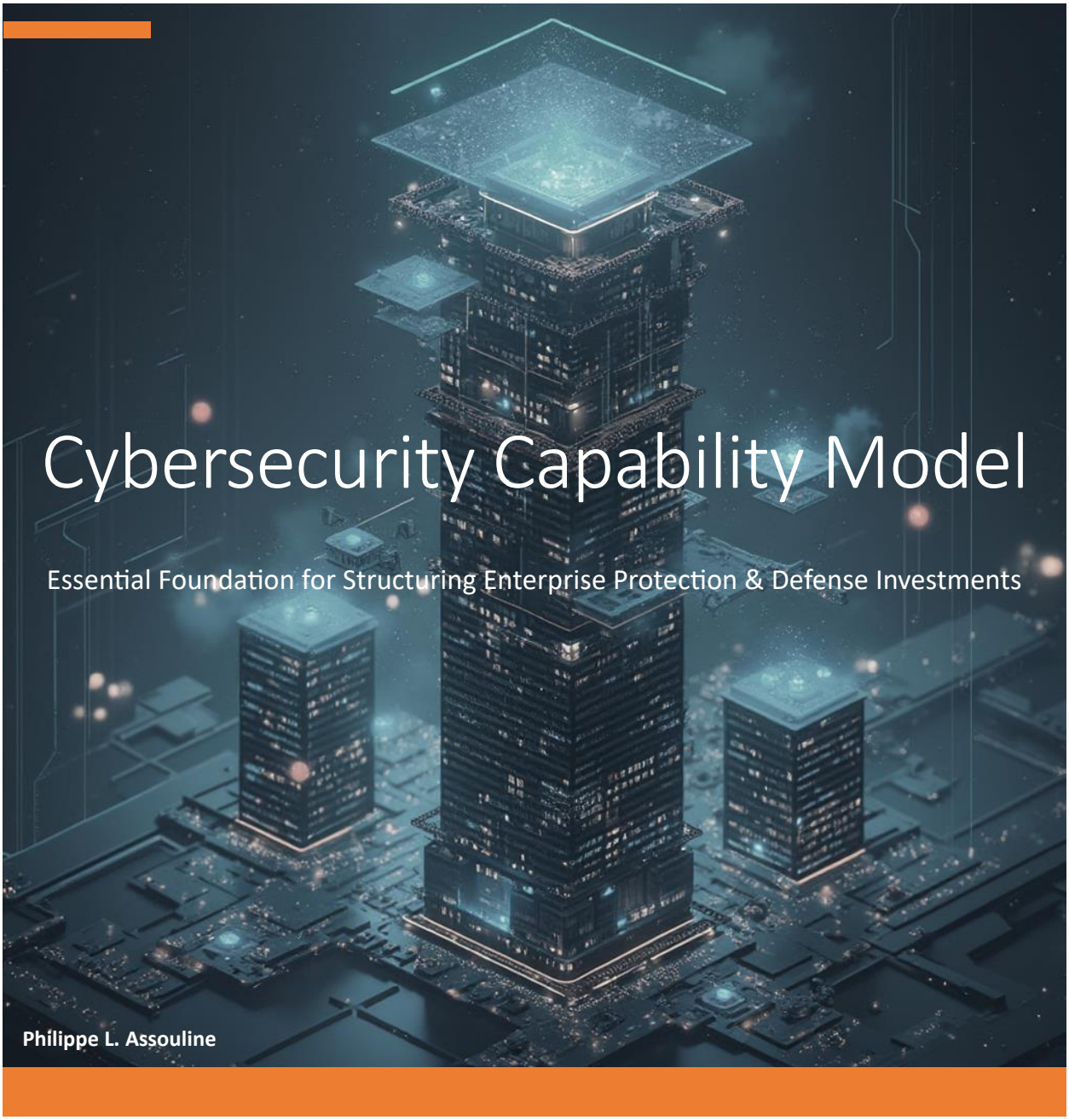
Position Paper



Cybersecurity Capability Model

Essential Foundation for Structuring Enterprise Protection & Defense Investments

Philippe L. Assouline

March, 2025

Version: 1.0

Copyright Notice

Reviewers

Bobby Rusbjerg

Bobby is a distinguished infrastructure and security architect based in Copenhagen, Denmark. He has over two decades of experience designing, implementing, and managing cutting-edge IT and security solutions for some of the financial sector's leading organizations. He assumed many critical roles throughout his career, from infrastructure architect to network platform owner, to name a couple. His contributions have been instrumental in enhancing network platforms, optimizing load balancing, and advancing IT service management for several leading European financial institutions.

Bobby currently provides his expertise to the largest bank in the Nordics, where he architecturally shapes several domains ranging from cybersecurity, security policy formulation, data center migration, Cloud adoption, and governance.

 https://www.linkedin.com/in/bobby-rusbjerg-a0615a3

Ole Marius Brandt

Ole has over twenty years of experience in IT and security, primarily within the banking, finance, and utilities sectors in the Nordics. His extensive expertise spans from infrastructure and project management to security architecture. By working across multiple domains, Ole has developed the ability to create comprehensive solutions that encompass both technical and non- technical aspects.

 www.linkedin.com/in/ole-marius-b-3332224

Kim Kirchhoff

Kim is a seasoned infrastructure, Cloud, and security architect with over 25 years of experience. He currently works for the largest bank in the Nordics, specializing in Cloud architecture and cybersecurity.
Kim's extensive expertise spans architecture, IT security, regulatory compliance, and Cloud services. His career journey includes working for several major organizations, both as an internal architect and as a consultant. Kim has occupied pivotal roles in various large enterprises, particularly within Cloud and security domains. With a wealth of knowledge and versatility, Kim brings invaluable insights across multiple industries.

 https://www.linkedin.com/in/kimkirchhoff/

Neetika Singh

Neetika is a seasoned Enterprise Security Architect with 20 years of extensive experience in various security domains, including Identity and Access Management (IAM), Cloud Security, Data Protection, and Zero-Trust security. With her mixed background in product development and service delivery, she has led security initiatives through intricate transitions and transformations. Neetika excels in formulating security policies, defining architectural principles, setting security requirements, and guiding teams in robust security governance.

Currently, Neetika leverages her extensive expertise to shape security strategies at one of the largest banks in the Nordics, where she oversees multiple domains, including cybersecurity, security policy development, IAM, and the architectural definition of a custom Zero-Trust framework. Driven by a passion for building resilient security architectures, Neetika is committed to ensuring that organizations are well-equipped to navigate and defend against evolving cyber threats.

https://www.linkedin.com/in/neetika-singh-9a582a6b/

Table of Contents

A. Introduction

Business resilience as a competitive advantage has never been more relevant as economies worldwide start converging towards Web 3.0, whose motto is “Less Trust, More Truth.”

The enterprise architecture discipline has matured over the last 30 years, and literature on the topic is widely available. As a result, organizations can leverage well-defined enterprise architecture constructs, such as the business capability model, to strategically steer their investments and activities.

As of this writing, a similarly structured and equivalent concept in the cybersecurity field appears more challenging to find. Consequently, I decided to develop one to attempt to organize the vast knowledge body associated with cybersecurity and enable enterprises to treat the cybersecurity discipline as a critical part of operating a business and not simply as a necessary expense. The cybersecurity capability model presented in this softcopy is purposefully structured like a business capability model so that organizations can similarly apprehend their cybersecurity posture and strategically invest in strengthening it over time.

The document starts by defining the term Capability Model. An imaginable cybersecurity capability model is introduced next, beginning with its most abstract and foundational elements. The rest of the document subsequently decomposes and defines the core capabilities of the model into more detailed ability levels. Conceivable use for the cybersecurity capability model is covered last, followed by possible customizations to meet organizations’ unique requirements.

This document uses the terms Enterprise, Organization, Firm, Company, and Legal Entity interchangeably because they all refer to the concept of a business entity or a legally organized structure.

The cybersecurity capability model presented in this softcopy should not be considered authoritative or definitive, as capability model development is more art than science. The model is intended to be a starting point for readers interested in developing their respective models. Users of this material are encouraged to experiment and either modify existing capabilities or create new ones to fit their needs.

Your feedback is invaluable in enhancing the model. Please share your thoughts or suggestions by contacting me via my LinkedIn profile at https://www.linkedin.com/in/philippe-assouline/. Thank you.

1. What is a Capability Model?

This document adopts the definition offered by the ArchiMate 3.2 Language Notation guide [1] to explain the term Capability.

Supplementing the ArchiMate definition, a capability has contextual and non-contextual characteristics that shape its nature and behaviors. For example, a capability can be classified as a business capability when dealing with high-level business goals. Similarly, it becomes a cybersecurity capability when goals are focused on protecting and defending digital IT assets against cyber threats, as illustrated in Figure 1. Regardless of the context, a capability refers to an ability held by a legal entity [2], a natural person [3], or a system. Non-contextual characteristics include features such as automation, effectiveness, or cost.

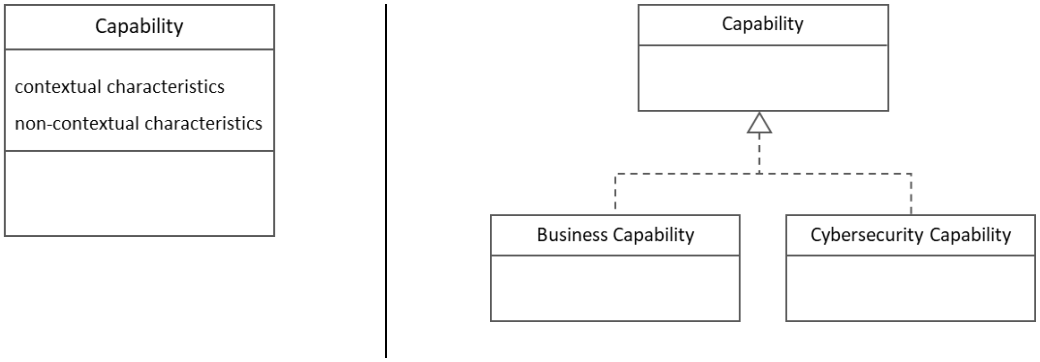


Figure 1

The maturity level of non-contextual characteristics paired with the skill and expertise of the labor force employed by a legal entity or organization affect the execution quality of a capability. Figure 2 shows the structure of a typical business capability. For example, the maturity or automation levels of a capability's underlying elements, including architectural complexity, are facets that are inherently understood to affect the execution performance or effectiveness of said capability.

Business Capability	Direct Cost			Indirect Cost	OLA	SLA
	Labor Cost (Hours)	Blended Averge Cost	Other Expenses			
Business Activities						
Application Layer						
Middleware Layer						
Data Layer						
Infrastructure Layer						
Security Layer						

Figure 2: Simplified &illustrative structure of a business capability

It is reasonable to surmise that a capability model is simply a collection of capabilities. A formal definition of a capability model follows.

Capability Model Definition
A capability model represents a curated collection of abilities or functional behaviors that can be performed by a legal entity [2], a natural person [3], or a system. These capabilities enable the execution of specific tasks [4] that contribute to the realization of desired goals and objectives, whether strategic or tactical [5].

It is important to note that contextual characteristics of a single capability are often transitive to capability models since they are a selected set of individual capabilities. For instance, a business capability model captures the universe of abilities a legal entity [2] (or accessorily a natural person [3]) must be able to perform to fulfill its overall mission, as illustrated in the figure below. Figure 3 generally depicts what (not how) most pharmaceutical companies must be able to accomplish to be in business. A business capability model does not imply how well this collection of abilities needs to be executed. It simply indicates that it needs to exist [6]. A business capability model is independent of the legal entity's structure, processes, people, or domains.

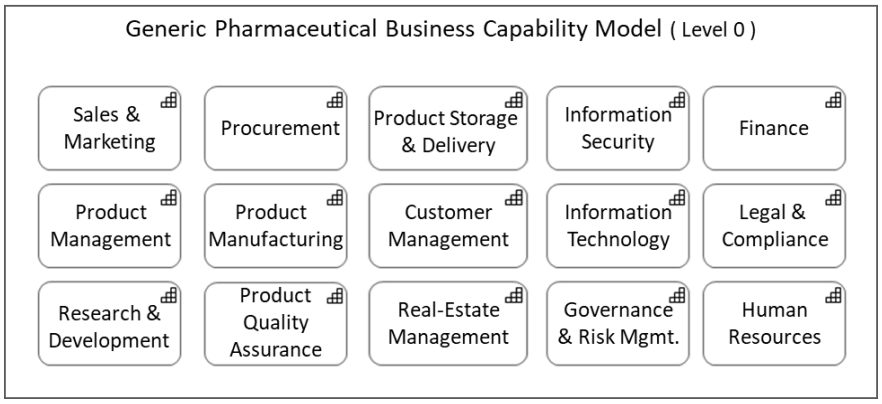


Figure 3: Illustrative pharmaceutical business capability model

Like a business capability model, a cybersecurity capability model represents the sum of abilities or functional behaviors a legal entity (or a natural person) must be able to do or perform to have a chance at protecting its IT assets by addressing threats to information processed, stored, and transported by internetworked information systems [7].

A business capability model and a cybersecurity capability model are architectural constructs designed to strategically guide investment decisions and actions to ensure the successful execution of an organization's business mission. Their correlation is essential for ensuring that an organization's strategic goals are supported by robust protective and defensive measures, even though these constructs serve the business differently. By aligning cybersecurity efforts with business capabilities, enterprises can manage risks, allocate resources efficiently, and achieve continuous improvement, all while maintaining compliance and stakeholder trust. This integrated approach enables organizations to protect their IT assets and sustain their competitive advantage in an ever-evolving threat landscape.

The figure below illustrates the symbiotic relationship between a business and cybersecurity capability model by correlating architecture layers that materialize a business capability to pertinent controls tasked to safeguard them.

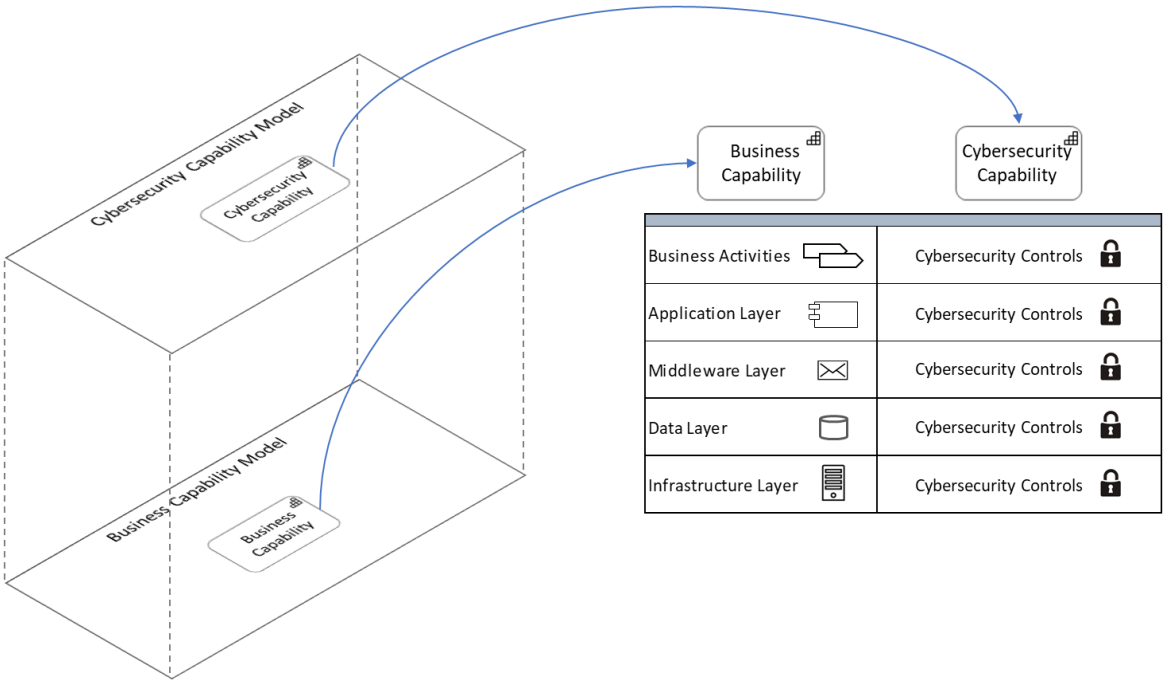


Figure 4

These relevant controls collectively form an architectural security layer designed to ensure the confidentiality, integrity, and availability of an organization's information and technology assets while providing necessary measures to protect them. Coupled with the architectural layers associated with a business capability, companies can price an individual business capability for strategic management, as illustrated in Figure 5.

Business Capability	Direct Cost			Indirect Cost	OLA	SLA
	Labor Cost (Hours)	Blended Averge Cost	Other Expenses			
Business Activities						
Application Layer						
Middleware Layer						
Data Layer						
Infrastructure Layer						
Security Layer						

Figure 5

The complementary nature of a business and cybersecurity capability model can also be used to integrate a cyber threat perspective, thus providing a cybersecurity posture across an organization's architectural layers. The diagram below suggests that the nature and types of controls vary according to the architectural layer they protect while evolving to stay abreast of evolving cyber threats. The distinct sum of all security controls across all architectural layers leads to the definition of an organization's control catalog that can then be evaluated against the ISO/IEC 27001:2022 standard for gaps and imaginable remediation actions. Note that a control catalog is simply a set of security and privacy checks coupled with related control enhancements to reduce the incidence or severity of adversarial cyber threats.

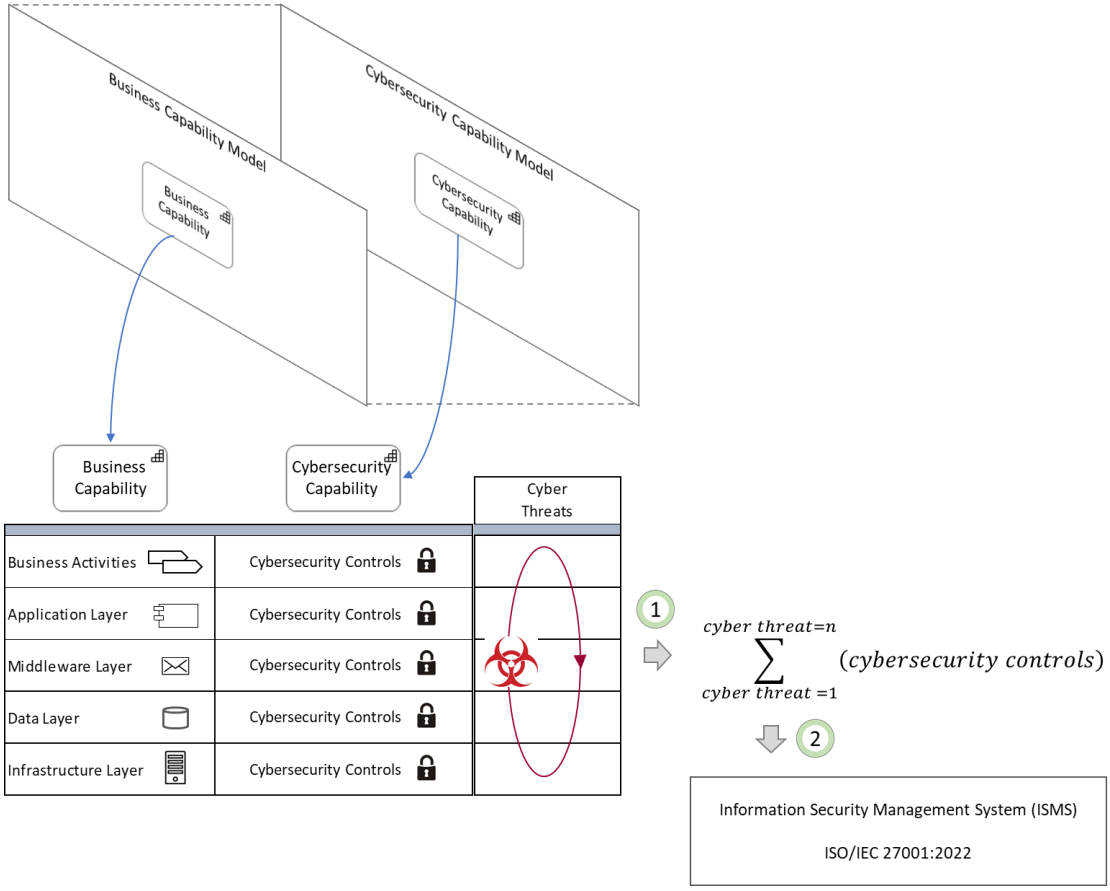


Figure 6

Information security and cybersecurity are frequently mistakenly substituted. Understanding the difference between the two will help readers better comprehend the cybersecurity capability model described in this softcopy. Paraphrasing ISACA, information security refers to safeguarding every bit of information, regardless of its format (paper, digital, visual, verbal, etc.), while cybersecurity only focuses on defending information in digital formats. Consequently, this document defines cybersecurity as a discipline for protecting digital assets by counteracting threats to data and information processed, stored, and transported by interconnected IT systems. Additionally, cybersecurity is considered a component of information security.

Figure 7 visually depicts the proposed cybersecurity capability model to help organizations better apprehend their unique cybersecurity posture and use it for strategic and operational (architectural) activities. Section 3 of the document includes a series of diagrams that show how to link the enterprise architecture and the cybersecurity disciplines for strategic investment decisions regarding the defense and protection of digital IT assets from cyber harm.

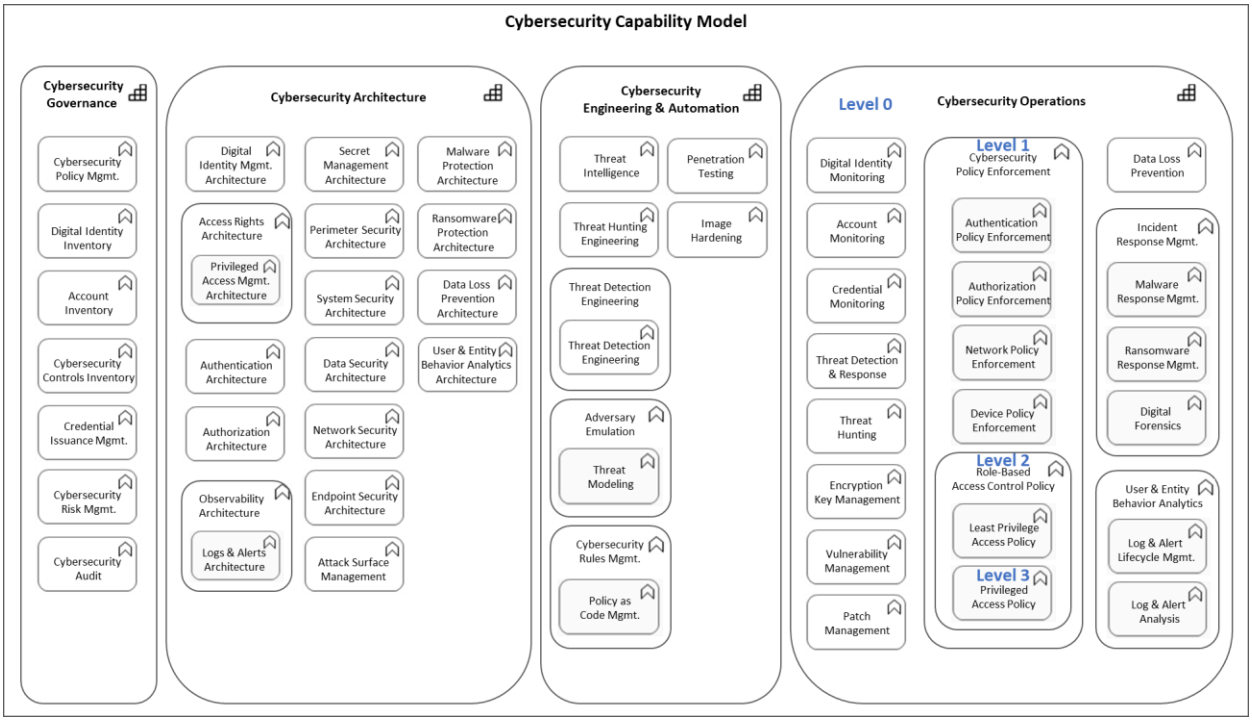


Figure 7

The remainder of the document defines each cybersecurity capability in depth according to its level. The model's foundational or level-zero cybersecurity capabilities are described in the next section.

Level Zero (0) Cybersecurity Capabilities

2. Cybersecurity Capability Model

2.1. Level Zero (0)

Level zero (0) refers to the model's most abstract cybersecurity capabilities. They are equally foundational to the cybersecurity discipline and the framework introduced in this document. The four essential cybersecurity capabilities are:

1. Cybersecurity Governance
2. Cybersecurity Architecture
3. Cybersecurity Engineering & Automation
4. Cybersecurity Operations

Figure 8 illustrates their placement in the context of a simplified but broader corporation's Information and Communication Technology (ICT) frame of reference. The definitions of these level-zero cybersecurity capabilities follow.

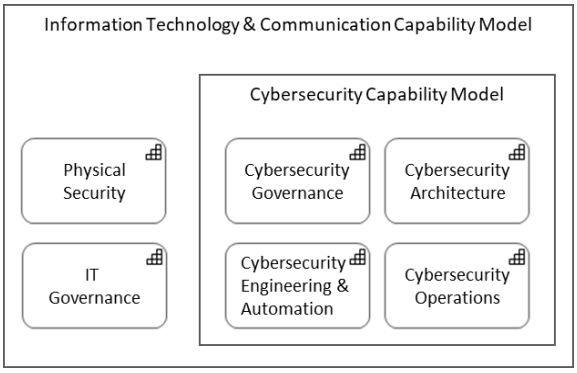
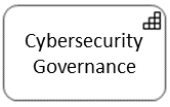
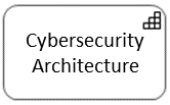


Figure 8: Cybersecurity capability model, level zero



The Cybersecurity Governance capability refers to overseeing the control and direction of protective and defensive mechanisms instituted by an organization to fend off cyberattacks and shield its digital IT assets from harm. These mechanisms range from the lifecycle management of new or existing cyber capabilities and their operational reifications, including cybersecurity-related policies, processes, standards, guidelines, and human and non-human resources, to name a few elements. Cybersecurity governance is associated with both the Risk and Compliance disciplines and is related to the broader IT governance of an enterprise. It is also often regarded as an intrinsic extension of corporate governance. Effective cybersecurity governance supports the realization of business objectives.

