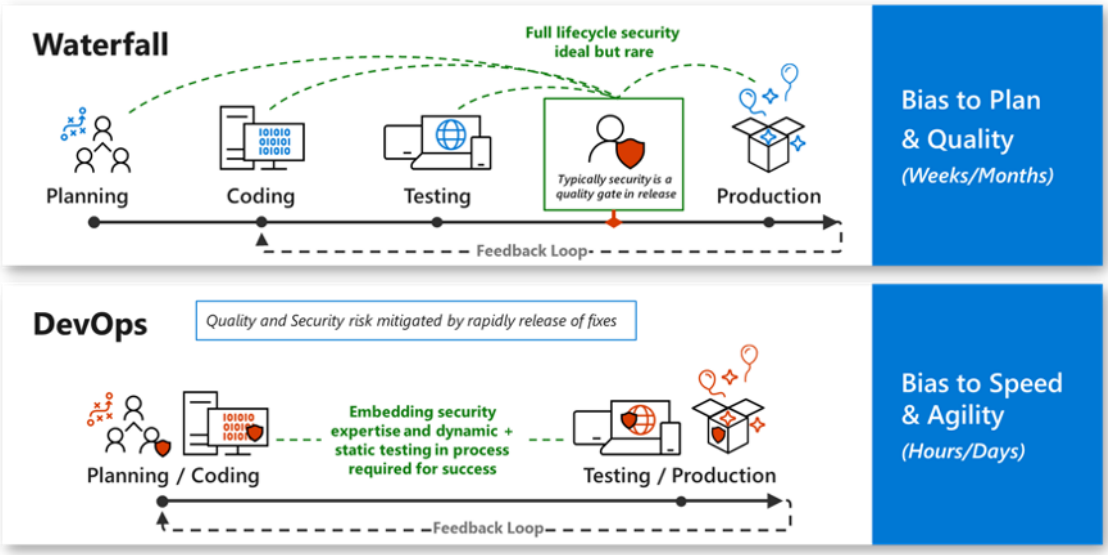

Figure 32: Zero Trust Integration of Security into DevOps Process

6.4.7.2 *Reused ABBs Associated to Other Capabilities*

The Zero Trust Governance Platform reuses ABBs from the Asset Centricity, Digital Identity, and Posture Management Platforms.

6.4.8 Security Zones Platform ABBs

These ABBs (Table 18) group systems with similar security requirements and apply similar controls over them (e.g., access controls, security configurations, maintenance processes, and exceptions).

Table 18: Security Zones ABBs

ABB Number	ABB	Level	Capability
SZP-1	Security Zone Platform	1	Security Zones (SZ-1).
SZP-1.1	Identity, Endpoint, and Application Based Security Zone Controls	2	Asset Grouping and Protection (SZ-1.1). Data Flow Direction Control (SZ-1.2). Limited Access (SZ-1.3). Monitoring of Data Flow (SZ-1.4). Data Protection at Rest, Use, and in Transit Across a Security Zone (SZ-1.5).
SZP-1.2	Data-Centric Security Zone Controls	2	Asset Grouping and Protection (SZ-1.1). Data Flow Direction Control (SZ-1.2). Limited Access (SZ-1.3). Monitoring of Data Flow (SZ-1.4). Data Protection at Rest, Use, and in Transit Across a Security Zone (SZ-1.5). Data Centric Protection of Data (SZ-1.6).
SZP-1.3	Network-Centric Security Zone Controls	2	Asset Grouping and Protection (SZ-1.1). Limited Access (SZ-1.3).
SZP-1.4	SecOps-Based Zone Controls	2	Asset Grouping and Protection (SZ-1.1). Data Flow Direction Control (SZ-1.2). Monitoring of Data Flow (SZ-1.4).