Further Reading:
Cybersecurity Governance | The U.S. Cybersecurity & Infrastructure Security Agency (CISA)
Understanding the Essence of Cybersecurity Governance to Organizations | Safety Culture
Building Effective Cybersecurity Governance | Harvard Law School Forum on Corporate Governance

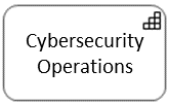


The Cybersecurity Architecture capability refers to the proactive identification, definition, and continuous adaptation of IT components that are functionally dedicated to protecting and defending an organization from cyber threats and cyberattacks. These specialized IT components are technology elements that encompass hardware, software, appliances, protocols, and networks. It also includes the structure(s), inter-dependencies, and how these specific IT components are collectively organized and integrated into an enterprise's landscape to safeguard against adverse events [8].
The reification of this capability outputs multiple blueprints from various views and viewpoints to guide the implementation of said IT components for resisting and defeating cyber assaults, including but not limited to the number, nature, and placement of cybersecurity controls within an organization's IT ecosystem.

Further Reading:
Enterprise Security Architecture—A Top-down Approach | ISACA
What Is Security Architecture? | Palo Alto Networks
What is a Cyber Security Architecture? | Check Point

The Cybersecurity Engineering & Automation capability combines software engineering and operational cybersecurity practices to protect legal entities or organizations from cyber threats in general and data breaches in particular. It includes building, configuring, maintaining, and monitoring IT systems and software to ensure their safe, secure, and resilient operation [9].
An efficient implementation of this cybersecurity capability relies heavily on leveraging technologies and automation. By doing so, organizations can achieve efficacy, accuracy, and cost-effectiveness through repeatability paired with the ability to adapt to the constantly evolving threat landscape.

Further Reading:
What Is Cybersecurity Engineering? And Why Do I Need It | Carnegie Mellon University



The Cybersecurity Operations capability alludes to detecting all events, whether adversarial or error-centric, via continuous monitoring and the subsequent purposeful orchestrated collaboration of cybersecurity components to protect and safeguard an organization against confirmed cyber threats. This capability coalesces methodologies, processes, best practices, tools, technologies, response plans, and a skilled staffing model into a homogenous and operational structural frame of reference, whose goal is to help enterprises deliver efficient, repeatable, effective, and resilient cyber defenses against a spectrum of events, ranging from subtle indicators of compromise to full-blown cybersecurity incidents [10] [11].

Further Reading:
Best Practices for Setting Up a Cybersecurity Operations Center | ISACA
What Is SecOps? Security Operations Defined | Splunk
What is SecOps? Security Operations Defined | Fortinet

As previously indicated, note the relationship between the Cybersecurity Governance and Cybersecurity Engineering & Automation capabilities and the broader IT Governance capability, which is, in turn, integrated into the larger corporate governance framework (Figure 9).

This integration scheme is crucial for holistic risk management, strategic alignment, accountability and oversight, regulatory compliance, protection of stakeholder interests, and resilience preparedness.

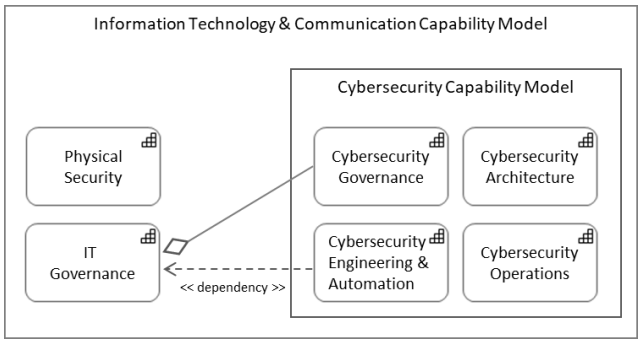


Figure 9

The foundational cybersecurity capabilities must also be carried out in a specific sequence. Figure 10 illustrates the preferred order of execution for these level-zero cybersecurity capabilities.

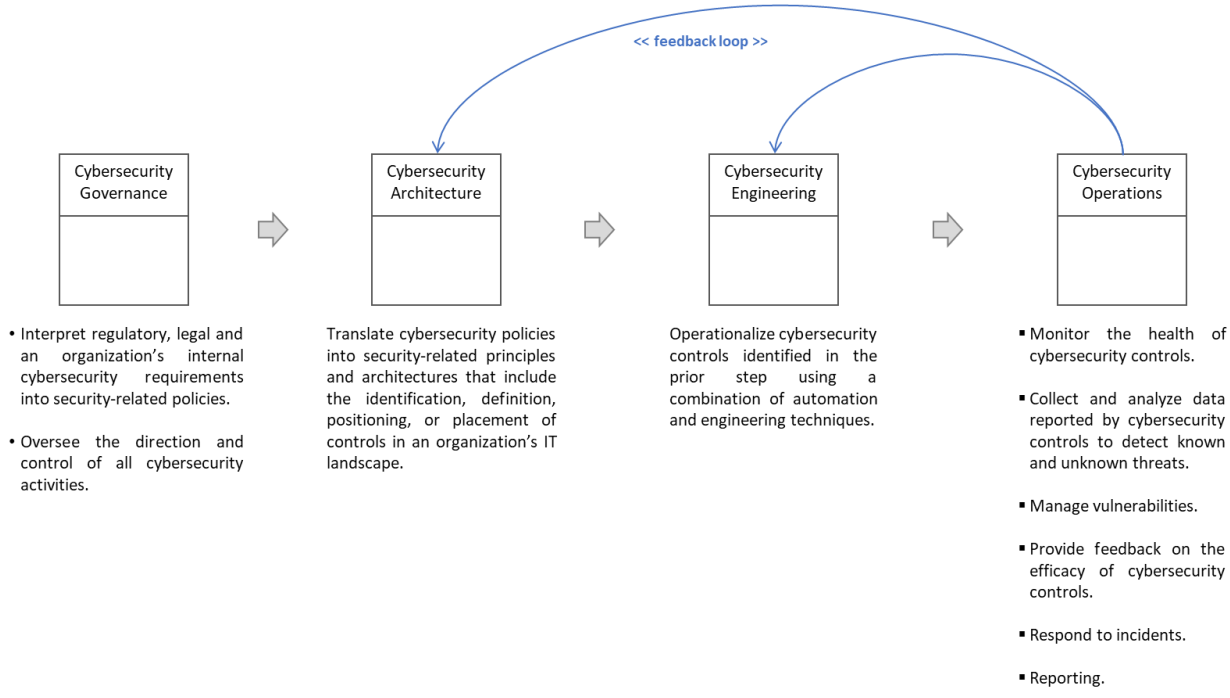
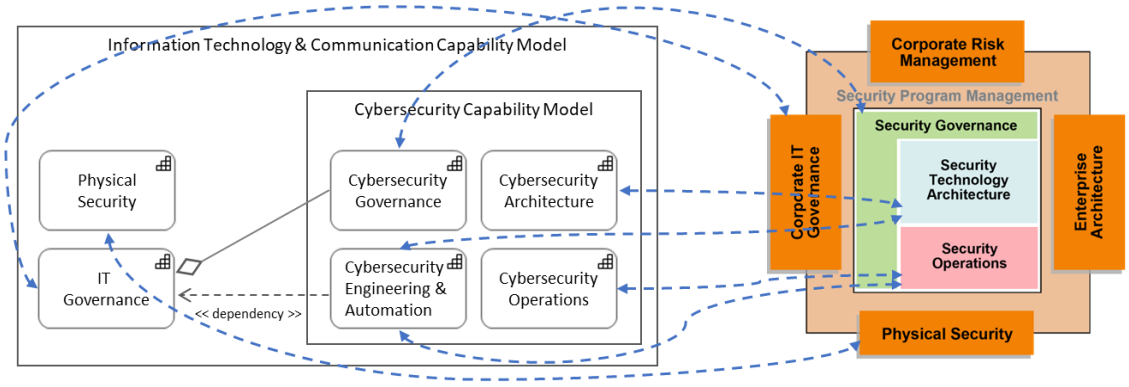


Figure 10

Neophytes tend to solely equate the cybersecurity discipline to cybersecurity operations. Putting aside the maturity level of these foundational cybersecurity capabilities, reifying all level-zero capabilities is essential for protecting and defending an organization from adversarial cyber threats. While cybersecurity operations are critical to safeguarding enterprises from adverse events on a daily basis, the importance of the Cybersecurity Architecture capability should not be underestimated. The incorrect selection of controls or their inadequate placements in an IT landscape will result in poor or incomplete data quality, which may very likely compromise the efficacy of cybersecurity operations.

Moreover, the cybersecurity capability model aligns seamlessly with the following three cybersecurity frameworks: The Open Enterprise Security Architecture (O-ESA), the NIST Cybersecurity Framework (CSF) 2.0, and the Open Security Architecture (OSA). The relationships between the cybersecurity capability model and the first two frames of reference are succinctly explained next. Section 3.1 examines the connection with the Open Security Architecture framework.

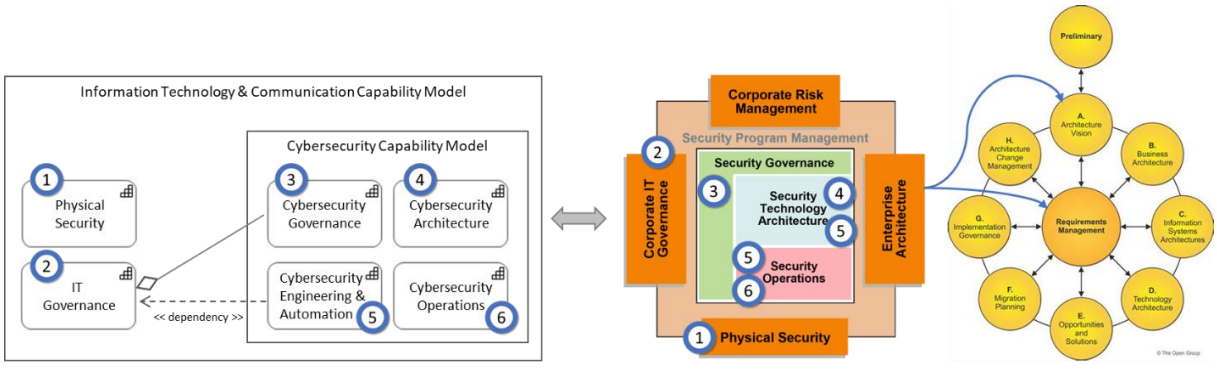
O-ESA is a security framework developed by the Open Group, the same entity responsible for managing the TOGAF enterprise architecture framework and the ArchiMate language notation. O-ESA provides a structured method for designing and implementing security policies within an organization while ensuring that security controls are aligned with business goals and integrated into an overall enterprise architecture context. Figure 11 illustrates the alignment between the cybersecurity capability model and components of the Open Enterprise Security Architecture framework, including its fitness within the broader corporate context [12].



Source: Open Enterprise Security Architecture (O-ESA) – The Open Group

Figure 11

The diagram below depicts the connections between the cybersecurity capability model, the O-ESA frame of reference, and the TOGAF Architecture Development Method (ADM) to infuse the cybersecurity discipline into each phase of the ADM to architect a comprehensive and resilient security posture when developing target state architectures.

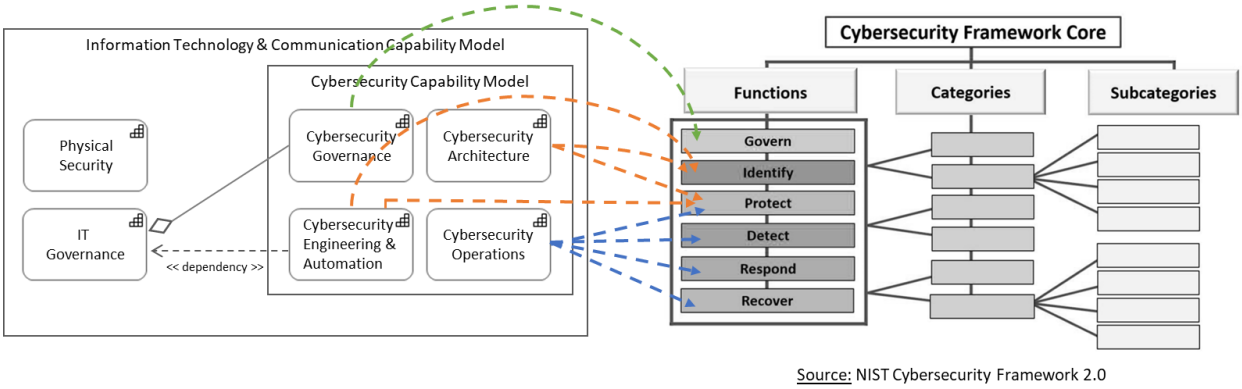


Source: Open Enterprise Security Architecture (O-ESA) – The Open Group

Source: TOGAF – The Open Group

Figure 12

The second framework reviewed is the NIST Cybersecurity Framework 2.0 (CSF 2.0). It is a comprehensive and neutral framework that guides enterprises in managing and mitigating cybersecurity risks. The framework describes six core functions organizations can utilize to apprehend, evaluate, prioritize, and communicate cybersecurity efforts to protect digital IT assets from harm. As depicted in Figure 13, the cybersecurity capability model can be leveraged to achieve these outcomes. Section 2.2.5 provides a more detailed view of the connection between both frames of reference by mapping cybersecurity-related functional behaviors defined by the cybersecurity capability model to the NIST cybersecurity outcomes.



Source: NIST Cybersecurity Framework 2.0

Figure 13

The relationship between the cybersecurity capability model and a cybersecurity framework is primordial because these constructs contribute to establishing operational resilience, or an organization's ability to anticipate, prepare for, respond to, and adapt to incremental change and sudden disruptions to maintain continuous business operations, as shown in Figure 14.

A separate white paper addresses the engineering of operational resilience, as mandated by the European Digital Operational Resilience Act (DORA) or the American Federal Information Security Modernization Act (FISMA). Both regulations aim to enhance the digital operational resilience of financial entities in their respective jurisdiction. Yet, operational resilience has become so fundamental to remaining in business nowadays that exempt organizations should strongly consider investing in it.

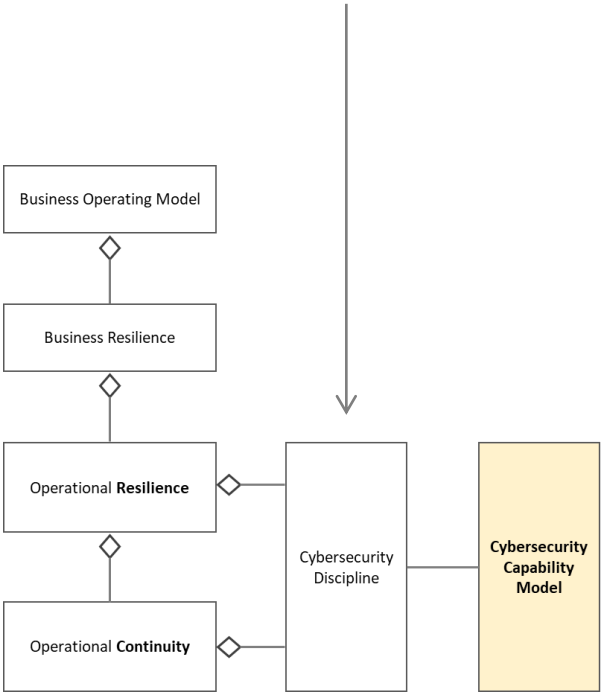


Figure 14

Next, the foundational cybersecurity capabilities are broken down into the subsequent level of detail or level 1.

Level-1 Cybersecurity Capabilities

2.2. Level 1

Level 1 refers to the model's second most abstract cybersecurity capabilities. A Level-1 capability represents a high-level unit of collective cybersecurity behavior and is more concrete than its parent capability. They are purposefully visually rendered as an ArchiMate business function to distinguish them from level-zero ones. Readers can alternatively depict them as ArchiMate capabilities when developing their model. Level-1 capabilities provide a comprehensive inventory of cybersecurity abilities required to protect and defend an organization. They serve as the starting point for further decomposition into more detailed levels of abilities.

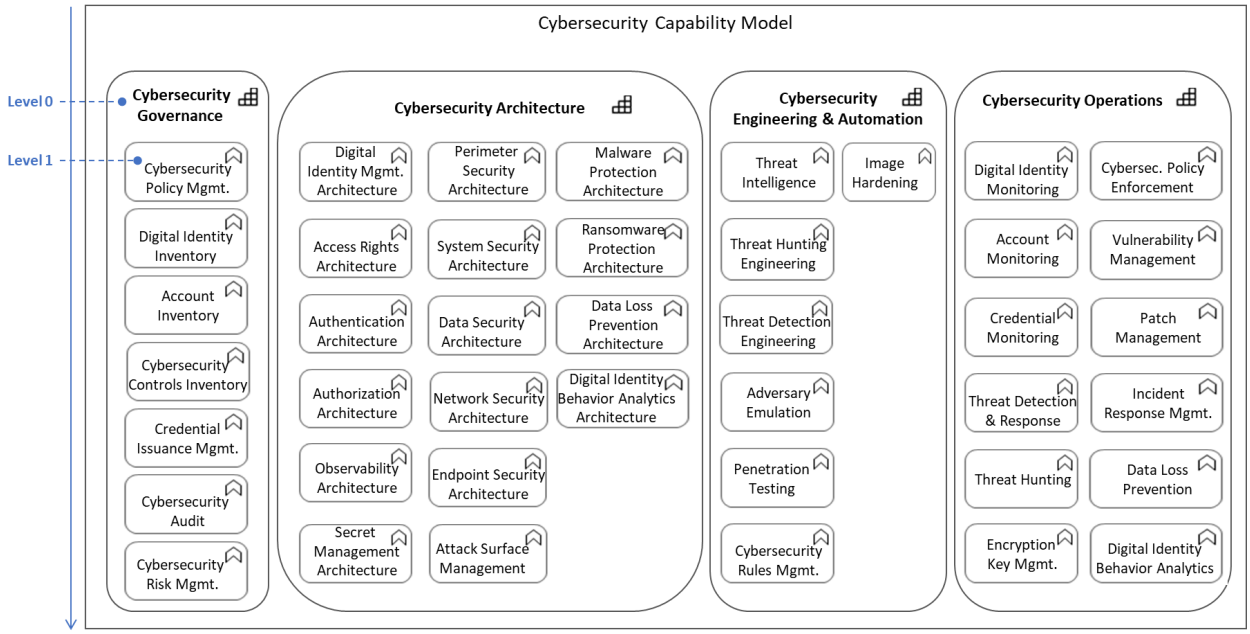


Figure 15

2.2.1. Cybersecurity Governance Capability – Level 1

Purposeful and effective lifecycle management of rules and associated procedures for safeguarding the integrity, confidentiality, and availability of digital assets, especially those of a sensitive nature. These rules foster a clear and consistent understanding of cybersecurity within an organization while guiding expected behaviors and practices to protect an organization against cyber threats. Cybersecurity rules or policies cover access control to digital assets, data protection, incident response, acceptable behavior with a firm's resources, password management, network security, etc.

Further Reading:
Cybersecurity Policies: Types & Best Practices | Splunk
Cybersecurity Policies and Procedures: How to Develop One | Cybrary

Digital Identity Inventory

The document defines a Digital Identity as an electronic or digitalized version of a legal entity [2], a natural person [3], or a machine. Similarly, in the context of this paper, digital entities are assumed to be managed by organizations. They are unique within an enterprise and often equally distinctive across different organizations, but not always.

Digital identities often represent both humans and non-humans or machines. Machine digital identities refer to systems, applications, software programs, devices, or servers. Digital identities provide access to an enterprise's digital assets via accounts (see next entry).

Consequently, the Digital Identity Inventory function points to activities and tools associated with the intentional recording and itemization of digital identities in an organization, including managing their lifecycle. Keeping a precise, complete, and accurate inventory of digital identities is crucial for any organization wanting to uphold its cybersecurity posture. Indeed, improperly managed digital entities can be used by adversaries to mount attacks. This is particularly dangerous if a compromised digital identity has privileged access rights.

Mapping a digital identity to a single legal and natural identity or machine is considered a best practice.

Please cross-reference with the Digital Identity Monitoring function anchored in the Cybersecurity Operations capability.

Further Reading:
Guidance on Digital Identity | FATF, Paris

This function is critical because several other cybersecurity functions depend on it, as illustrated in the figure below. It is also the basis for developing an identity-first cybersecurity architecture, a key component for reifying a zero-trust security architecture.

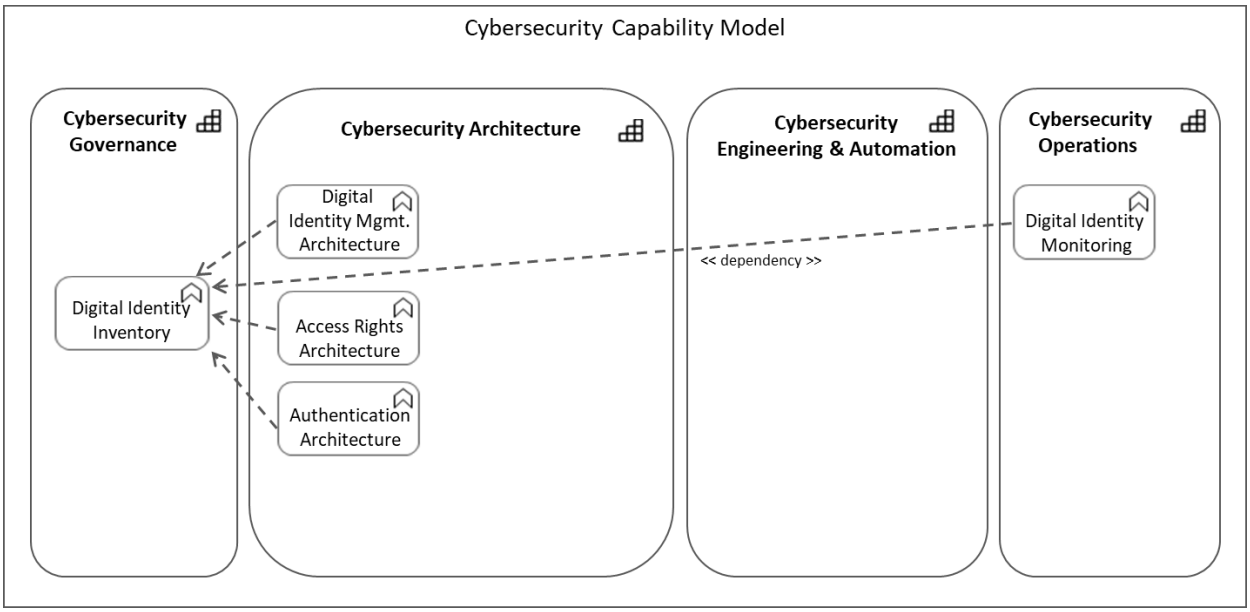


Figure 16

One of Merriam-Webster's definitions of Account is "an arrangement in which a person uses … services of a particular company." In the context of this document, an account refers to an agreement between an organization and its employees or authorized parties, represented as digital identities, to effectively utilize business, application, data, technical, or technology services offered by IT assets belonging to the organization.

Consequently, the Account Inventory capability focuses on actively keeping a comprehensive, complete, accurate, and precise list of all active accounts with or without access to an enterprise's IT assets, regardless of associated digital identities and usage granted.
Management activities to meticulously track accounts include creating, updating, and closing accounts to match the lifecycle of associated digital identities. It also entails applying policies, processes, standards, tools, and best practices to justify the status of each account.

Maintaining an accurate account inventory is crucial for the following reasons:

- Security: Helps identify unauthorized or inactive accounts that could be exploited by adversaries.
- Access Control: Prevents unauthorized (valid and fraudulent) digital identities from accessing IT assets they should not.
- Compliance: Demonstrates adherence to regulatory (if applicable) and an organization's internal requirements.
- Incident Response: Facilitates quicker response to security incidents by providing a clear view of all active accounts and their permissions.

Please cross-reference with the Account Monitoring function anchored in the Cybersecurity Operations capability.

The document defines a Control as a measurable examination, inspection, investigation, or restraining check designed to prevent, stop, or remedy the incidence and severity of an event. NIST SP 800-61 Rev.2 defines an event as "...any observable occurrence in a network or system". By the same token, a control inventory is simply an itemized list of controls.

Subsequently, the Cybersecurity Controls Inventory level-1 cyber function refers to activities and tools designed to precisely, accurately, and comprehensively catalog the number and nature of checks that protect and defend an organization's digital IT assets against adversarial events.
Checks can be categorized as preventive, detective, corrective, deterrent, physical, or compensating. An alternate scale could be leveraged to classify controls as physical, technical, logical, or administrative.

This function is associated with the Cybersecurity Architecture capability, whose essence is to place instances of controls across an enterprise's IT landscape to fulfill an organization's stated cybersecurity requirements, objectives, goals, and policies.

Further Reading:
CIS Critical Security Control 1: Inventory and Control of Enterprise Assets | CIS

Credential Issuance Mgmt.

The Credential Issuance Management cybersecurity level-1 function fundamentally refers to the systematic process of creating, distributing, and managing digital credentials leveraged for authentication and access control. It includes issuing credentials to all digital identities (human and non-human) defined in an enterprise, including their monitoring and auditing.

The quality and integrity of processes for executing this cybersecurity function are crucial due to the foundational nature of establishing and maintaining secure access to an organization's resources.

Further Reading:
Identity, Credential, and Access Management (ICAM) Strategy | U.S. Department of Defense
Plan your Microsoft Entra Verified ID issuance solution | Microsoft
OpenID for Verifiable Credential Issuance - draft 14 | OpenID Digital Credentials Protocols

Cybersecurity Risk Mgmt.

The Cybersecurity Risk Management function proactively identifies, classifies, and quantifies potential harm to an organization's digital assets based on its cybersecurity posture and the threat landscape faced by said enterprise.

The amount of potential harm (impact) and its probable materialization (likelihood) continuously evolve, as do the threat landscape (due to its dynamic nature) and a firm's protection and defense abilities. Consequently, continuously anticipating and controlling the amount of possible or actual harm an organization is willing to take (or unwillingly assumes) is the essence of this cybersecurity function.
Control is exercised by uniquely applying acceptance, reduction, avoidance, sharing, or transfer techniques, or any combination of these methods.

Cybersecurity Risk Management is a vital level-1 cybersecurity capability central to the entire model, as depicted in Figure 17 below.

Further Reading:
Integrating Cybersecurity and Enterprise Risk Management (ERM) | NISTIR 8286

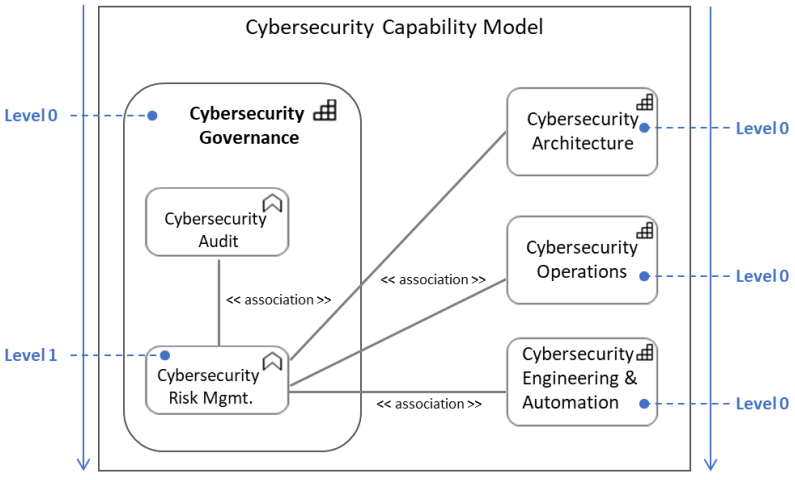


Figure 17

The significance of the level-1 Cybersecurity Risk Management capability is also underscored by its essential role in realizing the Digital Operational Resilience Act (DORA). DORA is an extensive regulatory framework instituted by the European Union to bolster the digital resilience of financial institutions. The act, to simplify, aims to stabilize and maintain the public's trust in local and broader financial systems by demanding that financial institutions can withstand, respond to, and recover from all information and technology-related disruptions and threats. At its heart, DORA is about setting up operational resilience or an organization's ability to adapt to changing conditions and withstand and recover rapidly from adverse situations, such as natural disasters, cyber attacks, and system failures. One can easily comprehend the pivotal function of cyber risk management activities when relationships between the cybersecurity capability model's elements and the operational resilience conceptual module are formally arranged, as illustrated in the figure below.

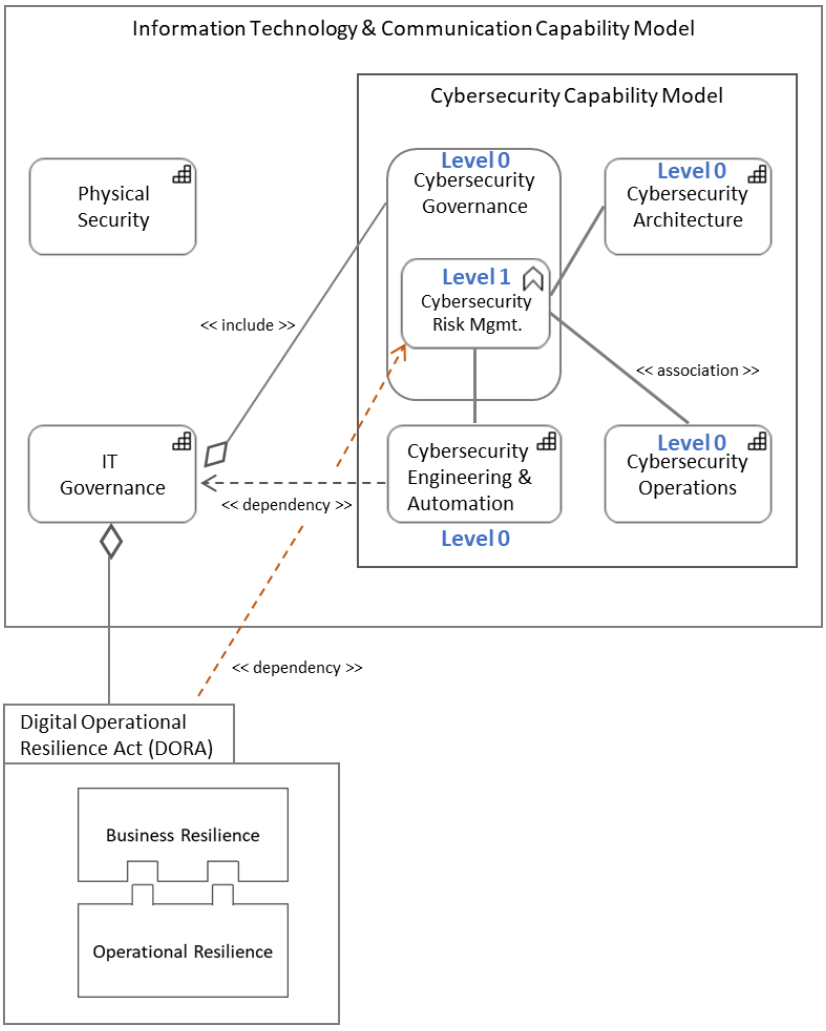


Figure 18

Cybersecurity Risk Management capability is also central to other laws and regulations (e.g., GDPR, CIP standards) designed to enhance the security and resilience of an organization's digital operations against adversarial or disruptive events.

The Cybersecurity Audit function refers to the methodical examination and review of an organization's protective, defensive, and offensive measures to safeguard its digital assets against unauthorized access and cyber threats [13].

The main objective of this function is to validate the robustness and veracity of said organization's cybersecurity posture by assessing its existing control objectives and their reification, including gaps or misalignments. This level-1 cybersecurity capability also verifies compliance with relevant regulatory, industry, and internal requirements such as laws, regulations, policies, and standards.

The output of this cybersecurity function is actionable insights for strengthening an enterprise's overall cybersecurity stance. This function is often associated with the Cybersecurity Risk Management function.

The definition inherently collapsed and included a cybersecurity assessment aspect as an intricate part of executing a cybersecurity audit. Alternatively, the assessment part can be purposefully disassociated from the audit aspect, resulting in a couple of possible relationships, as illustrated in the figure below. The original definition offered in this document mirrors the first option without explicitly calling out a level-1 or level-2 Cybersecurity Assessment capability. Readers should adjust the cybersecurity capability model to reflect the needs of the organizations they support.

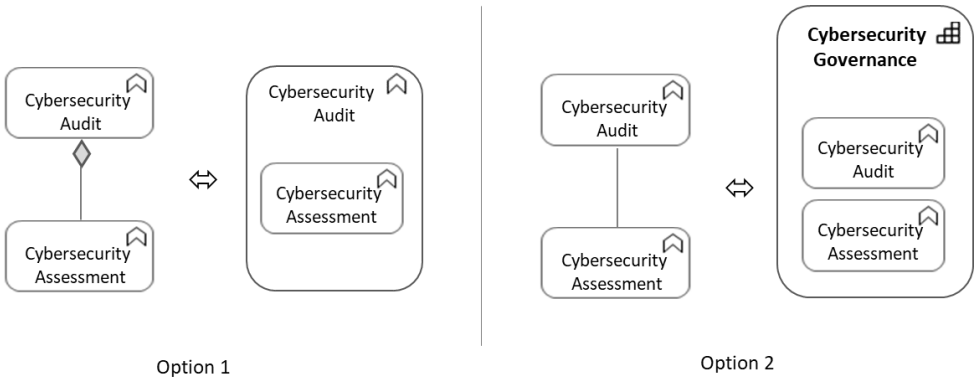


Figure 19

Please cross-reference with section 4.1. Cyberscurity Governance variations.

Further Reading:
IS Audit Basics: Auditing Cybersecurity | ISACA

2.2.2. Cybersecurity Architecture Capability – Level 1

Architecture Definition
The document adheres to the TOGAF definition of architecture, which states that architecture is "the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time." [14]

Cybersecurity architecture is often absent from cybersecurity conversations, even though it plays a pivotal role in protecting and defending an organization's digital assets. In addition to articulating the number, types, and placement of controls across an enterprise's IT landscape, cybersecurity architecture holistically and comprehensively glues risk management, information security, enterprise architecture, compliance, and business resilience into a coherent and cohesive structure [15] [16][17]. Cybersecurity architecture is most effectively defined within the broader context of enterprise architecture, as outlined earlier in this document.

The foundational cybersecurity architecture capability has 16 sub-capabilities, as depicted in the diagram to the right. This section defines each sub-capability, starting with Digital Identity Management Architecture.

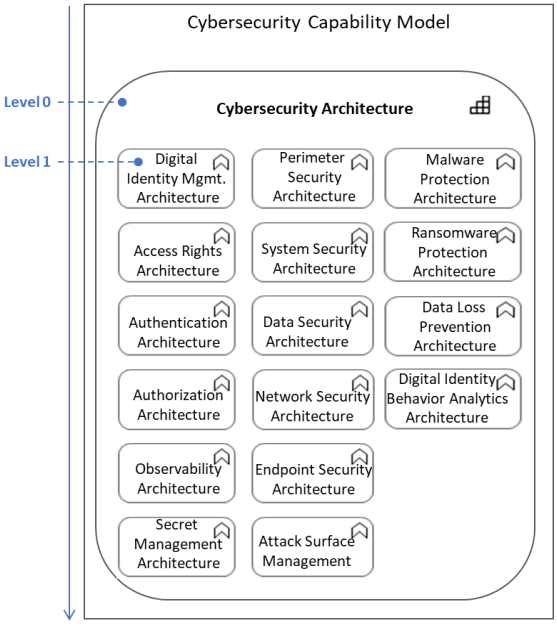


Figure 20

Digital Identity Mgmt. Architecture

This level-1 function refers to a set of design principles coupled with activities for defining, creating, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is the lifecycle management of all digital identities (human and non-human) within an organization, including but not limited to confirming their veracity, and validity. The execution of the Digital Identitiy Management Architecture function results in a series of blueprints that should preferably exhibit the following characteristics: complete functional coverage, evolvability, maintainability, reliability, usability, performance, security, interoperability, compliance with relevant standards, and cost efficiency. The quality and integrity of the architectures for reifying this cybersecurity function are essential because digital identities are one of the cornerstones for protecting and defending an enterprise's IT assets efficiently. The same architectures must also implement an organization's dedicated policies and standards for handling all digital identities.

Please cross-reference with the Digital Identity Inventory capability anchored in the Cybersecurity Governance capability.

Further Reading:
Digital identity architectures: comparing goals and vulnerabilities | arxiv.org

The Access Rights Architecture function refers to a set of design principles, frameworks, policies, and standards paired with activities for defining, creating, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is the lifecycle management, enforcement, monitoring, and auditing of access rights to an organization's IT assets by all digital identities (preferably) according to the CIA Triad. The CIA Triad is a cardinal concept in cybersecurity, standing for Confidentiality, Integrity, and Availability. Note that the lifecycle management of credentials, also known as credential issuance, may be included in the design.

Executing this cybersecurity function results in a series of blueprints that should preferably exhibit characteristics associated with architecture best practices, such as evolvability, maintainability, reliability, usability, performance, security, interoperability, compliance with relevant standards, and cost efficiency.

The quality and integrity of the architectures for reifying this cybersecurity function are essential because relevant access control policies and their enforcement mechanisms, along with digital identities, are crucial for protecting and defending an enterprise's IT assets.

The Access Rights Architecture function is associated with all cybersecurity functions anchored within the Cybersecurity Governance capability. Please refer to their definitions if necessary.

Further Reading:
Access Rights Management for the Financial Services Sector | NIST
Understanding Physical Access Control Architecture | PCSC Security
Requirements for Scalable Access Control and Security Management Architectures | Angelos D. Keromytis & Jonathan M. Smith

This function refers to a set of design principles coupled with activities for defining, creating, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is to confirm whether a digital identity genuinely belongs to an enterprise, and that said digital identity is still in a valid state.

Executing this cybersecurity function results in a distinct set of blueprints for an authentication service or module that verifies human and non-human digital identities before granting access to an organization's IT assets.

Further Reading:
Design Best Practices for an Authentication System | IEEE
OATH Reference Architecture, R2 | Open AuTHentication (OATH)

This function consists of design principles and associated activities for devising, modeling, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is to assess the right or permission (or lack thereof) granted to an organization's digital identities to access its digital IT assets. It could also incidentally include access privileges granted to digital identities or the act of granting those privileges. Executing this cybersecurity function results in a unique set of blueprints for an authorization service or module that determines which IT asset(s) a digital identity is permitted to exploit. They should exhibit characteristics associated with architecture best practices, such as evolvability, maintainability, reliability, usability, performance, security, interoperability, compliance with relevant standards, and cost efficiency.

Further Reading:
Authorization architecture | Springer

The function points to a set of design principles, frameworks, and activities for defining, developing, and maintaining conceptual, logical, and implementation architectures for a (usually complex) technology element or solution whose functional behavior is to assess or measure (ideally in a quantitative way) the internal operational health (state) of IT assets by only analyzing their external outputs such as logs or traces. The resulting outcome is a collection of distinct blueprints for a (nontrivial) observability service or module that estimates the internal condition of IT assets while they are running by solely examining the information or data they externally produce. From a cybersecurity perspective, a well-designed and robust observability service is crucial because it may affect the quality of an organization's intrusion detection ability or the effectiveness of a firm's broader threat detection and response competency.

Further Reading:
What is Observability? An Introduction | Splunk
Implementing Observability Architecture - A Practical Guide | SigNoz

Merriam-Webster defines the word secret as “something kept hidden…”. From a cybersecurity discipline perspective, it is a confidential (secret) piece of data that behaves similarly to a key to unlock protected digital IT assets. Common types of secrets include passwords, API keys, SSH keys, encryption keys, database credentials, digital certificates, tokens, and private keys. Consequently, the Secret Management Architecture function points to a set of design principles, activities, frameworks, and best practices for defining, developing, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is to securely store, manage, and control access to secrets. As with the other entries, a well-architected secret management solution is critical. Secret management is one of several building blocks for realizing a layered approach to cyber defense (also known as defense-in-depth). Managing secrets effectively throughout an enterprise is essential to avert data breaches, unauthorized access, and other cyber-related incidents. It involves securely storing secrets, controlling their access, regularly rotating them, and monitoring their usage.

Further Reading:
What is Secrets Management? | CyberArk

Perimeter Security Architecture

The Perimeter Security Architecture capability refers to a set of design principles, frameworks, policies, and standards paired with activities for defining, creating, and maintaining conceptual, logical, physical, and implementation architectures for a technology element or solution whose functional behavior is to protect an organization's boundaries (usually network wise) from unauthorized access and cyber threats.
Executing this cybersecurity function results in a series of blueprints that indicate the placement and number of physical and logical information security-related controls to create a secure barrier (with a focus on networking) around an enterprise, ensuring that only authorized digital identities (human and non-human) can access said enterprise's IT and digital resources. Perimeter Security Architecture applies to protecting and defending data centers and Cloud environments. The quality and integrity of the Perimeter Security Architecture are primordial because the latter acts as the first line of defense between a firm's (internal) corporate network(s) and the potential successful execution of external threats.
This level-1 cybersecurity capability could alternatively be part of the peer capability labeled Network Security Architecture. The document purposefully distinguishes them to emphasize the relevance of protecting and defending an organization's perimeter. Concepts such as zero-trust or identity-first security architectures do not negate the need for securing the perimeter.

Further Reading:
Perimeter networks | Microsoft
What Is Perimeter Security In Cybersecurity? | Security Forward

The internet's substitution of the central brick-and-mortar element is at the heart of digital transformation, making endpoint devices the primary medium for conducting business, as illustrated by the diagram below. As a result, digital identities became and continue to be the only factor for identifying parties with whom an organization is transacting, leaving static ways of recognizing authorized customers or vendors, such as IP addresses, as a thing of the past. However, the advent of modern security paradigms, such as zero-trust or identity-first security, does not negate the need to protect an organization's perimeter. For instance, identity-first security is a forward-thinking approach that prioritizes identities and credentials as the central element of an enterprise's cybersecurity strategy, as opposed to authorized IP addresses. Therefore, this softcover asserts that Perimeter Security Architecture capability remains a key pillar to contemporary cyber defense paradigms.

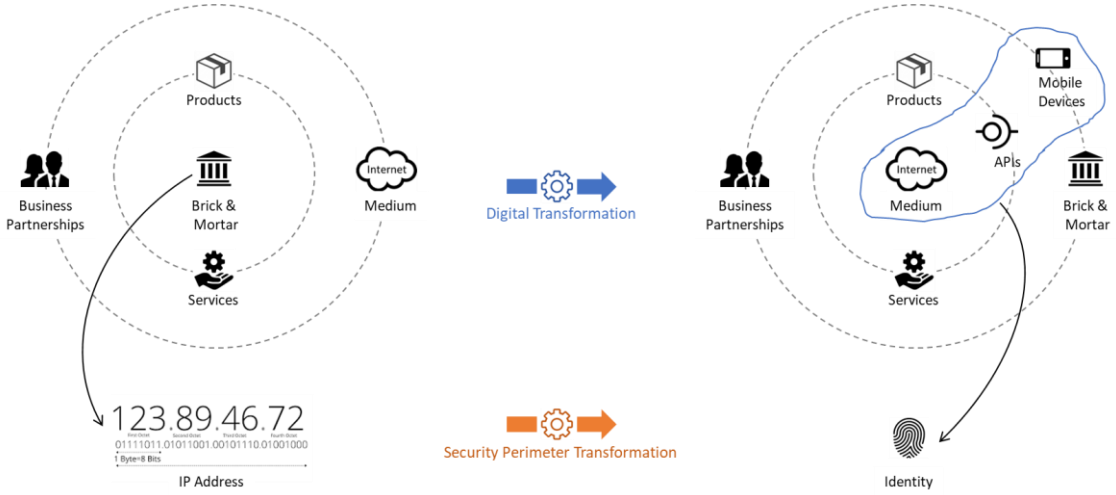


Figure 21

System (or Application) Security Architecture encompasses a set of design principles, methodologies, frameworks, policies, standards, and guidelines paired with software development activities for defining, creating, and maintaining conceptual, logical, physical, and implementation architectures for securing technology solutions against cyber threats. This function is best executed when integrated within an organization's software development lifecycle (SDLC). It includes actions such as secure coding practices, threat modeling, cybersecurity testing, vulnerability management, and the inclusion of security controls to protect technology solutions against threats and vulnerabilities.

Like Perimeter Security Architecture, the quality and integrity of System Security Architecture are paramount, as technology solutions deployed in a production environment are directly in the line of fire from cyberattacks.

This level-1 cybersecurity capabilty should be extended to Commercial off-the-shelf software.

Please cross-reference with the Cybersecurity Controls Inventory and Cybersecurity Policy Management functions anchored in the Cybersecurity Governance capability.

Further Reading:
Complete Guide to Application Security: Tools, Trends & Best Practice | Snyk
What is application security (AppSec)? | IBM
Five Key Components of an Application Security Program | ISACA

Data Security Architecture encompasses a comprehensive set of design principles and associated activities aimed at devising, modeling, and maintaining conceptual, logical, and implementation architectures to safeguard (inherently including data encryption) data and information throughout their entire lifecycle—from creation to disposal. This cybersecurity function operates within the context of the CIA Triad (Confidentiality, Integrity, and Availability), regulatory requirements, and an organization's policies and data classification standards.
In this document, the terms "data" and "information" refer to digital records of facts or events generated during the execution of an organization's business mission, commonly known as the course of business. Digital events include but are not limited to personal identifiable information (PII), intellectual property, personnel, financial, customer, vendor, partner, or operational facts pertinent to the running of said enterprise.

Executing this cybersecurity function results in a distinct set of blueprints that capture the number, nature, type, and placement of cybersecurity controls to protect and defend a firm's entire digital terrain from adversarial events. Examples of cybersecurity controls include the deployment of encryption, access controls, data masking, and data loss prevention (DLP) mechanisms, as well as the establishment of governance policies and procedures to manage data security. Like any architectural work product, outputs from this cybersecurity function should exhibit characteristics associated with best practices, such as evolvability, maintainability, reliability, usability, and performance.

cont.

Data Security Architecture

cont.

In summary, Data Security Architecture's main objective is to prevent, reduce, and/or mitigate risks related to data or information breaches while complying with regulatory and an enterprise's internal requirements.

Lastly, as illustrated in the diagram below, (data) backup architecture may be considered by some individuals as an integral component of the overall data security architecture.

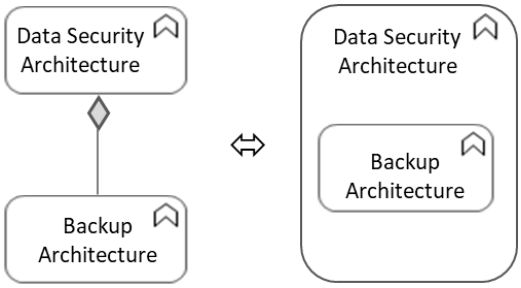


Figure 22

Further Reading:

How to Successfully Design and Implement a Data-Centric Security Architecture | Gartner

Data Security | NIST's National Cybersecurity Center of Excellence

Data security and protection solutions | IBM

SP-013: Data Security Pattern | Open Security Architecture

The Data Security Architecture Level-1 cybersecurity capability is not only crucial but intricate to implement correctly, given its high interdependency level, as illustrated in the accompanying figure below.

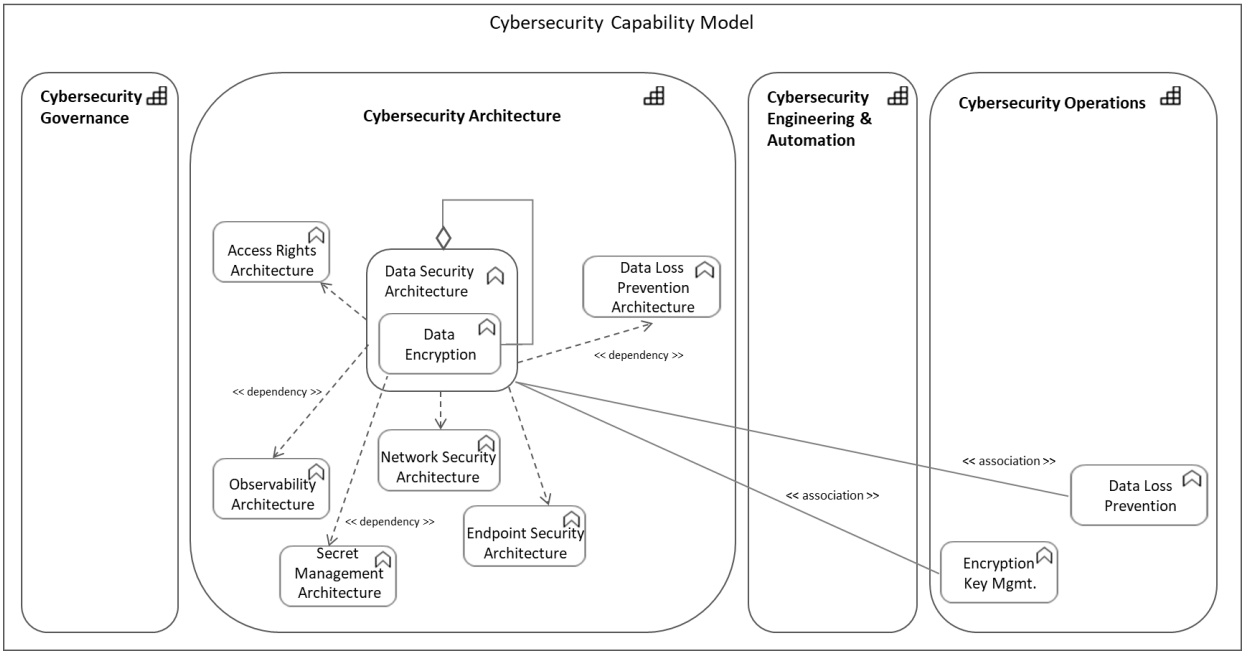


Figure 23: Key interdependencies

There is an undeniable relationship between data protection and having a robust mechanism to backup and restore said data in the event of an adverse event. However, this document opines that (data) backup architecture should be treated in the context of operational continuity as opposed to being included as an element of the cybersecurity discipline. The diagram below offers a possible framework for defining business resilience to reify the European Digital Operational Resilience Act (DORA). While the DORA implementation is the subject of another publication, this softcover places the (data) backup function (architecture & operations) as part of an organization's ability to maintain essential functions during and after a disruptive event, also known as business continuity.

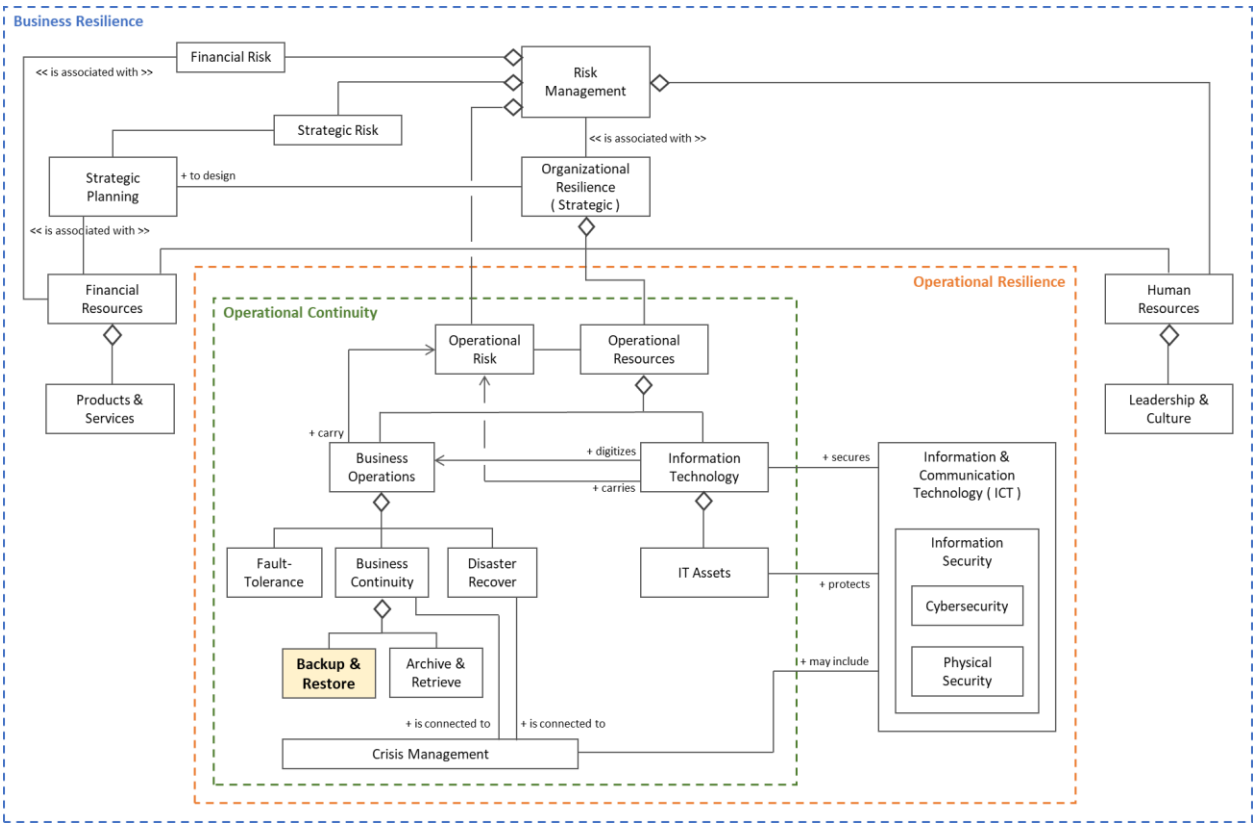


Figure 24

[Intentionally left blank for formatting purposes]

The function consists of design principles, frameworks, and associated proactive activities aimed at devising, modeling, and maintaining conceptual, logical, and implementation architectures to safeguard an organization's corporate network from adverse cyber events, including resisting and defeating such events to the extent possible.