In Zero Trust terms, these ABBs include what are traditionally considered to be network zones including tiering and micro-segmentation, as well as logical zones created through access control

using a similar micro-segmentation approach and asset and data classification techniques. This allows for increasing restrictions and monitoring of high value data, attack surface reduction techniques to remove unneeded copies of data or other assets (such as tokenization where different zones are targeted for assigning replacements of the actual data), or access control. A ZTA will usually include multiple types of security zone controls.

Note: Technical controls must be fully supported by processes and people (training, awareness, skills, etc.) to be effective. Real world incidents happen regularly because there are insufficient process controls and training for how to securely support required business workflows. One example is a fully "air-gapped" manufacturing floor that was infected by a variant of Wannacrypt[16] brought in on a hardware vendor's maintenance laptop.

Zero Trust Security Zones can be divided into the following groups that act as L2 capabilities. Note that a Zero Trust approach will often combine one or more of these ABBs:

- Security Zones Platform (ABB SZP-1) – Enables the organization to discretely protect groups of highly sensitive, highly valuable, or highly fragile assets with common controls and processes

  — Identity, Endpoint, and Application-based security zone controls (ABB SZP-1.1) – Separates the technical estate based on policies that link consumer to resource

  This is implemented by the ABBs associated with Asset-Centricity, Adaptive Access Control, Asset-Centric Protection, and Asset Availability Protection.

  — Data-Centric Security Zone Controls (ABB SZP-1.2) – Allows different groupings of data to be secured in a similar way

  An example is token zones based on different keys for the same data element being tokenized to be established. See the Data Asset Protection Platform ABB for more details on the associated ABBs.

  — Network-Centric Security Zone Controls (ABB SZP-1.3) – Creates a tiered, micro-segmented environment

  Based on solution context, would have Solution Building Blocks such as firewalls, access control lists, and a micro-segmentation policy engine ABB.

  In cloud environments, access control policies, and API gateways or service meshes support this capability. The L2 ABBs are not itemized.

  Note: Network centric controls must be supplemented by other controls to provide strong assurances. Allowing exceptions in network controls for application and identity protocols without providing complementary network and application-based controls allow attackers a path to traverse a network-centric security zone boundary.

  — SecOps based Zone Controls (ABB SZP-1.4) – Mitigates realized risk to assets in a zone by limiting the time that adversaries have access to business assets

  Asset-Centric Security Operations rapidly detect and remediate threats to a subset of assets on any network, anywhere.

The ABB consists of prioritizing ABBs under Asset-Centric Security Operations Platform (ACSOP-1) based on the sensitivity of assets in a particular Zone. This supports the Zero Trust

[16] Refer to: https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/.

principle of reducing complexity by focusing security analysts first on a smaller set of alerts that are more likely to mitigate major business damage. The security zones that get increased prioritization are those with assets that have:

- High exposure to attack (such as assets directly or indirectly exposed to the public internet)
- High fragility assets (such as devices with our of support operating systems and applications that are unable to receive security updates)
- High value asset (assets that could result in a potential material loss or other major business impact)
- Combinations of the above

6.4.8.1 Reused ABBs Associated to Other Capabilities

ABBs from the Asset Centricity Platform are reused.

6.4.9 Control Management Platform ABBs

Zero Trust Operations need to have the ability to ensure that there is a framework of controls used as an overarching framework to ensure that risk is managed from a security context. Table 19 lists each Controls Management Platform capability and which ABBs support it.

Table 19: Controls Management Platform ABBs

ABB Number	ABB	Level	Capability
CMP-1	Control Management Platform	1	Control Management (CM-1).
CMP-1.1	Controls Repository	2	Control Classification (CM-1.1).
CMP-1.2	Controls Manager	2	Control Maintenance (CM-1.2).
CMP-1.3	Controls Engine	2	Control Maintenance (CM-1.2).
CMP-1.4	Controls Integration Services	2	Control Maintenance (CM-1.2).
CMP-1.5	Controls Reporting Manager	2	Control Audit (CM-1.3).