Executing this level-1 cybersecurity function results in a distinct set of blueprints that capture the number, nature, type, functional behavior, and placement of network-focus cybersecurity controls to protect and defend a firm's entire network from cyber threats and attacks. Examples of network-centric cybersecurity controls include firewalls, intrusion detection and prevention systems (IDS/IPS), honeypots, network address translation (NAT), virtual private networks (VPNs), network access controls (NACs-IEEE 802.1X), and encryption protocols, to name a few. Network policies, procedures, standards, and guidelines supplement technical controls while guiding the outputs related to fulfilling the Network Security architecture function.

Network Security Architecture is related to the Observability Architecture function. Well-architected, network-focused observability blueprints are essential for adequately monitoring all events across a corporate network. The act of monitoring is actually performed by several cybersecurity functions within the Cybersecurity Operations capability.

Like Perimeter Security Architecture and System Security Architecture, the quality and integrity of Network Security Architecture are paramount, as corporate networks are directly in the line of fire from cyberattacks.

In summary, the primary objective of Network Security Architecture is to protect an enterprise's network infrastructure from cyber threats, prevent breaches, and ensure compliance with regulatory and an organization's internal requirements. Additionally, it contributes to an enterprise's overall cybersecurity posture and is part of a defense-in-depth strategy.

Further Reading:
Network Security Architecture | Check Point
What are the elements of modern network security architecture? | TechTarget
Guide to a Secure Enterprise Network Landscape | NIST SP 800-215

[Intentionally left blank for formatting purposes]

Endpoint Security Architecture refers to design principles, frameworks, and associated proactive activities aimed at devising, modeling, and maintaining conceptual, logical, and implementation architectures to protect most currently known endpoint devices within an organization's network.

Executing this cybersecurity function results in a series of blueprints and artifacts encompassing a range of strategies, technologies, technical controls, and policies aimed at safeguarding endpoints from cyber threats while maintaining compliance with regulatory and a firm's internal requirements. This level-1 cybersecurity function is related to the Observability Architecture function, like Network Security Architecture.

Technical control examples include endpoint protection platforms (EPP), endpoint detection and response (EDR) solutions, encryption, access controls, and continuous monitoring. Non-technical controls may involve device management policies, for instance.

The main objective of this cybersecurity function is to secure endpoints against unauthorized access, malware, and other cyber threats. Additionally, it contributes to an enterprise's overall cybersecurity posture and is part of a defense-in-depth strategy.

Further Reading:
What is Endpoint Security | CrowdStrike
The Importance of Endpoint Security in the Evolution of Modern Security Architecture | ESG
What Is Endpoint Security? How Does It Work? | Fortinet

The Attack Surface Management function refers to methodologies, frameworks, policies, procedures, standards, guidelines, formulas, plans (e.g.: mitigation, response, etc.), and tools paired with proactive activities for identifying, analyzing, and reducing all potential entry points (attack surfaces) through which threat actors could infiltrate an organization's digital environment. It includes external and internal digital assets, network interfaces, applications, and any exposed services, to name a few examples.

Executing this cybersecurity function results in a series of blueprints and plans to minimize an enterprise's attack surface and strengthen its overall security posture. Proactively managing the attack surface is a fundamental aspect of a robust cybersecurity strategy, enabling organizations to stay in front of cyber threats and shield their digital assets. This level-1 cybersecurity function is related to the Observability Architecture function, like Network Security Architecture.

Note that the monitoring aspect of Attack Surface Management is performed by several cybersecurity functions within the Cybersecurity Operations capability, such as Threat Detection & Response, Threat Hunting, or Digital Identity Monitoring.

Further Reading:
What is Attack Surface Management | CrowdStrike
What is Attack Surface Management |IBM
What is Attack Surface Manageemnt | Palo Alto Networks
Microsoft Defender External Attack Surface Management | Microsoft

Malware Protection Architecture

This softcopy defines malware as a broad range of software that is designed to [1] cause intentional harm to systems, devices, and/or networks, [2] gather and exfiltrate data or information, [3] provide unauthorized access to an organization's digital IT assets, or [4] take a range of actions that an enterprise may not want to occur.
Malware is polymorphic and comes in various forms, including viruses, worms, trojans, ransomware, spyware, rootkits, keyloggers, and botnets, to name common shapes.

Therefore, Malware Protection Architecture refers to design principles, frameworks, best practices, and associated activities aimed at proactively devising, modeling, and maintaining conceptual, logical, and implementation architectures to defend an organization's digital IT assets against malicious software (malware). This level-1 cybersecurity function is also related to the Observability Architecture function.

Executing this cybersecurity function results in a distinct set of blueprints that capture the number, nature, type, functional behavior, and placement of cybersecurity controls designed to detect, prevent, and respond to malware threats. Malware-specific policies, procedures, and response plans supplement dedicated anti-malware technical controls.

Further Reading:
How to Build an Effective Malware Protection Architecture | Gartner
Malware Protection | Bitdefender TechZone
Improving Malware Protection Maturity by Using Attack Scenarios | Gartner

Ransomware Protection Architecture

Ransomware is a type of malicious software that seizes control of a computer or device and demands payment for its release. There is no singular type of ransomware, but all ransomware has the following common characteristics:

- It is a malicious software program
- It is secretly placed onto a victim's computer(s) or device(s)
- It encrypts files
- It asks for a ransom to provide decryption key(s)

Ransomware Protection Architecture encompasses design principles, frameworks, best practices, and associated activities aimed at proactively devising, modeling, and maintaining conceptual, logical, and implementation architectures to protect an organization's digital IT assets from being encrypted by adversaries and rendered inoperative. Architecture artifacts must contain the number, nature, type, functional behavior, and placement of all preventive, detective, and corrective controls that collaboratively protect against ransomware.
Cybersecurity control instances may include advanced endpoint protection solutions, regular data backups, and robust access controls. Theat intelligence, security awareness training, and security assessments could supplement these technical controls.

This cybersecurity function could have been integrated with the Malware Protection Architecture function, as ransomware is a type of malware. However, due to the specific nature of ransomware and the unique preparations required to defend against such threats, this document has opted to address it separately, as highlighted in Roger A. Grimes' seminal book, Ransomware Protection Playbook (published by Wiley).

Data Loss Prevention Architecture

Data Loss Prevention (DLP) Architecture refers to design principles, frameworks, best practices, and associated activities aimed at proactively devising, modeling, and maintaining conceptual, logical, and implementation architectures to protect an organization's data and information in all states (whether in use, in motion, or at rest) while ensuring authorized access and preventing unauthorized use or exfiltration.

Executing this cybersecurity function results in a distinct set of blueprints that capture the number, nature, type, functional behavior, and placement of cybersecurity controls designed to safeguard sensitive data or information and prevent it from leaving the confines of an organization.
Cybersecurity control instances may include Data Loss Prevention solutions, data movement monitoring, enforcing security policies, and providing alerts for potential data breaches. This level-1 cybersecurity function is related to the Observability Architecture function.

Consider leveraging the DLP Architecture cybersecurity function to help establish operational resilience, as defined in the Digital Operational Resilience Act (DORA), for example.

Further Reading:
Understanding Data Loss Prevention Architecture | Stracker
Data Loss Prevention: Comparing Architecture Options | Gatner
Data Loss Prevention | NIST

Digital Identity Behavior Analytics Architecture

The Digital Identity Behavior Analytics Architecture function refers to design principles, frameworks, best practices, and associated activities aimed at proactively devising, modeling, and maintaining conceptual, logical, and implementation architectures to monitor and analyze behaviors associated with an organization's digital identities. This architecture function aims to define a technology solution that allows an enterprise to proactively detect digital identities' behavior deviations and subsequently investigate whether these behavior deviations are signs of possible threats or the product of existing breaches.

Executing this cybersecurity function results in a distinct set of blueprints that capture the number, nature, type, functional behavior, and placement of cybersecurity controls designed to record and collect data associated with digital identities' activities. This level-1 cybersecurity function is also related to the Observability Architecture function

In practice, architecture blueprints must depict integration with a behavior analytics service, identity & access management (IAM) provider, and a real-time monitoring & alert mechanism, to name a few.

This level-1 cybersecurity capability may alternatively not be limited to digital identities.

To close this section, the document contends that Cloud environments and data centers share the same underlying technological construct or fabric, setting aside the financial impact on an organization's balance sheet and income statement. The key distinction lies in the mechanism (or form) in which associated information and communication technology (ICT) services are delivered and consumed.

The diagram below compares the structures of a generic data center and a Cloud environment, aligning their respective fabrics with the ArchiMate layers. This architectural alignment highlights that, regardless of the operating industry, both share similar control objectives. These objectives are realized through functionally equivalent technical controls, systematically organized within comparable cybersecurity architecture blueprints, which are likely shaped by shared architecture and design principles. As such, this document asserts that all level-1 cybersecurity sub-capabilities within the foundational (level-zero) Cybersecurity Architecture element are equally applicable to data centers and Cloud environments.

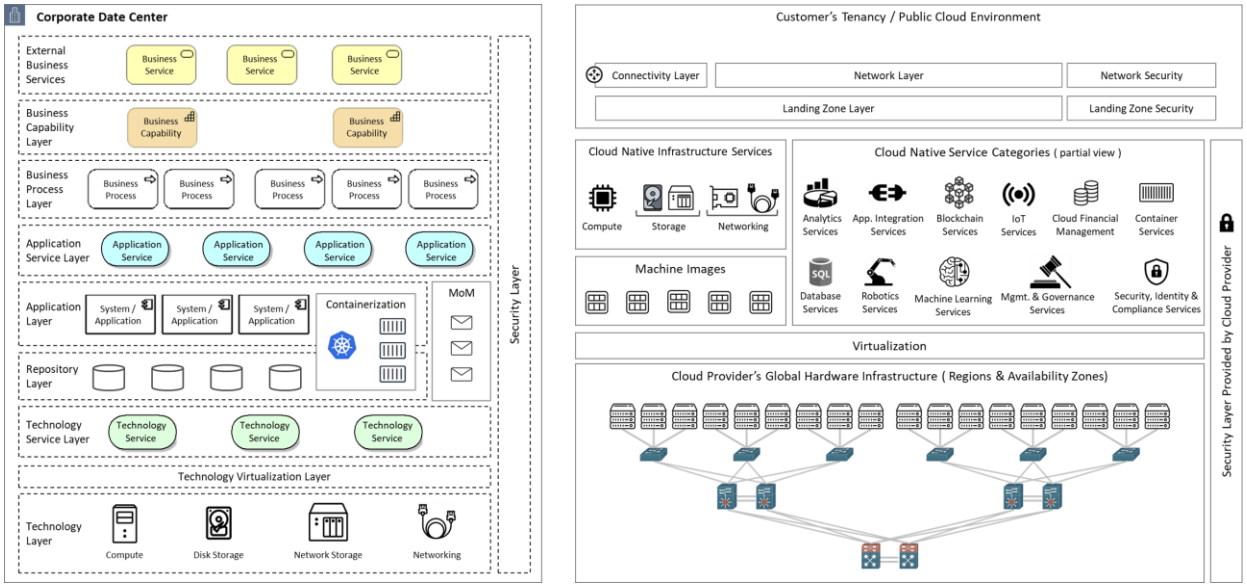


Figure 25: Data Center vs. Cloud Construct – a side-by-side comparison

Additional visuals highlighting alignments between a typical Coud environment and a data center construct along ArchiMate layers are available in sections 5.5 and 5.6 of the Appendix.

2.2.3. Cybersecurity Engineering & Automation Capability – Level 1

The Cybersecurity Engineering & Automation capability contains seven level-1 cybersecurity functions, as illustrated in the figure to the right. It is recognized that image hardening could be placed outside the parent cybersecurity capability, like hardware hardening. Readers leveraging this material to develop their custom cybersecurity capability model will need to decide where to place Image Hardening. In the meantime, this softcopy anchors it within the cybersecurity discipline. Also, note the associative relationship between the Image and Hardware Hardening cybersecurity functions.

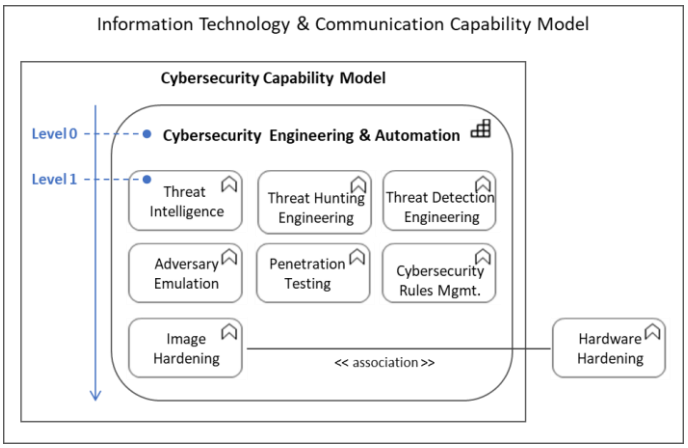


Figure 26

Threat Intelligence

This level-1 function involves collecting cybersecurity-related raw data from internal and external sources, which is then analyzed to infer relevant information and derive actionable intelligence. It specifically entails researching and analyzing the collected raw data to establish fresh trends, unmask new technical developments, and uncover novel indicators of compromise, tactics, techniques, or procedures to provide an understanding of potential threat events and related threat actors. The essence of Threat Intelligence is to discover actionable knowledge that enables an organization to determine the appropriateness of controls to mitigate cyber threat events and possibly stay one step ahead of adversaries. Note that this cyber function includes intrusion analysis. In practice, the industry in which an organization operates is a relevant factor, among several others, to consider when executing this cyber function.

Further Reading:
What Is Threat Intelligence? | A Complete Overview | Zscaler
Cyber Threat Intelligence: A Comprehensive Guide | Palo Alto Networks

Threat Hunting Engineering

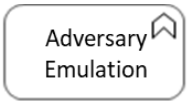
This document distinguishes Threat Hunting from Threat Hunting Engineering. Threat Hunting Engineering focuses on preparing and honing the logistics (via engineering, data, and automation techniques) required to successfully and continuously carry out the Threat Hunting function. Tacking the word Engineering is purposeful and signifies some scientific method when executing threat hunting. Threat hunting involves scrutinizing data, identifying unusual patterns, discovering suspicious activities, and investigating anomalies to uncover hidden threats and prevent some exploitation before they cause harm. Please cross-reference with the definition of the Threat Hunting function.

Further Reading:
Scientific Method | Wordnik
Learn Threat Hunting & Detection Engineering | MITRE

This document distinguishes Threat Detection & Response from Threat Detection Engineering. Threat Detection Engineering (also known as Detection Engineering) focuses on preparing and honing the logistics (via engineering, data, and automation techniques) required to successfully and continuously carry out the Threat Detection & Response function. Tacking the word Engineering is purposeful and signifies some scientific method when executing threat detection and responding to any threat that may harm an organization's digital assets.

Activities associated with the Threat Detection & Response function include but are not limited to designing and implementing analytics to discover malicious activities coupled with other automated techniques, such as tuning existing controls. Executing this function is part of a foresighted defense to reduce incident response time in an ever-evolving threat landscape. Please cross-reference with the definition of the Threat Detection & Response function.

Further Reading:
Scientific Method | Wordnik
Detection Engineering Explained | Splunk
What is Detection Engineering | CrowdStrike
Purple Teaming and Threat-Informed Detection Engineering

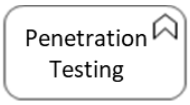


One of the challenges associated with the term Adversary Emulation is that a standard definition has yet to emerge to codify it. This document defines this function as imitating, impersonating, duplicating, or simulating tactics, techniques, and procedures (TTPs) used by real-world adversaries to test and improve an organization's cybersecurity posture. The level of exactness and precision in emulating adversaries' behavior or operations is the subject of vigorous debates in the cybersecurity community. The words to define this set of activities (imitation vs. impersonation vs. duplication vs. simulation) reflect the wealth of opinions regarding the essence of adversary emulation.

Threat Emulation, Purple Teaming, or Red Teaming are synonyms often used to describe the same concept(s) linked to Adversary Emulation.

This document does not equate penetration testing with adversary emulation. Both are crucial in evaluating and improving an organization’s cybersecurity capabilities.

Further Reading:
How Purple Team Can Use Continuous Adversary Simulation | SANS
Adversary Emulation and Red Teaming | MITRE
What is Adversary Emulation? | Picus Security



Penetration testing, commonly known as pen testing, is a set of predefined and well-scoped activities focused on unmasking, identifying, and exploiting vulnerabilities (including entry points) in specific IT assets. One of the main objectives of penetration testing is to evaluate the effectiveness of existing cybersecurity controls that protect an organization's specific IT assets by using various techniques, such as attempting to gain unauthorized access, escalate privileges, or extract sensitive information. Another key goal is to prevent the exploitation of uncovered vulnerabilities by threat adversaries.
Unlike adversary emulation, penetration testing does not imperatively leverage tactics, techniques, and procedures (TTPs) and does not try to assess an organization's overall cyber resilience. It only looks for specific weaknesses in targeted IT assets.

The output of this function is a set of actionable recommendations for enterprises to strengthen their cybersecurity posture.

This document does not equate penetration testing with adversary emulation. Both are crucial in evaluating and improving an enterprise's cybersecurity capabilities.

Further Reading:
NIST Glossary
What is penetration testing? | What is pen testing? by CLOUDFLARE
What is penetration testing? | IBM
Penetration Testing | BLACKDUCK

The Cybersecurity Rules Management function proactively defines, develops, implements, monitors, and maintains policies and procedures to protect and defend an organization's IT assets from cyber threats. These policies and procedures span the entire Open Systems Interconnection (OSI) model, covering all respective IT assets and their classes.

Automation has recently gained traction in realizing this function and is labeled Security Policy Automation. The latter is often associated with Policy as Code, which consists of expressing security policies in code, making them enforceable, verifiable, and integrated with agile software development techniques.

Image Hardening is the systematic process of securing virtual images (virtual machine images, container images, OS images) by configuring them to adhere to established security standards and best practices. It includes applying patches, making inoperative unnecessary services, configuring access controls, and using other measures to mitigate vulnerabilities and protect virtual images from cyber threats. Strengthening virtual images allows organizations to substantially boost their security stance and minimize the chances of being exploited by malicious entities.

Further Reading:
CIS Hardened Images® | Center for Internet Security

To conclude this section, one could challenge whether Development Security and Operations (DevSecOps) should be a level-1 cybersecurity capability and added to the model. Historically, the Development and Operations (DevOps) technical movement was initially created to bridge the gap between development and IT operations, enhancing collaboration and speeding up the delivery pipeline. However, as cyber threats became more sophisticated and frequent, it became evident that security needed to be integrated seamlessly within this framework. Subsequently, DevSecOps emerged as a natural progression, aiming to "shift left" security, meaning security is addressed at the earliest stages of the development process, as illustrated in the figure below. This document asserts that the DevSecOps technical movement is not a core cybersecurity capability and purposefully decided to exclude it from the model. Readers should feel free to disagree with this stance and integrate this imaginable level-1 cybersecurity capability within either the Cybersecurity Architecture or Cybersecurity Engineering & Automation foundational (level-zero) capability.

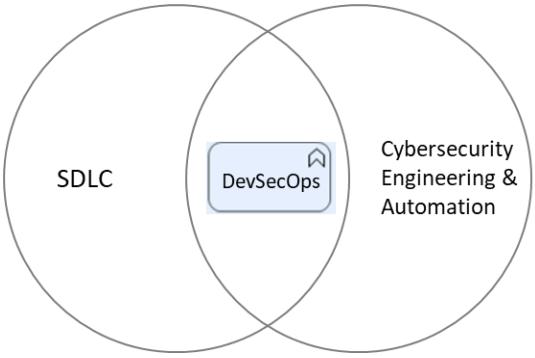


Figure 27

[Intentionally left blank for formatting purposes]

2.2.4. Cybersecurity Operations Capability – Level 1

Cybersecurity operations are fundamental to protecting an organization's digital assets, maintaining business continuity, and safeguarding it against a litany of risks linked to strategy and operations. As cyber threats continue to increase in frequency and potency, the importance of robust cybersecurity operations will only grow, making it a critical component of any successful organization. The cybersecurity capability model presented in this document offers 12 level-1 cybersecurity functions under the parent and foundational Cybersecurity Operations capability, as illustrated in the Figure to the right. They are:

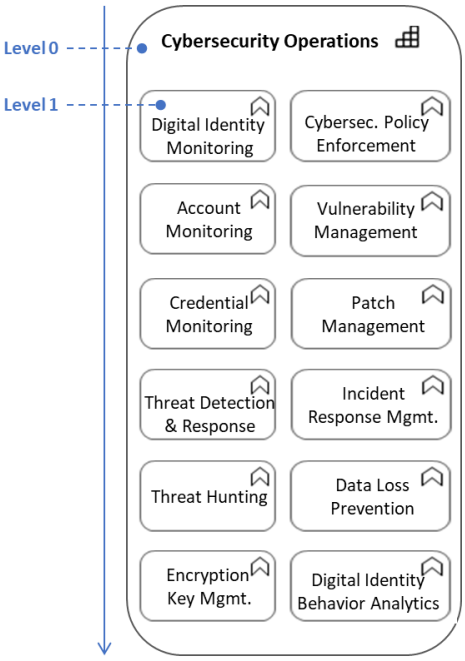


Figure 28

1. Digital Identity Monitoring
2. Account Monitoring
3. Credential Monitoring
4. Threat Detection & Response
5. Threat Hunting
6. Encryption Key Management
7. Cybersecurity Policy Enforcement
8. Vulnerability Management
9. Patch Management
10. Incident Response Management
11. Data Loss Prevention
12. Digital Identity Behavior Analytics

Their definitions follow next.

Digital Identity Monitoring is a collection of frameworks, policies, standards, procedures, activities, and tools to proactively and continuously track a firm's digital identities' actions across its entire IT landscape to detect, prevent, and respond to potential abnormal or unauthorized behaviors paired with indications of compromise.
The analytic aspect of surveilling digital identity has intentionally been removed from this level-1 cybersecurity function to be explicitly defined by the Digital Identity Behavior Analytics cyber function. Readers wanting to create their cybersecurity capability model can certainly collapse the analytic dimension of monitoring digital identities into the Digital Identity Monitoring function and eliminate the Digital Identity Behavior Analytics one.

The Digital Identity Monitoring cybersecurity function is not only a cornerstone of any robust cybersecurity strategies, but it is also, as detailed in this document, closely connected to (at a minimum) the following level-1 elements of the model:

- Digital Identity Inventory
- Digital Identity Behavior Analytics
- Threat Intelligence
- Threat Detection & Response

One of Merriam-Webster's definitions of Account is "an arrangement in which a person uses … services of a particular company." In the context of this document, an account refers to an agreement between an organization and its employees or authorized parties, represented as digital identities, to effectively utilize business, application, data, technical, or technology services offered by IT assets belonging to the organization.

Therefore, Account Monitoring refers to the proactive and continuous surveillance of all account activities within an organization's IT environment to detect abnormal or malicious behaviors, unauthorized access attempts, and potential cybersecurity threats. This function involves tracking login patterns, monitoring access to all IT assets, analyzing digital identities' behaviors, and generating alerts for suspicious activities, among other forms of supervision.

In summary, the objective is to proactively safeguard accounts from compromise by detecting uncommon behavior patterns, ensure compliance with an organization's cybersecurity policies, and protect the broader enterprise from harm should an account be compromised.

This cybersecurity function is closely related to the Account Inventory function, which is included in the broader Cybersecurity Governance capability.

Further Reading:
What is Account Monitoring | ReasonLabs
Account Monitoring and Management Guideline | UC Berkely
Critical Control 16: Account Monitoring and Control | Rapid 7

This document defines Credential(s) as a set of verification data used to authenticate and authorize an organization’s digital identities before they are allowed to exploit IT assets of said enterprise.

Therefore, Credential Monitoring refers to the proactive and continuous surveillance of the utilization and status of all credentials (e.g., usernames, passwords, and access tokens) within an organization's IT ecosystem to detect abnormal or unauthorized use of verification data to access IT assets, including credential theft.

Discharging this function involves automated tools and techniques to efficiently and cost-effectively monitor login attempts, detect compromised credentials, assess the risk of credential exposure, and ensure compliance with the organization's cybersecurity policies.

This Crential Monitoring is closely related to the Credential Issuance Management function, which belongs to the broader Cybersecurity Governance capability.

Further Reading:
Detecting Compromised Credentials: A Comprehensive Guide | Silverfort
Third-Party Compromised Credential Monitoring | Intel 471
What is Credential Theft? | SentinelOne

This cybersecurity function is the operationalization of Threat Detection Engineering, which belongs to the Cybersecurity Engineering and Automation cyber capability. Threat Detection & Response has three key facets. The first facet is a body of practices centered on proactively monitoring and analyzing digital activities across an organization's entire IT landscape. The intent is to discover and/or identify abnormal events, whether unrecognized or already known (threat detection).
The second aspect concentrates on investigating said unusual events to uncover suspicious and potentially or actual harmful behavior (threat investigation).
The third facet involves executing mitigation actions to contain the impact of questionable events once their unsafe nature has been confirmed. Containment processes are followed by threat removal activities until recognized or normal digital behavior patterns are again observed (incident response).

The effectiveness of the Threat Detection & Response function is related to the level of automation achieved during the preceding and preliminary engineering phase (Threat Detection Engineering).

Further Reading:
What Is Threat Detection and Response (TDR)? | Microsoft
What is Threat Detction and Response (TDR)? | CrowdStrike
What is Threat Detction and Response (TDR)? | Fortinet

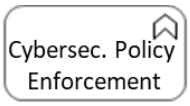
Several different understandings of the term Threat Hunting exist within the Information Security community. This document defines this function as a proactive, as opposed to reactive, approach to detecting and investigating suspicious and potentially malicious activities to uncover existing but hidden and unknown vulnerabilities or threats in an organization's IT ecosystem.

This cybersecurity function focuses on operationalizing Threat Hunting Engineering, which belongs to the Cybersecurity Engineering and Automation cyber capability. It includes selecting and reifying hypotheses, collecting and analyzing data, unmasking new anomaly patterns, and identifying matching tactics, techniques, and procedures.
The creation and dissemination of documentation regarding newly uncovered vulnerabilities or threats are next. Recorded findings are paired with remediation steps taken to address freshly discovered deficiencies before their exploitation by adversaries.

The effectiveness of the Threat Hunting function is related to the level of automation achieved during the preceding and preliminary engineering phase (Threat Hunting Engineering).

Further Reading:
What Is Threat Hunting? | Fortinet
What is threat hunting? | Cloudflare
What is threat hunting? | IBM

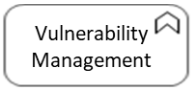
The Encryption Key Management function *"is the administration of policies and procedures for protecting, storing, organizing, and distributing encryption keys. Encryption keys (also called cryptographic keys) are the strings of bits generated to encode and decode data and voice transmissions. Effective encryption key management is crucial to the security of land mobile radio (LMR) communications and the sensitive information those communications contain. In addition to ensuring security, key management also ensures that encryption does not impede the interoperability of LMR systems and radios within and among agencies."* Source: Cybersecurity and Infrastructure Security Agency (CISA), Encryption Key Management Fact Sheet.



Cybersecurity Policy Enforcement refers to applying and monitoring adherence to an organization's defined cybersecurity policies (including Policy as Code) by deploying technical controls, administrative procedures, and behavioral guidelines. Executing this cybersecurity function includes, for instance, activities such as access control, monitoring user activities, conducting regular audits, and using automated tools to ensure that cybersecurity policies are consistently applied and enforced across all systems and users.

The primary goal of this function is to reify the CIA Triad to the extent defined by cybersecurity policies and ensure compliance with regulatory and an enterprise's internal cybersecurity requirements.

Further Reading:
Cybersecurity Policy Enforcement: Strategies for Success | TrustedSec



Vulnerability Management is the durable, proactive, and comprehensive approach to identifying, evaluating, treating, and reporting cybersecurity vulnerabilities for all IT assets owned, leased, or rented by an organization and across the Open Systems Interconnection (OSI) model.

This cybersecurity function is critical for maintaining or improving an enterprise's cybersecurity posture over time. It also helps reduce opportunities for said cyber-related flaws to be exploited by threat actors. It is also closely related to the Patch Management cyber function.

Practically, Vulnerability Management must adopt automation to be effective.

Note that this Level-1 cybersecurity function is closely linked to the Threat Intelligence function, which is anchored in the Cybersecurity Engineering & Automation capability.

Further Reading:
What is vulnerability management? | Microsoft
What is Vulnerability Management? | CISCO
What is Vulnerability Management? | Palo Alto Networks

Additionally, vulnerability management is closely tied to the goals of an enterprise's risk management program, and understanding that this level-1 cybersecurity function exists at the crossroads of vulnerability, threat, and risk is primordial to safeguard an organization's digital assets effectively. More specifically, vulnerability management is always confined within the risk boundary and can never be greater than the risk dimension itself because risk incorporates vulnerability. Indeed, risk assessment considers the existence of vulnerabilities paired with the likelihood and impact of threats exploiting these vulnerabilities. Without considering threats and their impact, the concept of risk would be incomplete. Consequently, vulnerability management is essentially a subset of risk management.

Figure 29

Vulnerability management is evolving to become a more strategic function to adapt to the pace and sophistication of cyber threats. Conventional vulnerability management often focuses on identifying and patching all vulnerabilities regardless of their potential impact. While this method provides a baseline level of security, it can be inefficient and overwhelming, especially for organizations with limited resources. Conversely, Risk-Based Vulnerability Management (RBVM) is a forward-thinking approach that prioritizes vulnerabilities based on the verifiable risk they pose to an enterprise. This document opines that Risk-Based Vulnerability Management is likely paving the way for the Future of cybersecurity.

[Intentionally left blank for formatting purposes]

Patch Management

In its simplest form, a patch is an update. In computer science, a patch is usually a change in the source code of a specific software component, such as the kernel, a service, or a bespoke piece of software. Patches may address existing security problems, service upgrades, or coding errors (bugs) in software deployed in an enterprise.

Patch Management refers to activities (identify, acquire, test, and install), processes, and procedures for applying updates to any software component across an organization's entire IT landscape.

This cybersecurity function is closely related to vulnerability management because patches are often applied to close cyber-related deficiencies or gaps.

Practically, Patch Management must embrace automation to be effective.

Further Reading:
What is patch management? Lifecycle, benefits and best practices | TechTarget
What is Patch Management | CrowdStrike
What is patch management (and automation)? | RedHat

Incident Response Mgmt.

NIST SP 800-61 Rev. 2 defines an event as "any observable occurrence in a network or system." An incident, however, is a specialized event that threatens or may threaten the confidentiality, integrity, or availability (CIA Triad) of an organization's digital IT assets, including the data and information stored or transmitted by those assets.
Consequently, Incident Response Management refers to the set of practices, contingency plans, frameworks, coordinated processes, synchronized activities, and tooling required for an organization to defend itself after identifying incidents or their materialization into intrusions, breaches, or exploits.

The primary goal of the Incident Response Management function is to prepare an enterprise to defend against any incident, regardless of its state. Preparation requires the readiness of policies and response plans to effectively lead a firm through defeating cyber adversaries. Incident response planning is a fundamental element of the overall field of business continuity management. Some organizations use the term "incident response" to describe readiness activities, while "crisis management" depicts the execution of a response plan. However, this document does not make such a distinction.

This function aims to reduce the impact of incidents so organizations can resume their interrupted business operations as soon as possible.

Always prioritize the protection of life when responding to an incident. When making decisions about priorities, ensure that safety is the foremost consideration.

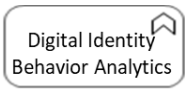
Further Reading:
Incident Response | NIST

Data Loss Prevention (DLP) refers to a collection of practices, inspection techniques, and tools used to proactively and continuously protect, detect, and prevent access to data or information from unauthorized access, use, exfiltration, or unwanted destruction, especially when data or information is sensitive.

DLP's main objective is to protect sensitive data and information, like personally identifiable facts, financial records, intellectual property, and other vital business knowledge, from unauthorized access, use, or transmission.

DLP also includes policies and processes designed to ensure that data or information remains within an organization's digital boundaries and is not lost, misused, or accessed by unauthorized digital identities.

Further Reading:
What is Data Loss Prevention (DLP)? | CrowdStrike
Data Loss Protection | Gartner Glossary
What Is Data Loss Prevention (DLP)? | Palo Alto Networks



Digital Identity Behavior Analytics (DIBA) is an advanced methodology that combines digital identity with behavioral analytics to bolster cybersecurity. It involves continuously tracking and analyzing digital identities' behaviors relating to verified deviations from routine patterns, detecting potential security threats, and ensuring the integrity and security of digital IT assets. DIBA demands using advanced analytics tools and techniques to monitor digital identities' activities, assess risk levels, and implement proactive measures to prevent unauthorized access and data breaches.

This document recognizes that advanced and behavioral analytics can also be effectively applied to various organizational entities and business functions to strengthen an enterprise's overarching cybersecurity posture. For example, in the context of financial transactions, modern analytics techniques excel at detecting anomalies or preventing fraudulent activities. Consequently, readers are encouraged to incorporate behavioral analytics level-1 elements when tailoring the Cybersecurity Capability model to meet the specific needs of the organizations they support.

Further Reading:
Adaptive Authentication and Behavior Analytics | The Identity Management Institute

2.2.5. Level-1 Cybersecurity Capability Model & the NIST Cybersecurity Framework 2.0

Section 2.1 of this softcopy mapped the foundational or level-zero cybersecurity capabilities to the NIST Cybersecurity Framework 2.0. This sub-section maps the level-1 cybersecurity functional behaviors to the same NIST frame of reference, highlighting the strong link between both work products. The interconnect between both frameworks can be leveraged to develop NIST-aligned cybersecurity strategies.

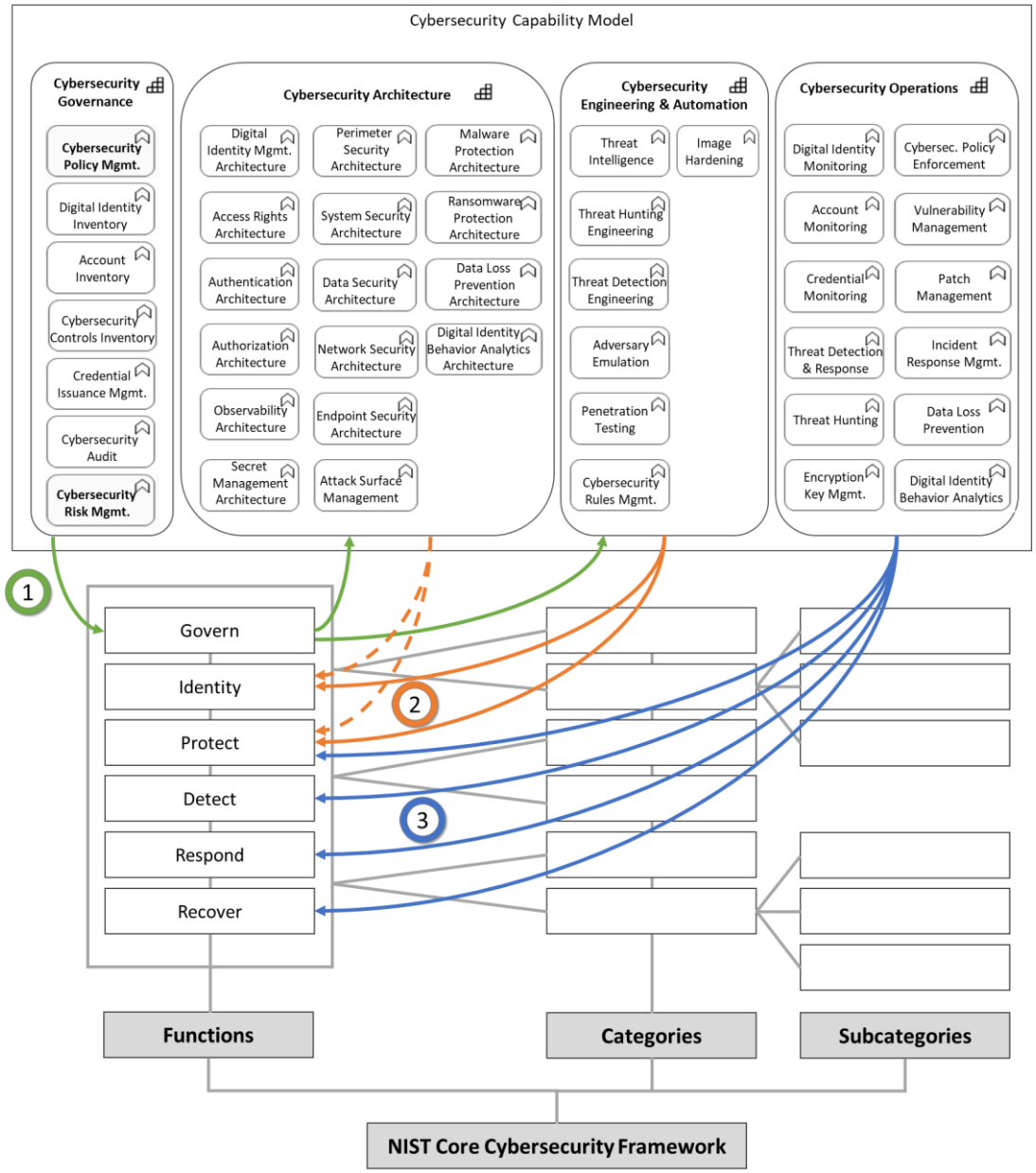


Figure 30

Level-2 Cybersecurity Capabilities

2.3. Level 2

Level 2 refers to the model's second decomposition layer and further reveals the structure of level-1 cyber capabilities. Level-2 cybersecurity capabilities are becoming more specific and concrete, leading to distinct activities. Like level-1 elements of the model, level-2 cyber capabilities are visually depicted as ArchiMate© functions. However, they are considered sub-functions or children of level-1 cybersecurity capabilities. Fifteen level-2 cybersecurity capabilities are detailed, as highlighted in the table and figure below. They are as follows:

Level-1 Cyber Function (Parent Function)	Level-2 Cyber Sub-Functions
Access Rights Architecture	1. Privileged Access Management Architecture
Observability Architecture	2. Logs & Alerts Architecture
Adversary Emulation	3. Thead Modeling
Cybersecurity Rules Management	4. Policy as Code Management
Threat Detection Engineering	5. Deception Engineering
Cybersecurity Policy Enforcement	6. Authentication Policy Enforcement 7. Authorization Policy Enforcement 8. Network Policy Enforcement 9. Device Policy Enforcement 10. Role-Based Access Control Policy
Incident Response Management	11. Malware Response Management 12. Ransomware Response Management 13. Digital Forensics
User & Entity Behavior Analytics	14. Log & Alert Lifecyle Management 15. Log & Alert Analysis

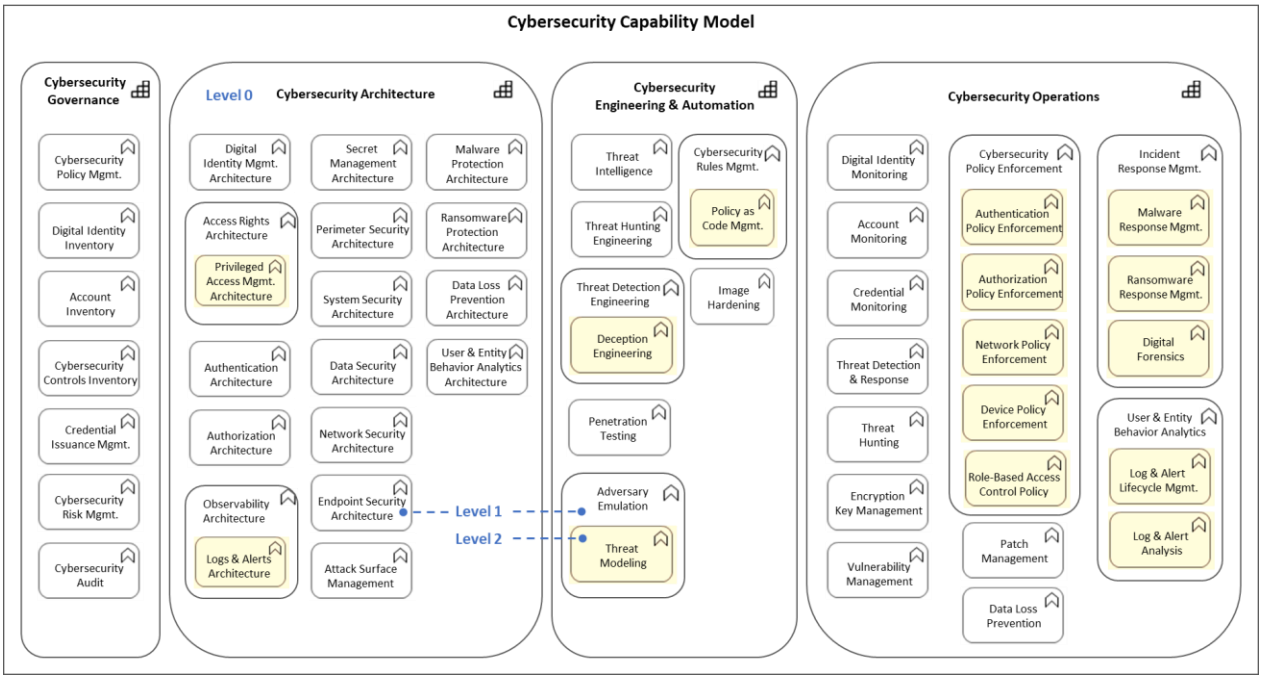


Figure 31

2.3.1. Cybersecurity Architecture Capability – Level 2

As articulated earlier in the document, cybersecurity architecture is the backbone of the cybersecurity discipline. Poor identifications and placement of cybersecurity controls across an enterprise's IT estate will continuously erode the digital trust and cybersecurity posture any organization must maintain to operate digitally, regardless of investment levels.

The cybersecurity capability model presented in this document suggests two level-2 cybersecurity sub-functions under the parent and foundational Cybersecurity Architecture capability, as illustrated in the figure to the right. They are:

1. Privileged Access Management Architecture
2. Logs & Alerts Architecture

Their definitions follow next.

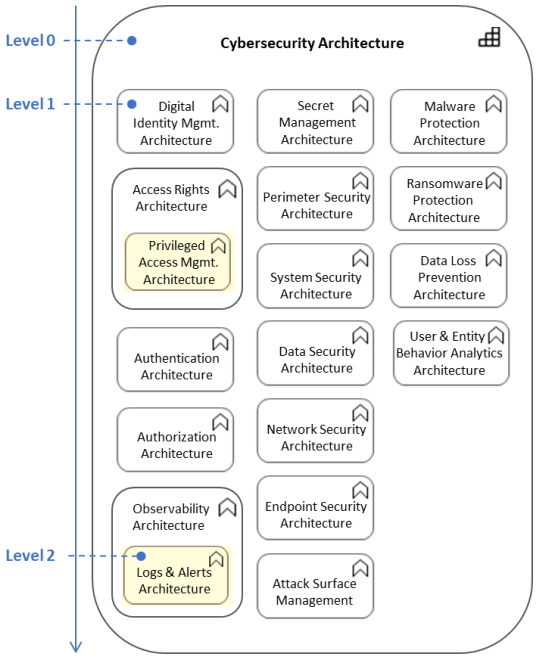


Figure 32

The Privileged Access Management (PAM) Architecture sub-function refers to a set of design principles, frameworks, policies, and standards paired with activities for defining, creating, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is to govern, control, and monitor digital identities that have elevated permissions to interact with a firm's IT assets.

Executing this cybersecurity sub-function results in a series of blueprints that should preferably exhibit characteristics associated with architecture best practices, such as evolvability, maintainability, reliability, usability, performance, security, interoperability, compliance with relevant standards, and cost efficiency. Effective PAM architecture integrates identity and access management, access controls, session monitoring, credential management, and compliance requirements, providing a holistic approach to securing privileged access.

The quality and integrity of the architectures for reifying this cybersecurity sub-function are essential because relevant access control policies and their enforcement mechanisms are crucial for protecting and defending an enterprise's IT assets. The Privileged Access Management Architecture cyber sub-function is not only an essential component of a robust cybersecurity strategy, but it is also closely connected to the following non-exhaustive level-1 elements of the model:

- Digital Identity Inventory
- Account Inventory
- Credential Issuance Management
- Cybersecurity Audit
- Threat Detection & Response
- Digital Identity Monitoring
- Account Monitoring

The Logs & Alerts Architecture sub-function refers to a set of design principles, frameworks, policies, and standards paired with activities for defining, creating, and maintaining conceptual, logical, and implementation architectures for a technology element or solution whose functional behavior is the collection, monitoring, and analysis of log and alert data originating from an organization's entire IT ecosystem.

Executing this cybersecurity sub-function results in a series of blueprints that should preferably exhibit characteristics associated with architecture best practices, such as evolvability, maintainability, reliability, usability, performance, security, interoperability, compliance with relevant standards, and cost efficiency. The result architecture blueprints must provide visibility into IT asset activities, detect potential cybersecurity incidents, and trigger alerts for timely response and mitigation.

The proper realization of the outputs generated by executing the Logs and Alerts Architecture sub-function is a critical ingredient of a comprehensive cybersecurity strategy. It also has dependencies on the following non-exhaustive level-1 elements of the model:

- Cybersecurity Audit
- Threat Detection & Response
- Digital Identity Behavior Analytics

In practice, the content of logs and alert notifications may need to be normalized to enable the consistent identification of key fields for subsequently establishing cybersecurity trends or deriving possible harmful activities. The Open Cybersecurity Schema Framework, or similar schemas, may be leveraged to normalize security-related telemetry across an organization.

Further Reading:
Design a Log Analytics workspace architecture | Microsoft
SIEM Architecture: 10 Key Components and Best Practices | Coralogix
Open Cybersecurity Schema Framework
Log Monitoring & 2025 Compliance: Undeniable Conjunction | The Cyber Security Hub Newsletter

[Intentionally left blank for formatting purposes]

2.3.2. Cybersecurity Engineering & Automation Capability – Level 2

The cybersecurity capability model offers three level-2 cybersecurity subfunctions under the Cybersecurity Engineering & Automation root element, as illustrated in the figure below. The first one is a subfunction of the level-1 Cybersecurity Rules Management function and is labeled Policy as Code. The second one is a subfunction of the level-1 Adversary Emulation function and is labeled Threat Modeling. The last one is a subfunction of the level-1 Threat Detection Engineering and is labeled Deception Engineering.

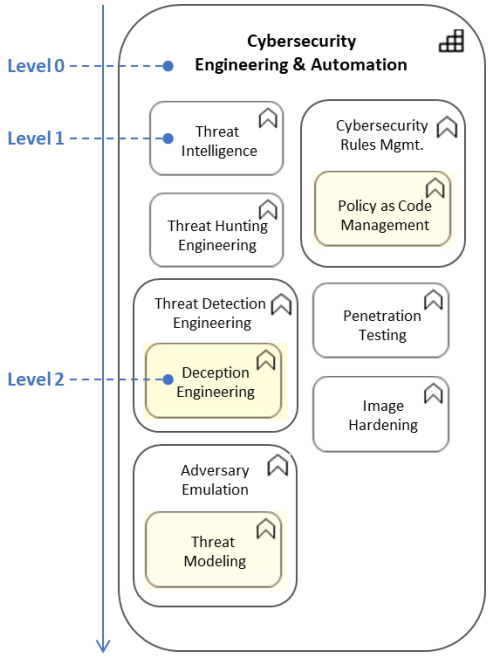


Figure 33

The Policy as Code Management cybersecurity sub-function is a methodology for defining and maintaining cybersecurity policies through machine-readable code instead of executing manual processes and configuration settings. This automated approach to cybersecurity policy management promotes execution agility and speed while fostering auditability. It also reduces human errors usually caused by a lack of automation. This cyber sub-function is associated with the broader corporate management of IT infrastructure.

The main output of this function, cybersecurity policies, are deployed in a Policy Decision Point's policy engine.

Further Reading:
What Is Policy-as-Code? | Palo Alto Neworks
What Is Policy as Code and How Does It Work? | Black Duck
Introduction to policy as code with automation | Red Hat
Policy Decision Point (PDP) | NIST

Deception Engineering

Deception Engineering is a proactive and advanced level-2 cybersecurity function that aims to mislead cyber adversaries and force them to artfully reveal themselves by intentionally creating and deploying IT assets designed to be probed, attacked, or compromised. These deceptive IT assets emulate business resources, including operating systems, technology services, application services, and data, which organizations typically rely on to conduct their operations. The main objective of Deception Engineering is to entice adversaries into revealing themselves and their techniques, tactics, and procedures (TTPs) by compelling threat actors to interact with fake or deceptive IT resources. Successfully executing this cybersecurity function allows organizations to gather valuable intelligence about their threat landscape and respond more effectively to future attack attempts or incidents.

Further Reading:
Deception Engineering | Zscaler© Blog
Deception and Intuition in Software Engineering | IEEE Xplore
RED: Reverse Engineering of Deceptions
CYBERSECURITY DECEPTION ENGINEERS: THE UNSEEN GUARDIANS OF CYBERSECURITY PROGRAMS AND THE UNSUNG HEROES IN THE BATTLE AGAINST CYBER THREATS | Taylor & Francis Online

Threat Modeling

The Threat Modeling cybersecurity function is a structured approach to identifying threats and vulnerabilities in software applications or systems and plays a critical role in protecting an organization. PASTA, STRIDE, VAST, and Trike are existing threat models that an enterprise can either leverage as initially conceived or tailor to fit its needs.
This function includes developing contextualized application architecture views after selecting a threat model. Technical controls are added next, followed by ingress and egress traffic flows to discover vulnerabilities that could be taken advantage of (exploited) through threat vectors in the context of said traffic flows. Threat and risk analyses are subsequently performed for each uncovered potential or actual vulnerability to assess materiality, impact, likelihood of exploitation, and plausible tactics, techniques, and procedures used by adversarial actors to capitalize on cybersecurity deficiencies.

The goal of threat modeling is to proactively identify potential cybersecurity flaws early in the software development life cycle so that they can be remedied before any piece of software is released for use.

Threat modeling is often associated with cybersecurity operations. However, this document opines that activities connected to this function must be discharged before any software application or system is deployed into a Production environment and not after. As a result, this softcopy positions threat modeling within the Cybersecurity Engineering and Automation capability and designates it as a sub-function of Adversary Emulation rather than within the Cybersecurity Operations capability.

Further Reading:
Threat Modeling | OWASP
What is threat modeling? | Black Duck
What is threat modeling? How does it work? | Fortinet

2.3.3. Cybersecurity Operations Capability – Level 2

The Cybersecurity Operations capability contains ten level-2 cyber subfunctions, as illustrated in the table and figure below. They are:

Level-1 Cyber Function (Parent Function)	Level-2 Cyber Sub Functions
Cybersecurity Policy Enforcement	1. Authentication Policy Enforcement 2. Authorization Policy Enforcement 3. Network Policy Enforcement 4. Device Policy Enforcement 5. Role-Based Access Control Policy
Incident Response Management	6. Malware Response Management 7. Ransomware Response Management 8. Digital Forensics
User & Entity Behavior Analytics	9. Log & Alert Lifecyle Management 10. Logs & Alert Analysis

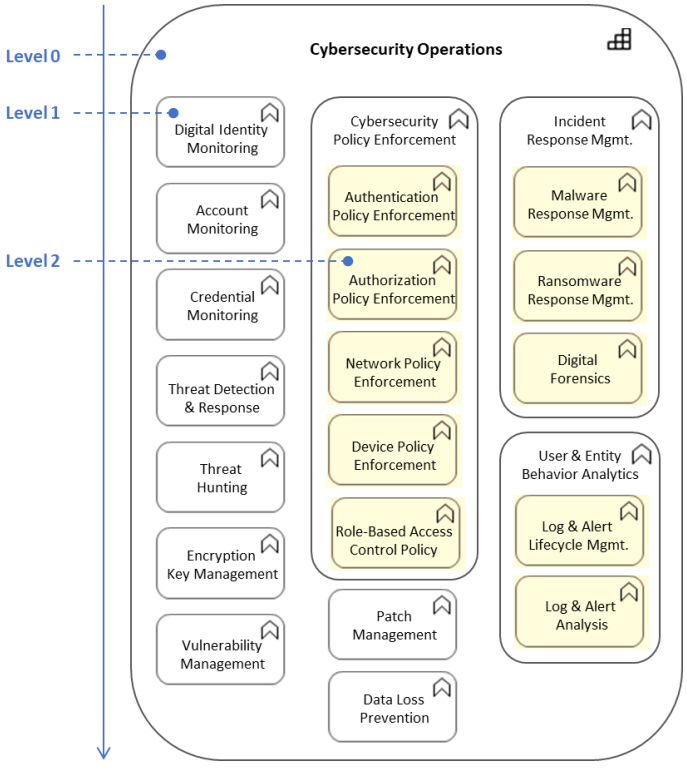


Figure 34

Their definitions are provided in the following pages.