The Control Management Platform includes the follow ABBs:

- Control Management Platform (ABB CMP-1) – Enables the organization to assess and manage risk across the technical estate and processes
    - — Controls Repository (ABB CMP-1.1) – Stores controls used by the framework, the associated policies and procedures, the mapping to assets, and their compliance
    - — Controls Manager (ABB CMP-1.2) – Controls the overall platform and all its components
    - — Controls Engine (ABB CMP-132) – Does policy mapping and adaptive analysis of asset to control mapping
    - — Controls Integration Services (ABB CMP-1.4) – Enables import and export of controls as well as integration to the asset repository and other tools
    - — Controls Reporting Manager (ABB CMP-1.5) – Provides on-demand reports of enterprise compliance with the controls, assists in creating baseline reports, and drives strategy and governance

6.4.9.1 Reused ABBs Associated to Other Capabilities

ABBs from the Asset Centricity, Asset-Centric Posture Management, and Zero Trust Governance Platform are reused.

7 Coming in the Next Version of this Snapshot

During implementation, the Capabilities and ABBs defined in Chapter 5 will be used to map, based on options (the technical environment, standards, etc.) and non-functional requirements to SBBs which are actual components. As solution architectures are realized, the standard developers will map the ABBs to standards and detailed implementation patterns, often determined by scenario. These will be covered in Chapters 7-9, which will be added.

The standard developers will also be building out points that might allow compliance testing.

Acronyms & Abbreviations

ABAC	Attribute Based Access Control
ABB	Architectural Building Blocks
AI	Artificial Intelligence
API	Application Program Interface
APP	Application
CCPA	California Consumer Privacy Act
CD	Continuous Delivery
CEO	Chief Executive Officer
CI	Continuous Integration
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officers
CIS	Center for Internet Security
CISA	Chief Information Security Architects
CISO	Chief Information Security Officers
CMDB	Configuration Management Database
CSPM	Cloud Security Posture Management
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Testing
DDOS	Distributed Denial-of-Service
DDoS	Distributed Denial of Service
DevOps	Development Operations
DevSecOps	Development, Security, and Operations
DID	Decentralized Identity
DoD	Department of Defense
EASM	External Attack Surface Management

EDR	Endpoint Detection and Response
ePHI	Electronic Protected Health Information
ERP	Enterprise Resource Planning
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
GRC	Governance, Risk, and Compliance
HIPAA	Health Insurance Portability and Accountability Act
IAST	Interactive Application Solution Testing
IDP	Identity Provider
InfoSec	Information Security
InfoSec	Information Systems Security
IoT	Internet of Things
ISM	Information Security Management
ISMS	Information Security Management System
IT	Information Technology
ITSM	IT Service Management
KPI	Key Performance Indicator
MDR	Managed Detection and Response
ML	Machine Learning
MSSP	Managed Security Service Providers
MTTA	Mean Time To Acknowledge
MTTR	Mean Time To Remediate
MVP	Minimum Viable Product
NGO	Non-Governmental Organization
O-ISM3	Open Information Security Management Maturity Model
OKR	Objectives and Key Result
OT	Operational Technology
OWASP	Open Worldwide Application Security Project

PAM	Privileged Access Management
PCI	Payment Card Industry
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PID	Privileged Identity
PII	Personal Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
RACI	Responsible, Accountable, Consulted, Informed
RASP	Runtime Application Self Protection
RBAC	Role Based Access Control
SaaS	Software as a Service
SAST	Static Application Security Testing
SBB	Solution Building Blocks
SBOM	Software Bill of Materials
SecOps	Security Operations
SIEM	Security Information and Event Management
SMB	Small and Medium-sized Businesses
SOA	Service Oriented Architecture
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Capability
SOP	Standard Operating Procedures
TRM	Technology (Capability) Reference Model
TVM	Threat and Vulnerability Management
UEBA	User and Entity Behavior Analytics
XDR	Extended Detection and Response
ZTA	Zero Trust Architecture

Index