Authentication Policy Enforcement refers to an enterprise's technology solution with which all digital identities (human and non-human) interact to be consistently validated and affirmed before they can interact with a firm's IT assets.
This cyber sub-function ensures an organization's authentication policy is rigorously applied. It also includes procedures, processes, guidelines, and measures for the monitoring, recording, and reporting of digital identity assertions. Under some conditions, failed identity affirmations may trigger real-time alerts for investigation by the Security Operations Center (SOC) team.
Implementing and firmly enforcing an authentication policy is crucial for safeguarding an organization's IT assets and ensuring that only authorized digital identities can access them. The Authentication Policy Enforcement sub-function enhances the confidentiality and integrity dimensions of the CIA Triad while strengthening an enterprise's security posture.

Automating this cybersecurity sub-function can greatly simplify and increase the efficiency of managing authentication policies within an organization.

Further Reading:
Tools for enforcing authentication policy | Okta

Authorization Policy Enforcement points to the use of an enterprise's technology solution with which all digital identities (human and non-human) interact to be consistently granted access permission to a firm's IT assets.
This cyber sub-function ensures an organization's authorization policy is rigorously applied. It encompasses procedures, processes, guidelines, and measures necessary for monitoring, recording, and reporting access requests made by digital identities, along with their granted or denied status. Depending on an enterprise's authorization policy, a predetermined number of denied access requests originating from a single digital identity may trigger a real-time alert for investigation by the Security Operations Center (SOC) team.

Authorization Policy Enforcement is a fundamental element of an organization's cybersecurity defense-in-depth strategy because it guarantees that access to all IT assets is strictly controlled based on a predefined set of policies. Like Authentication Policy Enforcement, this cyber sub-function enhances the confidentiality and integrity dimensions of the CIA Triad while strengthening an enterprise's security posture.

Automating this cybersecurity sub-function can greatly simplify and increase the efficiency of managing authorization policies within an organization.

Further Reading:
Authorization Enforcement | OSO
Authorization Policy Enforcement Points | Secure Auth IdP
Towards Automated Authorization Policy Enforcement | Penn State CSE
Policy-based authorization in ASP.NET Core | Microsoft

Network Policy Enforcement refers to the implementation processes, procedures, guidelines, and exploitation of an enterprise's technology solution for executing policies and rules that govern the behavior, access, and activities inside an organization's network. It also involves compliance with security protocols, standards, and guidelines to protect network resources and data assets.

This level-2 cybersecurity capability aims to maintain network integrity, confidentiality, and availability by monitoring and controlling access to the network, detecting and responding to violations, and ensuring that all network activities adhere to established cybersecurity policies. Automation in policy enforcement can significantly reduce the complexity and enhance the efficiency of managing cybersecurity policies within an organization. By leveraging automated tools and technologies, organizations can streamline policy enforcement, ensure consistent compliance, and minimize the risk of human error.

Further Reading:
What Is Policy Enforcement? | F5
What Is Network Policy? | CISCO
What is Network Policy Enforcement? | InteropNet Labs

The Device Policy Enforcement cybersecurity sub-function concentrates on the implementation processes, procedures, guidelines, and the use of an enterprise's technology solution for executing policies and rules that govern the use of devices within an organization's network. It ensures that devices, whether desktops, laptops, mobile devices, or IoT appliances, comply with established secured software and protocols to protect against adversarial events.
The objective of this level-2 cybersecurity capability is to ensure the integrity, confidentiality, and availability (CIA Triad) of organizational IT assets by monitoring, controlling, and managing device behavior and access.

Access control addresses how an organization's legitimate digital identities access IT assets, and it can take many forms. In addition to determining whether a digital identity has permission to interact with IT assets, access control may also constrain when and how said IT assets may be consumed.
Access control can take three main shapes: RBAC, PBAC, and ABAC. RBAC grants access to IT assets based on organizational roles, PBAC based on policies, and ABAC based on attributes associated with request types submitted for execution to IT resources. This document purposefully focuses on RBAC, but the generic form can be used instead.

Consequently, the Role-Based Access Control (RBAC) Policy cyber sub-function pertains to defining and maintaining an enterprise-wide policy that governs assignments and revocations of permissions and access rights to organizational roles fulfilled by digital identities. Included are a collection of implementation processes, procedures, guidelines, and activities coupled with an enterprise's technology solution to manage assignments 's lifecycle from birth to cradle. This level-2 cyber capability intends to enforce the principle of least privilege by ensuring that digital identities have only access to IT assets required to perform their job functions and nothing more unless necessary.

Incident response management has previously been described in this document as the set of practices, contingency plans, frameworks, coordinated processes, synchronized activities, and tooling required for an organization to defend itself after identifying incidents or their materialization into intrusions, breaches, or exploits.

Malware Response Management is a specialized version of the more generic level-1 Incident Response Management cyber function, which focuses on resisting and defeating malware-related adversarial events. This specialization stresses the need for organizations to devise multiple defense (or response) plans tailored to the specificity of cyber attacks.
Consequently, Malware Response Management refers to a formal policy paired with procedures and activities designed to manage and mitigate the effects of malware infections within an organization's IT environment. Included are the successful execution of detection, analysis, containment, eradication, and recovery functions to o ensure that malware incidents are handled efficiently and effectively to protect organizational IT assets.

Further Reading:
Incident Response Plan: Frameworks and Steps | CrowdStrike
Malware, Phishing, and Ransomware | CISA
7 Steps of a Complete Malware Incident Response Plan
Playbook of the Week: Malware Investigation and Response | Palo Alto Networks

In its simplest form, ransomware is a variety of malicious software that encrypts an organization's data and information, rendering it inaccessible until a ransom is paid.
Like Malware Response Management, this level-2 cyber sub-function is a specialized version of the more generic level-1 Incident Response Management cyber function. It focuses on preparing for, detecting, responding to, and recovering from ransomware in instances where it is still a threat or an actual incident.
An effective defense and response against ransomware involves a combination of proactive cybersecurity controls, immediate actions during such an attack, and comprehensive plans for recovery and mitigation.
Consequently, Ransomware Response Management refers to a formal policy paired with procedures and activities designed to prevent, contain, manage, and mitigate the crippling effects linked to ransomware infections within an organization's IT environment. The successful execution of this level-2 cybersecurity capability depends on the robustness and cohesiveness of dependent activities such as monitoring, detection, analysis, containment, eradication, and recovery to ensure that ransomware incidents are dealt with as efficiently and effectively as possible.

By preparing more generally for potential attacks, organizations can better protect their IT assets, minimize disruptions, and reduce the overall impact of cyber assaults. As cyber threats increase in frequency and potency, robust ransomware response management will remain essential for protecting digital assets and maintaining operational resilience.

Further Reading:
Ransomware Protection and Response | NIST
Ransomware incident response playbook framework | Microsoft

The Merriam-Webster dictionary defines forensics as applying scientific knowledge to legal problems. In the context of the cybersecurity discipline, Digital Forensics is a specialized field that concentrates on identifying, preserving, analyzing, and presenting digital evidence. The Digital Forensics cyber sub-function is crucial for investigating cybercrimes, security breaches, and other incidents related to electronic data to uncover facts and support legal or administrative actions.

It encompasses methodologies, processes, techniques, and tools for collecting, analyzing, and reporting digital data in a legally admissible manner. Digital Forensics also employs scientifically validated methods to investigate and reconstruct events or incidents involving digital devices and networks, ensuring the integrity and authenticity of the collected evidence.

Ken Zatyko described in a 2007 article in Forensic Magazine an eight-phase process that provides a frame of reference for laymen or laywomen to apprehend. The eight phases are: 1. Search Authority, 2. Chain of Custody, 3. Imaging/Hashing Function, 4. Validated Tools, 5. Analysis, 6. Repeatability (Quality Assurance), 7. Reporting, 8. Possible Expert Presentation.

Further Reading:
What is digital forensics? | IBM
Digital evidence | NIST
What is Digital Forensics? Tools, Types, Phases & History | Cyber Security News

The Log & Alert Lifecycle Management cyber sub-function refers to structured and continuous processes paired with tools for systematically managing the entire lifecycle of logs and alerts generated by an organization's IT assets. It includes collecting, storing, and archiving logs and alerts to ensure their availability for subsequent analysis.

The analysis, correlation, and response activities have purposefully been associated with a dedicated cyber sub-function labeled Log & Alert Analysis to emphasize the critical importance of this aspect. A variation of this cybersecurity capability model could merge the Log & Alert Analysis sub-function with the Log & Alert Lifecycle Management one.

Automating this cybersecurity sub-function is strongly recommended to enhance the effectiveness and efficiency of cybersecurity efforts.

Please cross-reference with the Log & Alert Analysis sub-function anchored in the Cybersecurity Operations capability.

Further Reading:
Log Management: Introduction & Best Practices | Splunk
What is Log Management? The Importance of logging and best practices | CrowdStrike
IT alert management: Guide, tools, and more | Freshworks
Log Monitoring & 2025 Compliance: Undeniable Conjunction | The Cyber Security Hub Newsletter

Log & Alert Analysis concentrates on the systematic investigation and evaluation of logs and alerts generated by an organization's IT assets to identify, understand, and respond to indicators of compromise and security incidents alike. This process involves proactively using automated tools and manual techniques to analyze log data, detect anomalies, correlate events, and assess the significance of alerts.

Organizations can gather valuable and actionable insights into their security posture by routinely executing this cyber sub-function because it can help prevent, detect, and mitigate cyber threats.

Log & Alert Analysis is a crucial aspect of cybersecurity operations, as it empowers enterprises to enhance their incident response capabilities by methodically examining logs and alerts.

Please cross-reference with the Log & Alert Lifecycle Management sub-function anchored in the Cybersecurity Operations capability.

Further Reading:
Log Analysis: A Complete Introduction | Splunk
Log Analysis Explained | CrowdStrike
What is log analytics? | Dynatrace

[Intentionally left blank for formatting purposes]

Level-3 Cybersecurity Capabilities

2.4. Level 3

Level 3 refers to the model's least abstract cybersecurity capabilities. They are visually represented as ArchiMate© functions but are considered sub-functions or children to level-2 cybersecurity capabilities.

Cyber Security Operations Capability – Level 3

The Cybersecurity Operations capability contains two level-3 cyber sub-functions, as illustrated in the figure below. They are labeled Least Privilege Access Policy and Privileged Access Policy. Their definitions are provided on the next page.

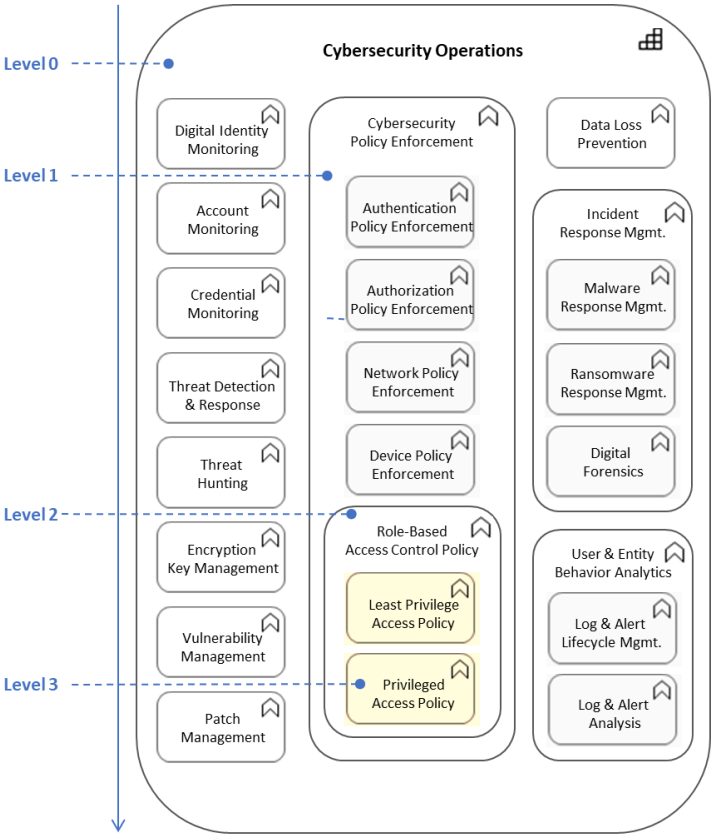


Figure 35

Least Privilege Access is a core principle in cybersecurity that mandates assigning the minimum level of access necessary for an organization's digital identities to discharge their duties. This approach aims to minimize the risk of unauthorized access and potential security breaches by limiting permissions granted to said digital identities (human and non-human) to IT assets to only what is essential.
Least Privilege Access equally includes a security policy designed to enforce the principle of least privilege by restricting access rights and permissions of digital identities to the minimum necessary for performing specific roles. This policy requires proactive, continuous evaluation and adjustment of access levels to ensure adherence to security protocols and mitigate risks associated with excessive or unnecessary access to IT assets. Policy changes are systematically implemented across all relevant policy enforcement points.

This cybersecurity sub-function is associated with several level-1 abilities, which are the Digital Identity Monitoring, Account Monitoring, Credential Monitoring, Cybersecurity Policy Enforcement, and Digital Identity Behavior Analytics functions. Threat Detection & Response, Data Loss Prevention, and Incident Response Management could also be related to the Least Privilege Access Policy sub-function based on several (objective and subjective) criteria.

The Least Privilege Access Policy sub-function is essential for maintaining robust cybersecurity defenses and protecting organizational IT assets from both internal and external threats. By ensuring that digital identities only have the necessary access to perform their duties, enterprises can significantly reduce their vulnerability to security breaches and enhance their overall cybersecurity posture.

Further Reading:
What is Least Privilege? | CyberArk
Principle of Least Privilege: Definition, Methods & Examples | Okta
The Principle of Least Privilege Explained (with Best Practices) | Splunk

A Privileged Access Policy (PAM) aims to define, monitor, and control the exploitation of elevated access rights for and by a few authorized digital identities across an organization's IT ecosystem. This cybersecurity sub-capability critically contributes to an enterprise's cyber defense strategy.
The policy element associated with the Privileged Access Policy capability establishes principles, procedures, and guidelines for granting, managing, and monitoring how digital identities with more freedom of action interact with and exploit IT assets in general and sensitive ones in particular.

The Privileged Access Policy sub-function aims to validate and confirm that only digital identities with legitimate needs are granted elevated permissions. The verification helps reduce the risk of unauthorized access and protect IT assets from possible abuse, threats, or harm by digital identities that have no justifiable reason to interact with said IT assets with more freedom of action than required by their role.
Like the Least Privilege Access Policy cybersecurity capability, this subfunction is also part of a multilayered security strategy that integrates various defensive mechanisms across different levels of an organization's IT environment to prevent, detect, and respond to cyber threats, also known as defense-in-depth.

Cybersecurity Capability Model Usage

3. Cybersecurity Capability Model Usage

This section provides several examples of how the cybersecurity capability model outlined in this document can be applied to support strategic decision-making and facilitate in-depth analysis.

3.1. Drive Strategic Cybersecurity Investments

In the current complex and ever-evolving threat landscape, organizations must embrace a holistic approach to cybersecurity that seamlessly integrates various frameworks and models to achieve comprehensive protection. By combining the cybersecurity capability model into curated frameworks and models, enterprises can create robust cybersecurity vision and strategy work products that align with business goals, enhance security capabilities, and effectively mitigate cyber threats, as illustrated in the diagram below [18][19][20].

Figure 36 depicts how the cybersecurity capability model bridges the enterprise architecture discipline and its outputs with a cybersecurity architecture framework and a TPP knowledge base. TTP stands for tactics, techniques, and procedures and catalogs the behavior of a threat actor. TTPs are generally used for cyber threat intelligence and proactive threat hunting.

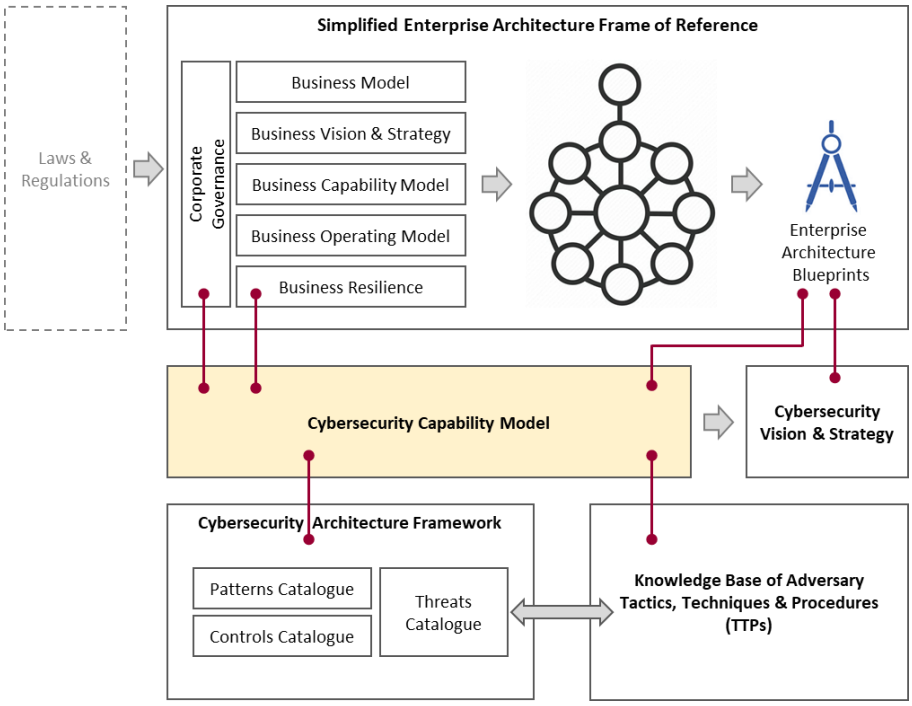


Figure 36

Figures 37 & 38 on the next couple of pages illustrate an imaginable reification of the above logical model using a custom enterprise architecture frame of reference based on TOGAF®, the cybersecurity capability model presented in this softcopy, the MITRE Att&Ck structure, and the Open Security Architecture (OSA) framework. The latter distills the know-how of the security architecture community and provides readily usable security patterns.

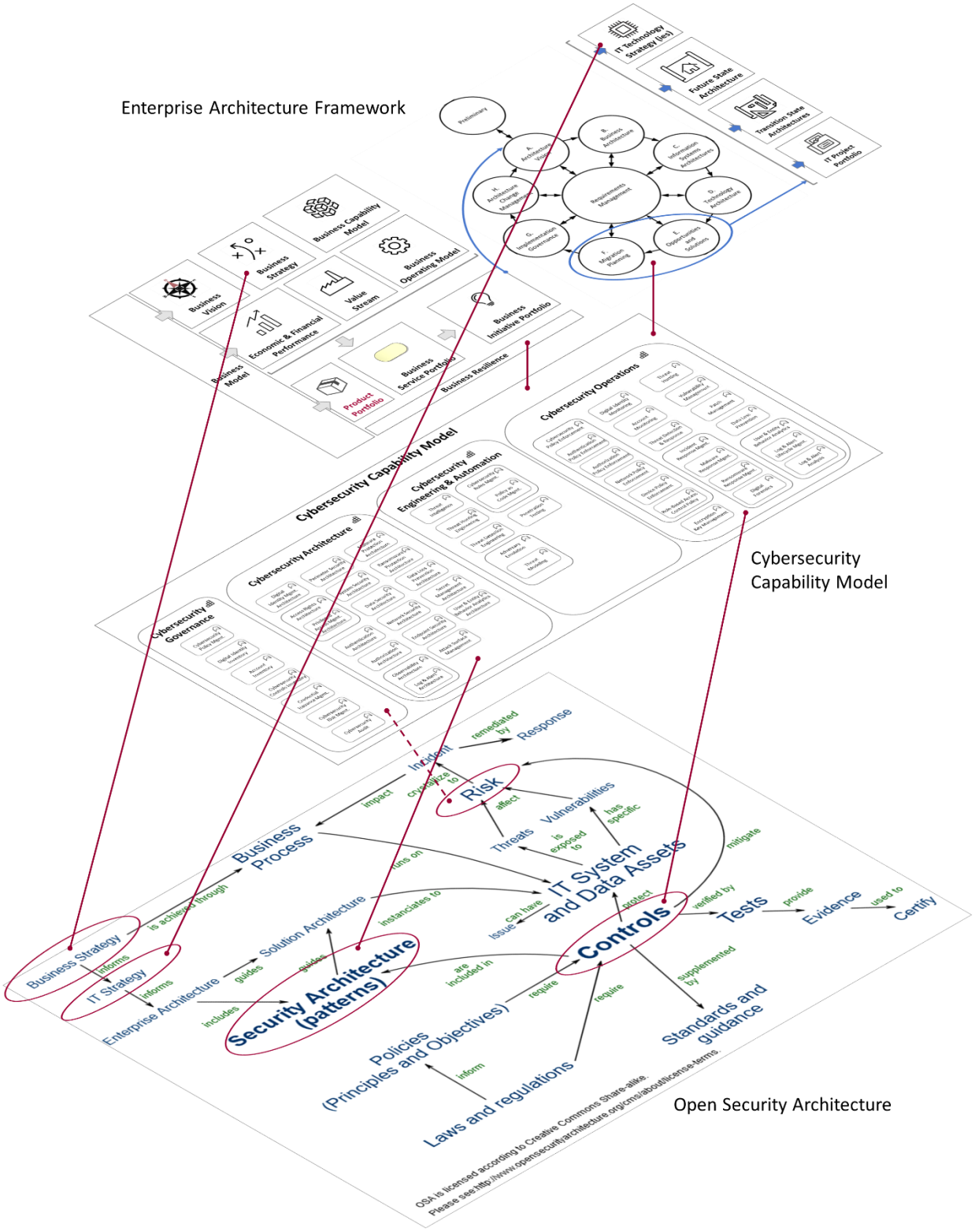


Figure 37: Connecting enterprise architecture, the cybersecurity capability model & a leading cybersecurity architecture framework

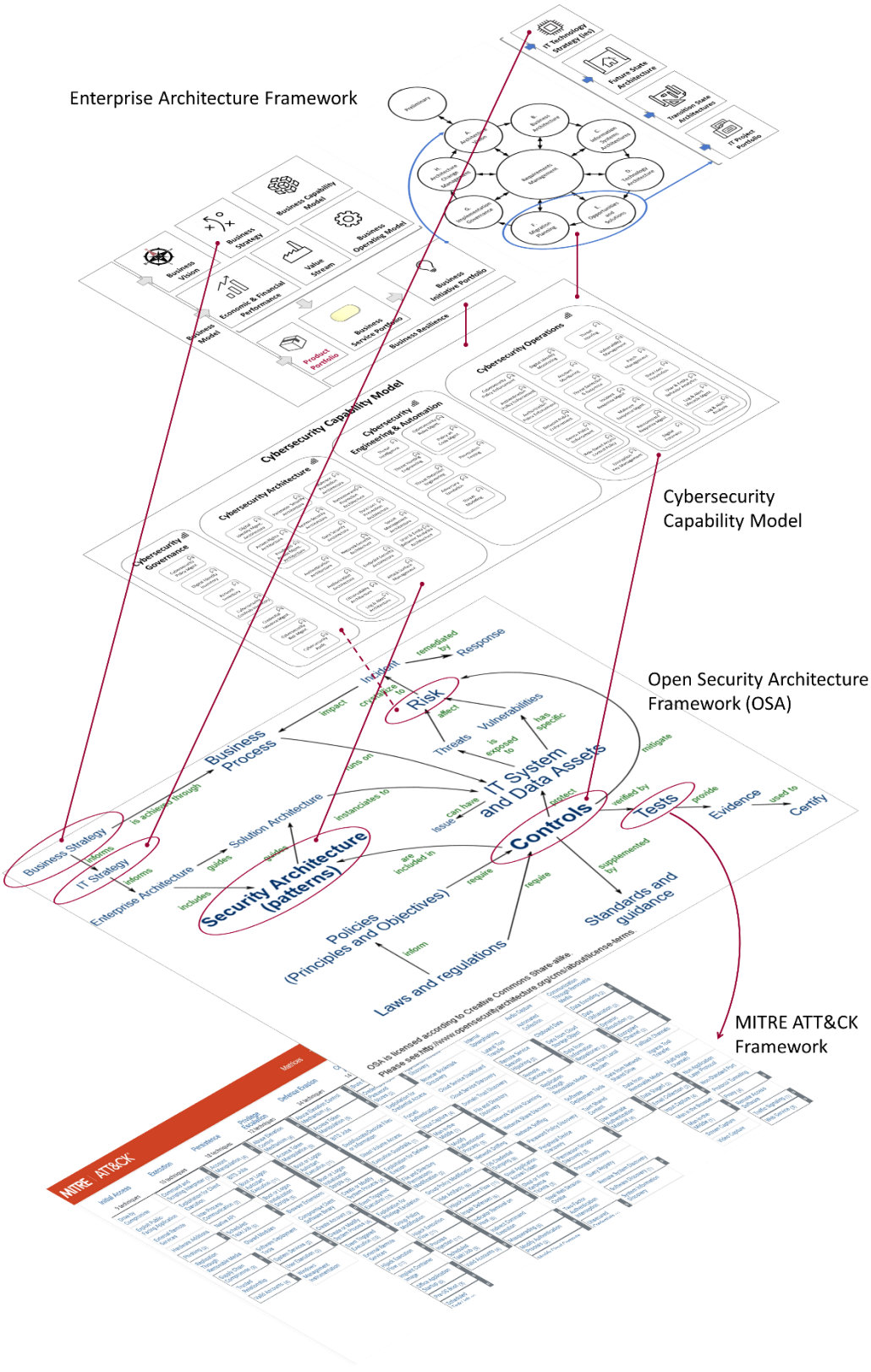


Figure 38: Connecting enterprise architecture, the cybersecurity capability model, a leading cybersecurity architecture framework, and the MITRE framework.

The cybersecurity capability model can also be used with The Open Enterprise Security Architecture (O-ESA) © from The Open Group. The latter advocates using a conceptual security framework, as shown in Figure 39. The cybersecurity capability model presented in this document can be utilized in this capacity, as illustrated in the figure below.

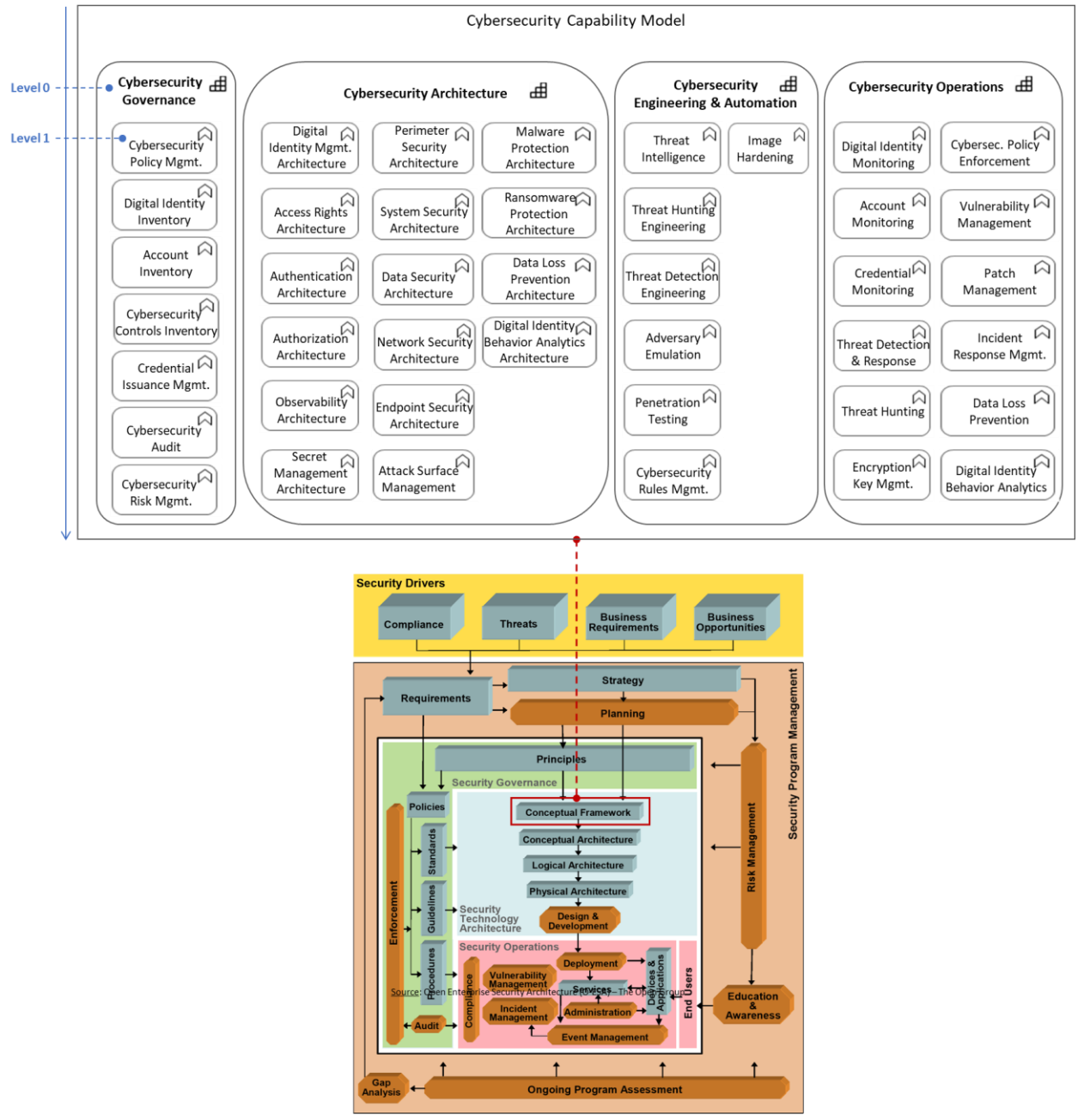


Figure 39

3.2. State Assessment/Projection & Maturity Analysis

The cybersecurity capability model is an essential tool for organizations to qualitatively assess and apprehend their current cybersecurity posture. It provides a structured frame of reference for evaluating an enterprise's cybersecurity capabilities, identifying gaps, and developing targeted improvements to enhance its defensive and protective measures. For example, the cybersecurity capability model can be effectively leveraged for current state assessment, as demonstrated in the accompanying figure below. The Red-Yellow-Green color scheme visually represents the effectiveness with which an organization executes specific cyber-related items, dimensions, or characteristics.

By leveraging a cybersecurity capability model for current state assessment, organizations can gain insights into their real cybersecurity posture, identify areas for improvement, and develop targeted strategies to strengthen their defenses against cyber threats. This approach may help enterprises not only improve their cybersecurity stance but also reinforce compliance with regulatory requirements and industry best practices. The same Red-Yellow-Green color scheme can also be used to visually communicate the desired state of effectiveness for specific cyber-related items, dimensions, or characteristics.

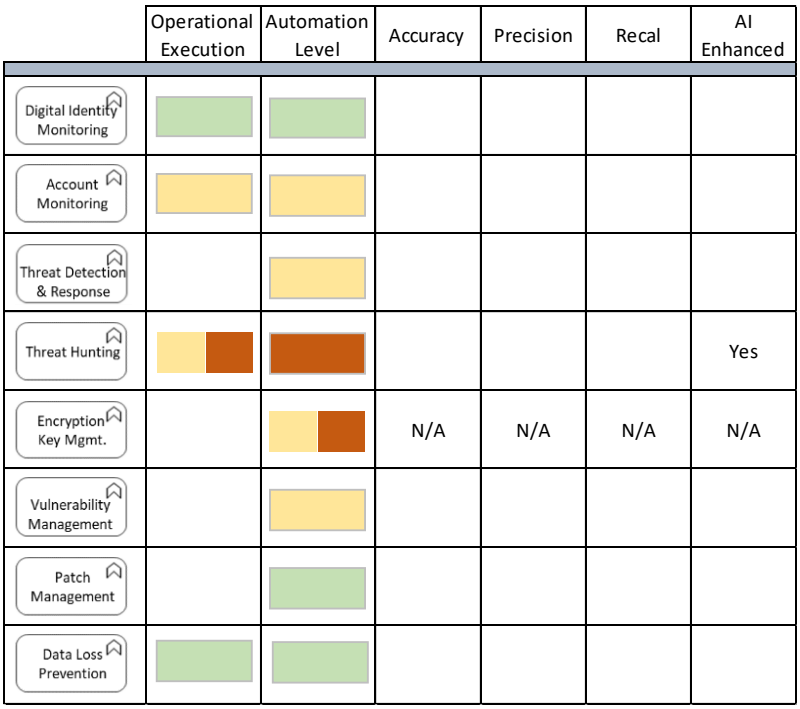


Figure 40: Illustrative

The cybersecurity capability model is also a strategic tool for projecting a desired maturity level so that organizations can plan and set cybersecurity goals, establish roadmaps, and systematically enhance their cybersecurity capabilities to reach targeted levels aligned with their digital ambitions.

3.3. Current & Future Cybersecurity Architecture Elaboration

The cybersecurity capability model also can be utilized to develop current and future state logical or physical security architectures in conjunction with the NIST framework and the ArchiMate© notation, as illustrated in the figure below.

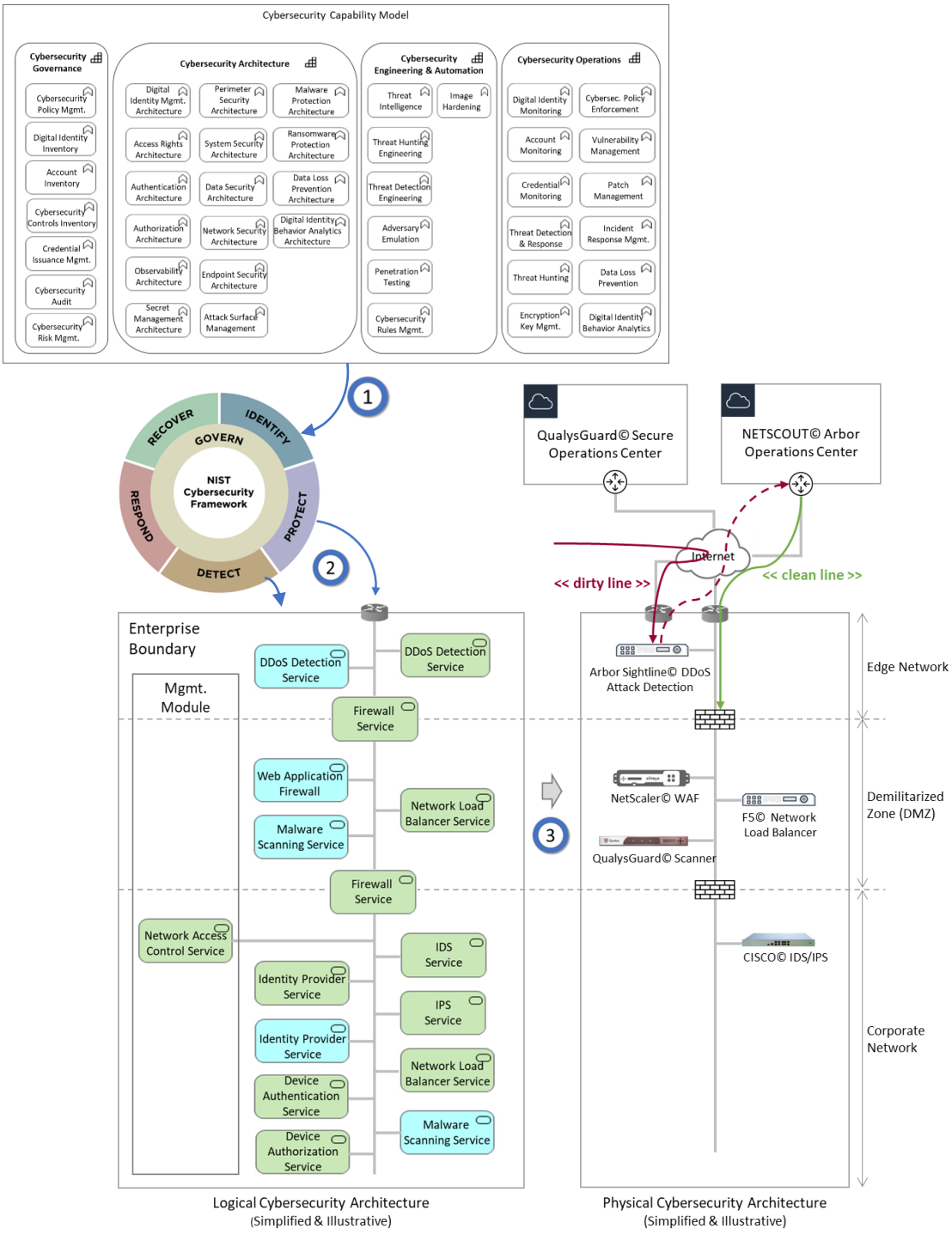


Figure 41: Illustrative

3.4. Regulatory Technology (RegTech)

Regulatory Technology, or RegTech, is the strategic application of innovative technologies to transform how organizations implement, manage, optimize, and maintain adherence to complex regulatory frameworks. By automating compliance processes and enabling proactive risk management, RegTech empowers organizations to adapt swiftly to evolving standards, ensuring operational efficiency and accountability in an increasingly dynamic regulatory landscape [21][22][23]. The figure below conceptually depicts the key elements to realizing RegTech from a cybersecurity perspective. The state of core characteristics associated with the Cybersecurity Governance and Cybersecurity Operations capabilities contribute to painting an organization's risk profile and operational resilience strength. The foundational Cybersecurity Operations capability and its underlying components provide the necessary data for automation engines to generate compliance and risk-related views.

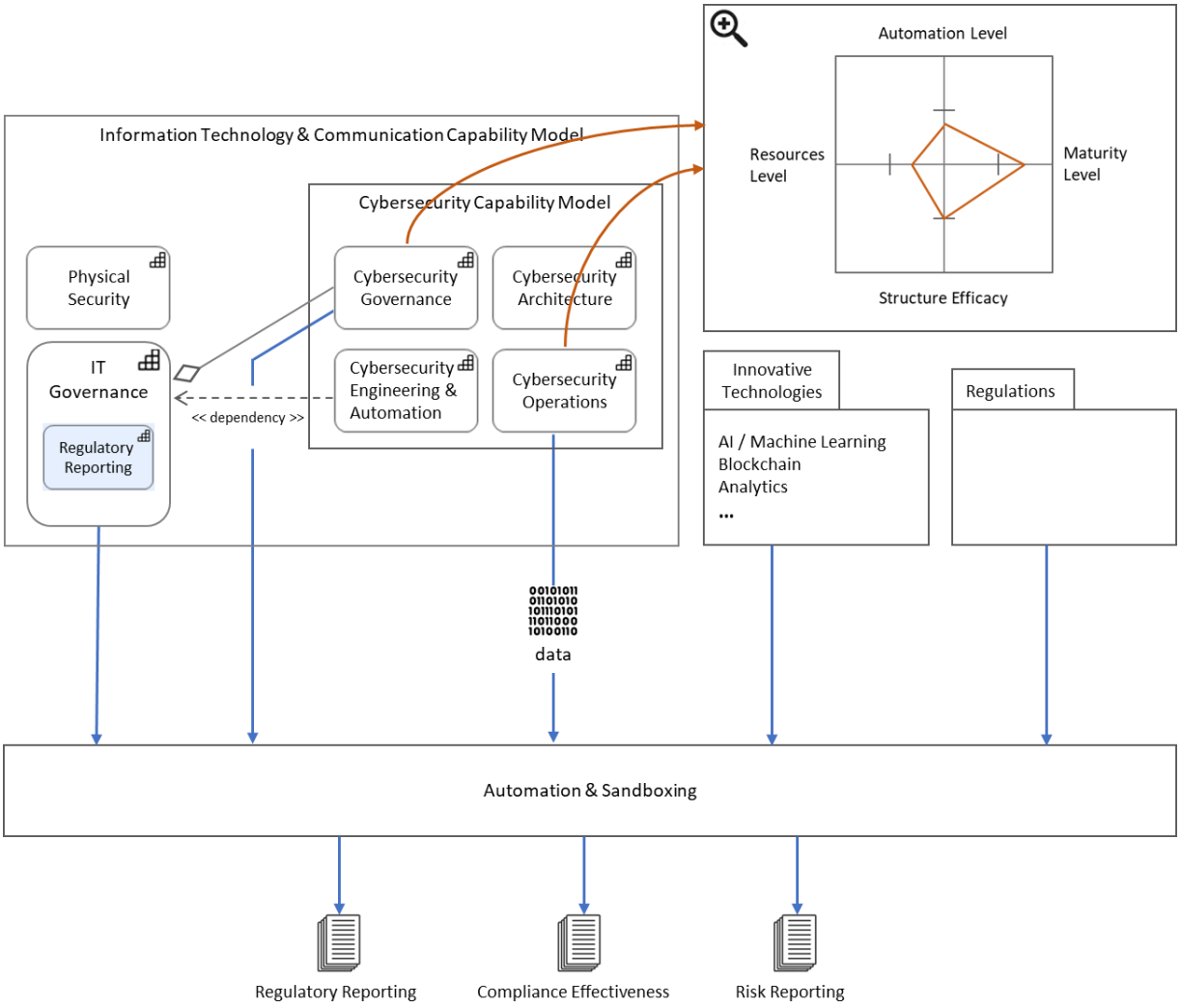


Figure 42: Linking the cybersecurity capability model to the regulatory technology (RegTech) discipline

Imaginable Variations of the Cybersecurity Capability Model

4. Imaginable Variations of the Cybersecurity Capability Model

The cybersecurity capability model presented in this document should not be interpreted as an authoritative source, as articulated in the Introduction. A few imaginable variants of the model are described in this section to spark its customization.

4.1. Cybersecurity Governance

4.1.1. Cybersecurity Audit

The foundational cybersecurity capability labeled Cybersecurity Governance was originally represented with seven level-1 cyber functions, as shown on the left-hand side of the figure below. The Level-1 Cybersecurity Audit capability could alternatively be renamed Cybersecurity Compliance & Audit, allowing two new level-2 sub-capabilities to be incorporated: Vulnerabilities Disclosure and Compliance Validation, as illustrated on the right-hand side of Figure 43.

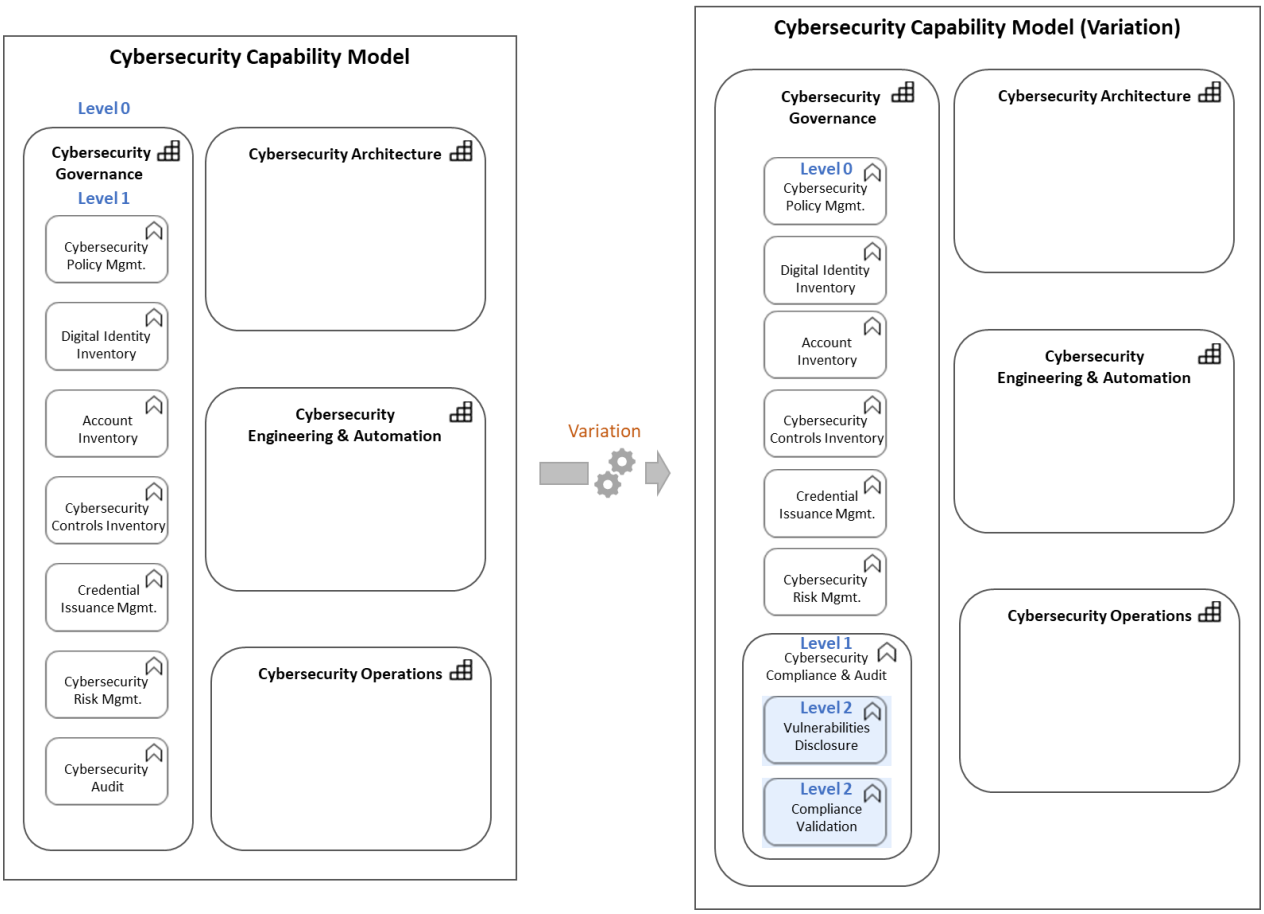


Figure 43

As articulated in the Cybersecurity Audit definition on page 25, the assessment aspect embedded within the audit cyber capability can be isolated into its distinct cybersecurity capability, as exemplified in the figure below. Figure 44 depicts the Cybersecurity Assessment capability as a level-2 cybersecurity function or a child of the level-1 Cybersecurity Audit capability. Both cybersecurity capabilities could alternatively be at the same level.

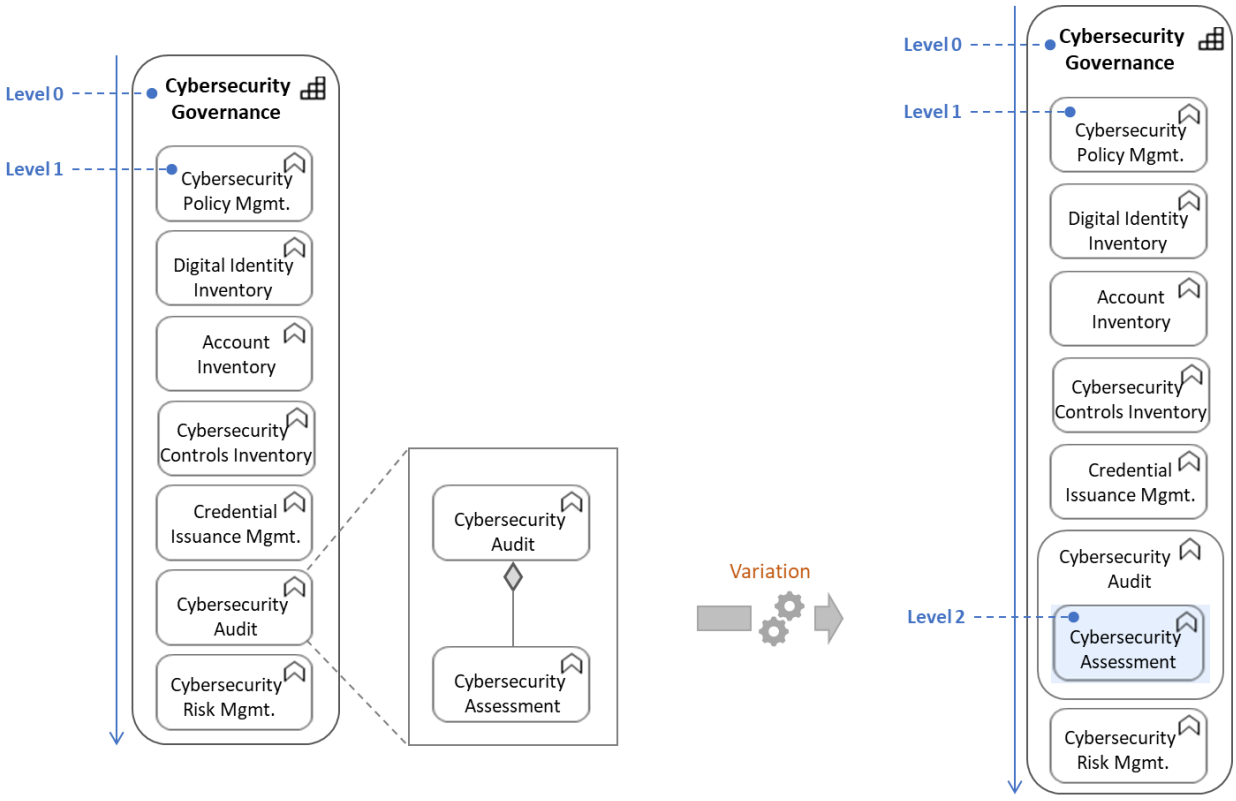


Figure 44

Finally, the proposed adaptations documented in Figures 43 and 44 could be merged to form a new level-zero Cybersecurity Governance capability.

4.1.2. Cybersecurity Awareness & Training

The cybersecurity capability model has privileged the core or "hard" abilities an enterprise must operationalize to protect, defend, and recover from adversarial events and activities. However, the human or "soft" element, including behavior, decision-making, and awareness, is one of the most significant factors in cybersecurity, as employees are simultaneously the first line of defense and the weakest link. Therefore, organizations must also foster a cybersecurity culture where their workforce is equipped with the knowledge to recognize and report suspicious activities. Consequently, a level-1 cybersecurity capability labeled Cybersecurity Awareness & Training could be added to the Cybersecurity Capability model, as illustrated in the figure below. The document deliberately omitted the human factor to direct the readers' attention to the more technical capabilities.

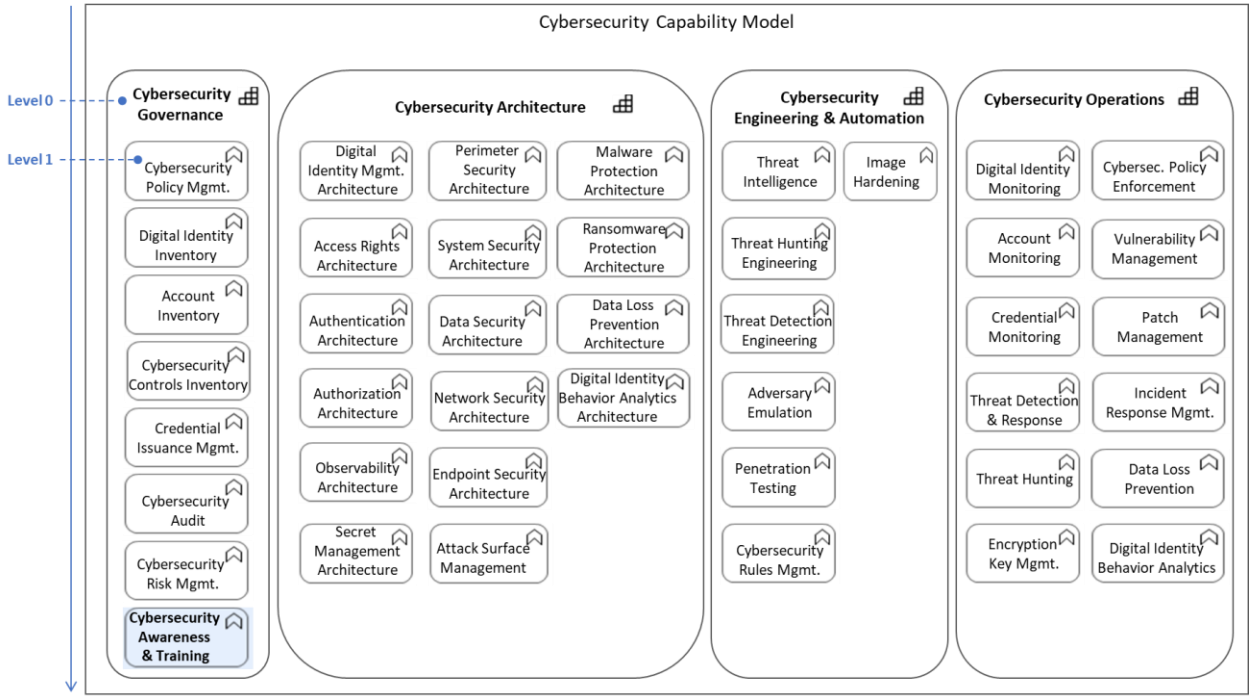


Figure 45

[Intentionally left blank for formatting purposes]

4.1.3. Regulatory Reporting

Regulatory reporting is a critical capability for any regulated entity or organization. However, it was not included as an element of the cybersecurity capability model, as this document did not consider it a component for actively protecting and defending against adversarial cyber events. Instead, this capability has been classified under the broader IT Governance capability, as illustrated in the figure below. Readers can disagree with the positioning of the Regulatory Reporting capability and incorporate it with either the Cybersecurity Governance or Cybersecurity Operations foundational capabilities.

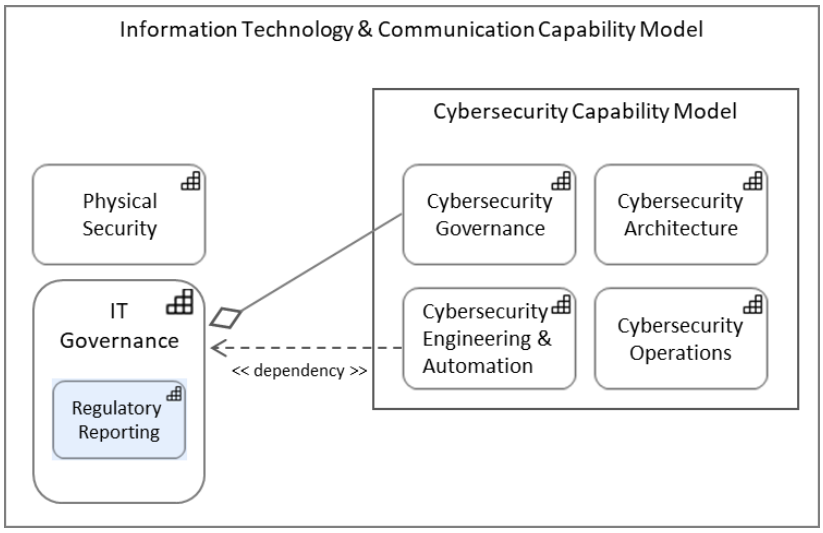


Figure 46

[Intentionally left blank for formatting purposes]

Appendix

5. Appendix

5.1. Enlarged Cybersecurity Capability Model Diagram – Level Zero & Level 1

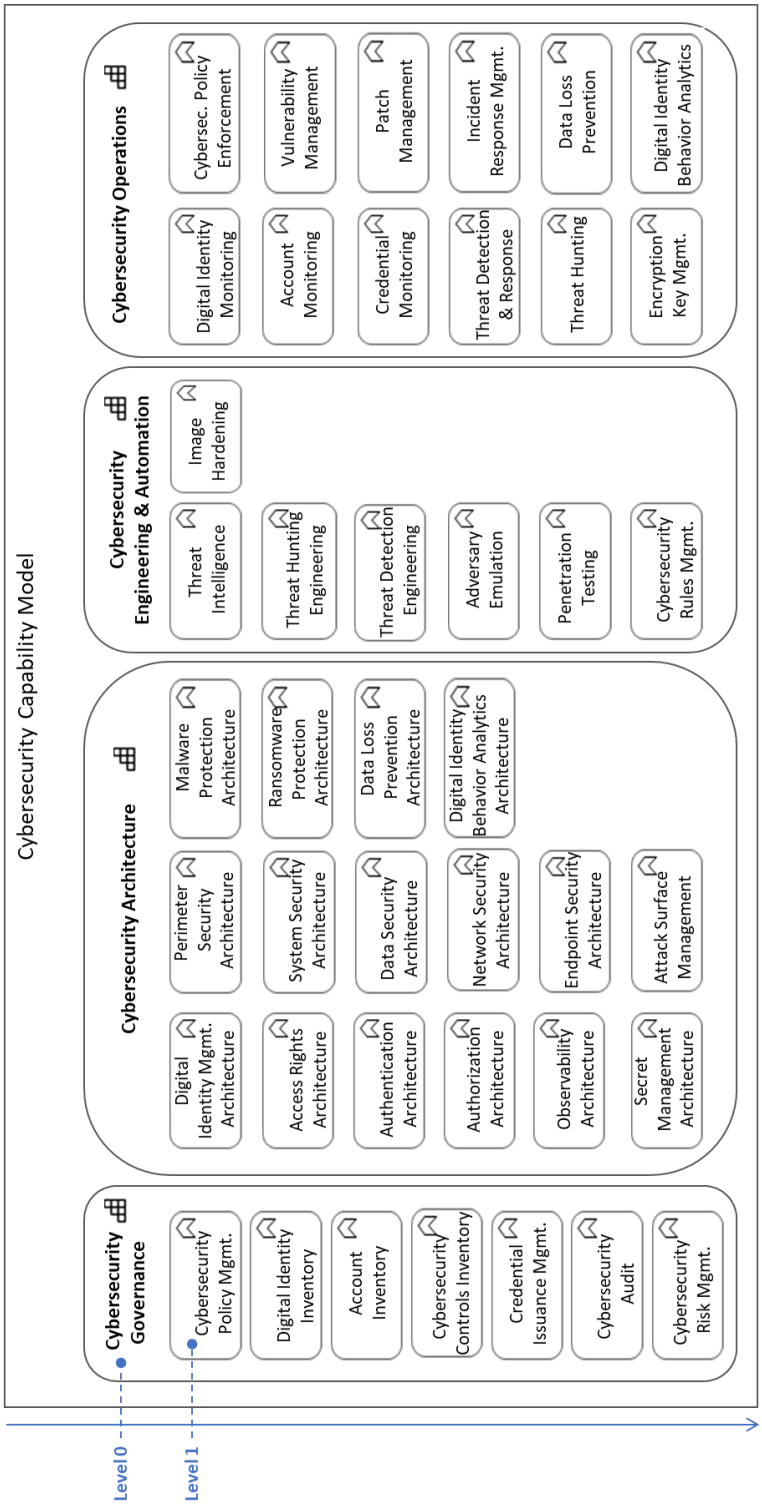


Figure 47: Level-zero (0) & level-1 cybersecurity capabilities

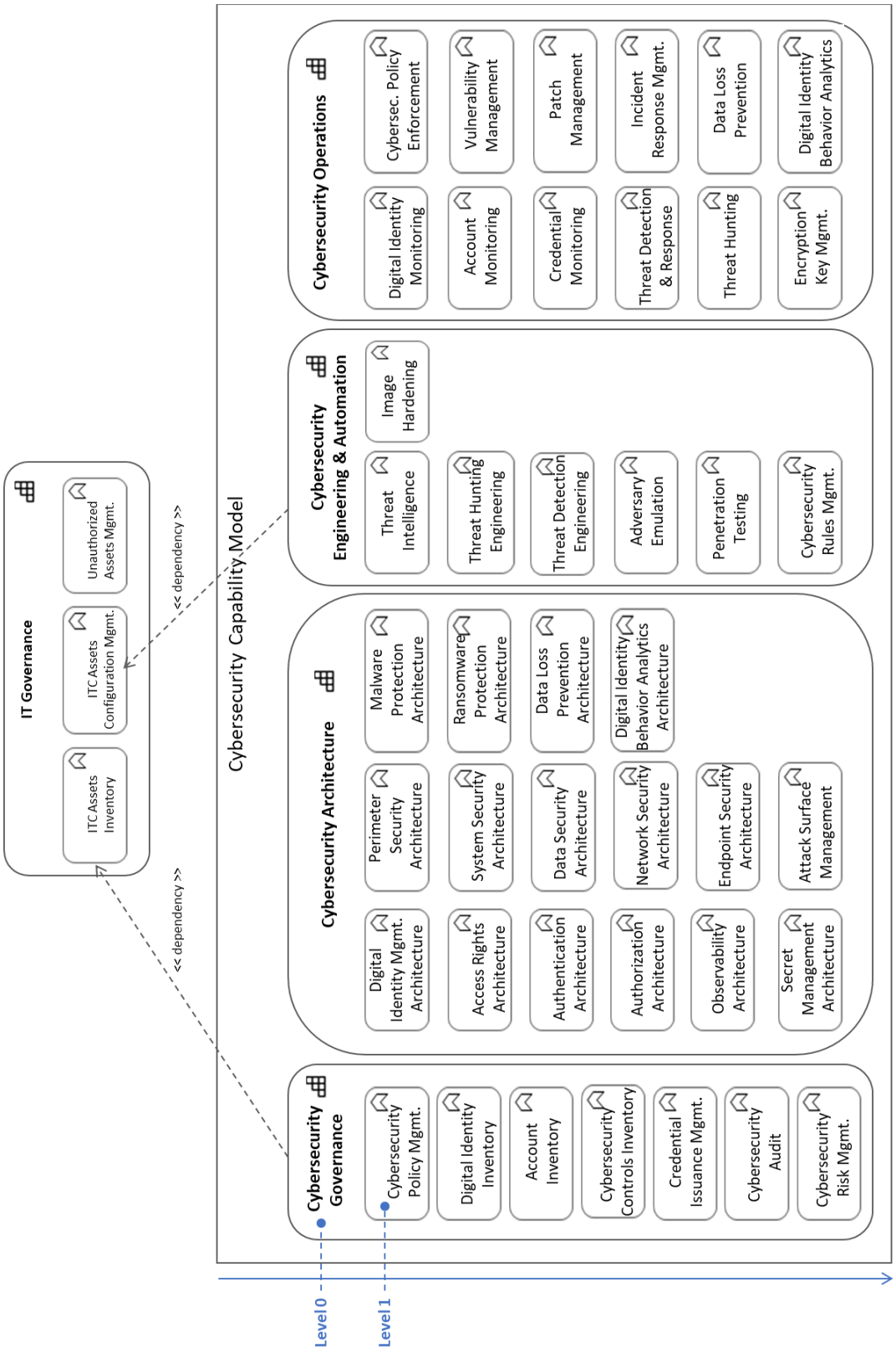


Figure 48: Level-zero (0) & level-1 cybersecurity capabilities in relation to a simplified IT governance capability

5.2. Enlarged Cybersecurity Capability Model Diagram – Level Zero, Level 1 & Level 2

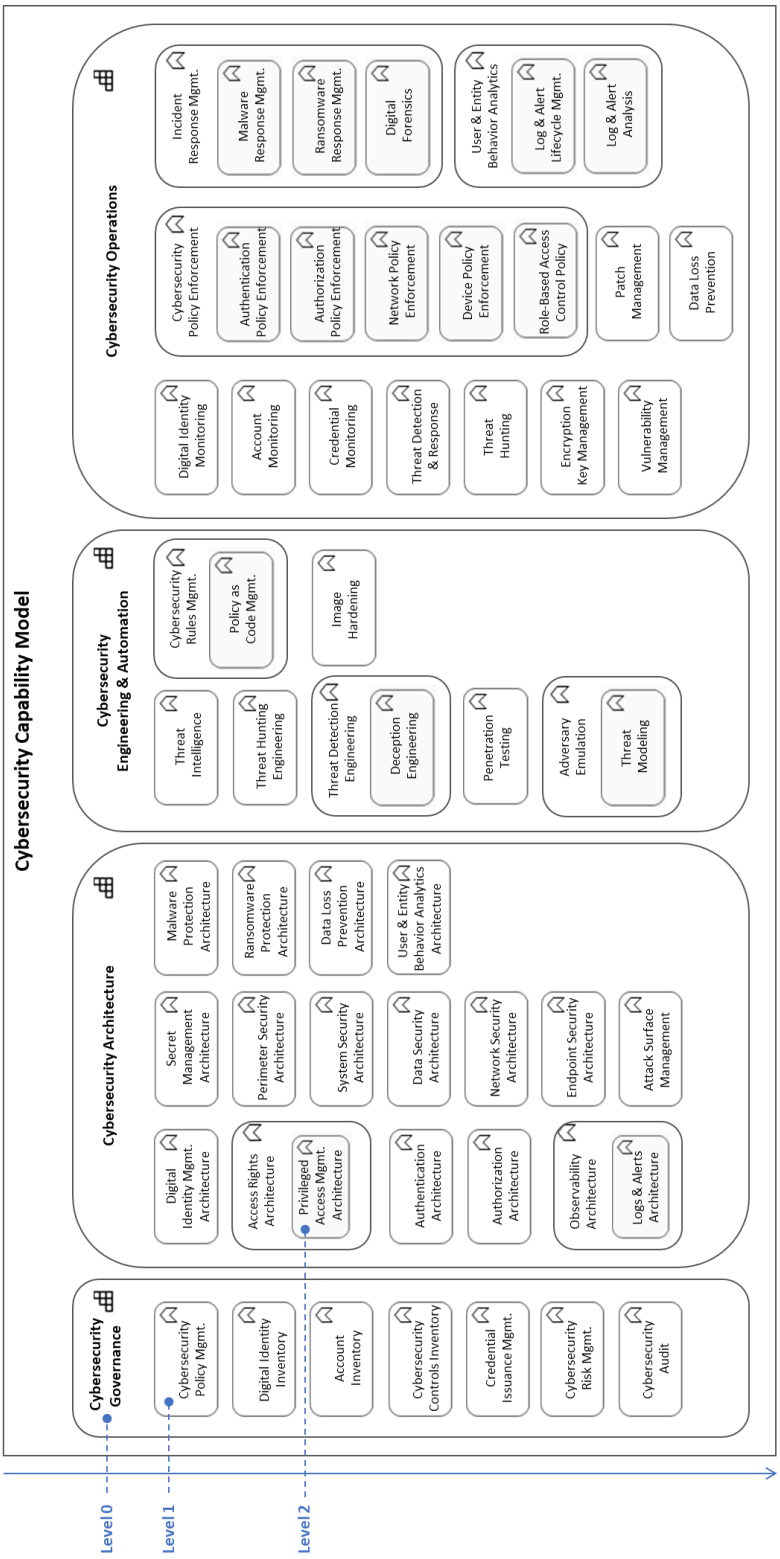


Figure 49: Level-zero (0), level-1 & level-2 cybersecurity capabilities

5.3. Enlarged Cybersecurity Capability Model Diagram – Level Zero, Level 1, Level 2 & Level 3

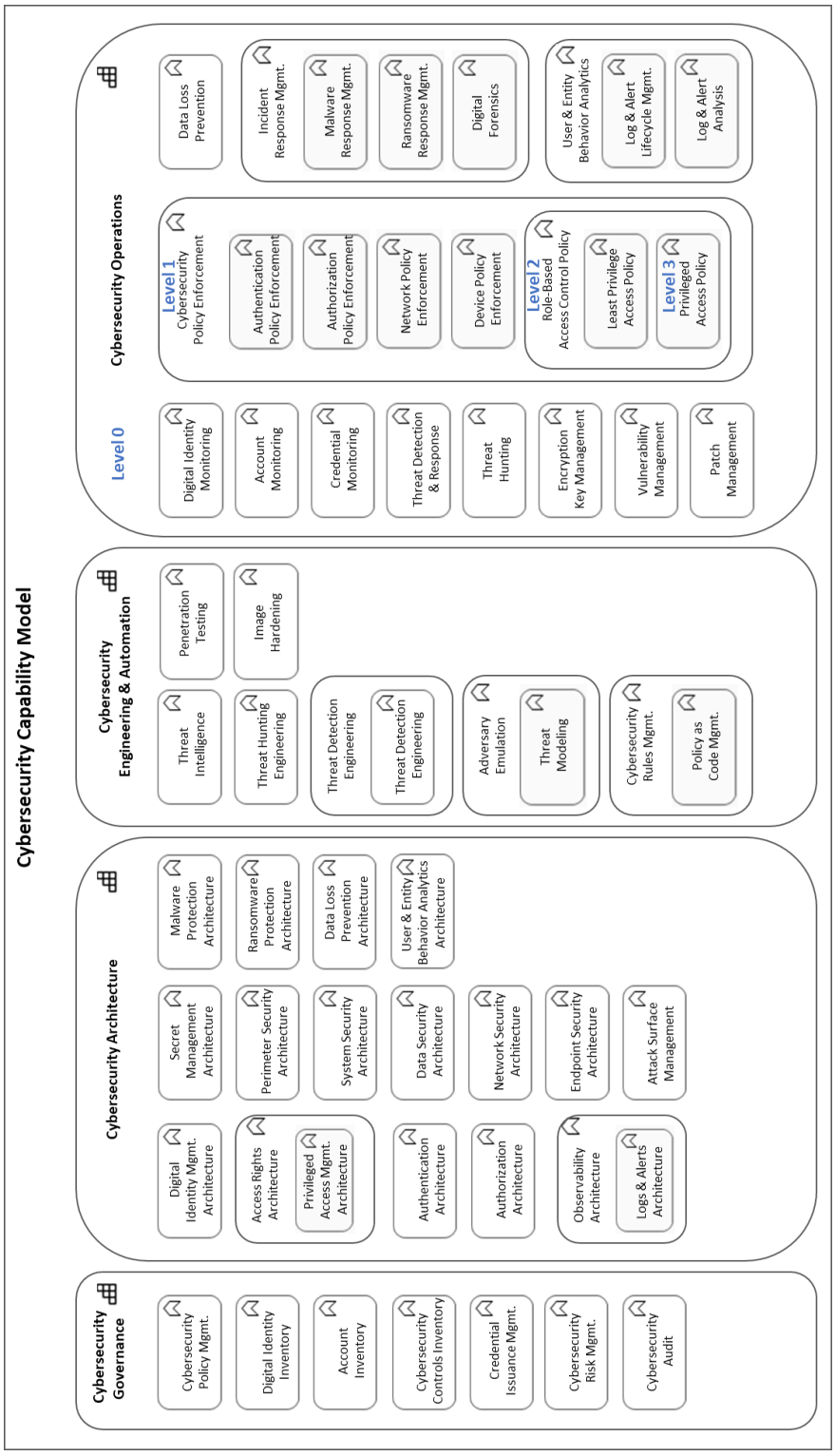


Figure 50: Level-zero (0), level-1, level-2 & level-3 cybersecurity capabilities

5.4. Enlarged Cybersecurity Capability Model with Logical & Physical Cybersecurity Controls

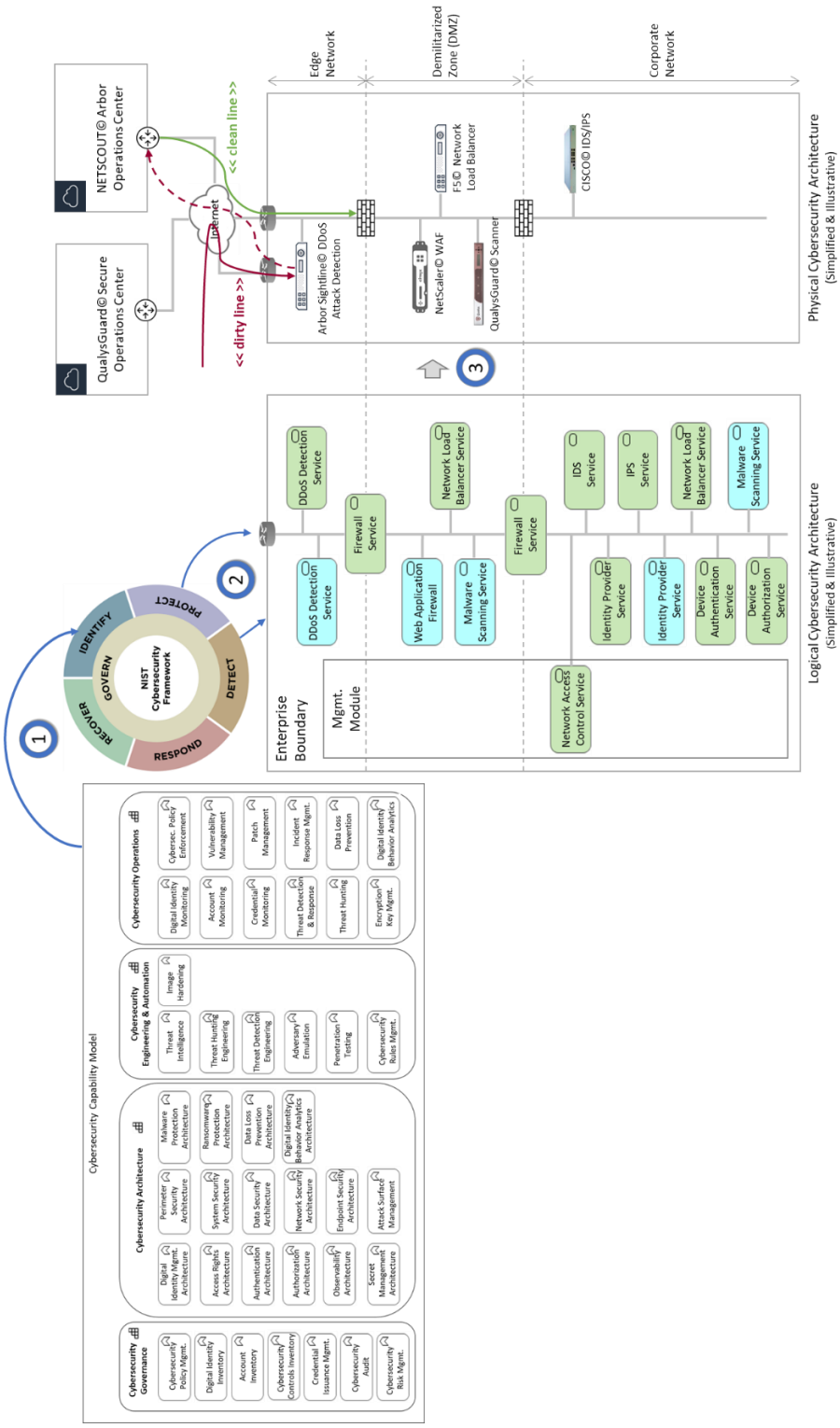


Figure 51: Crafting logical & physical cybersecurity architectures from the cybersecurity capability model

5.5. Enlarged Data Center vs. Cloud Construct Diagram – Infrastructure Focus

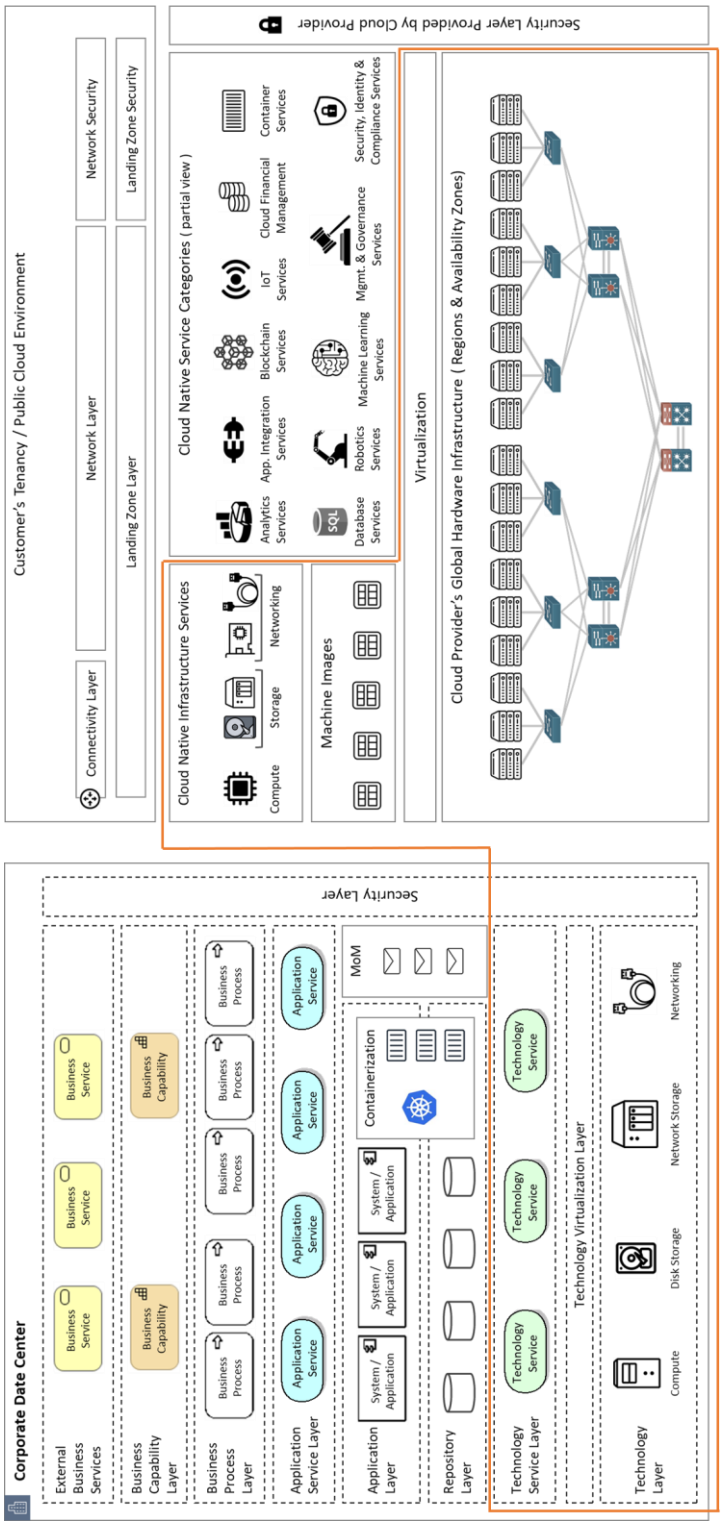


Figure 52

5.6. Enlarged Data Center vs. Cloud Construct Diagram – Application/Solution Focus

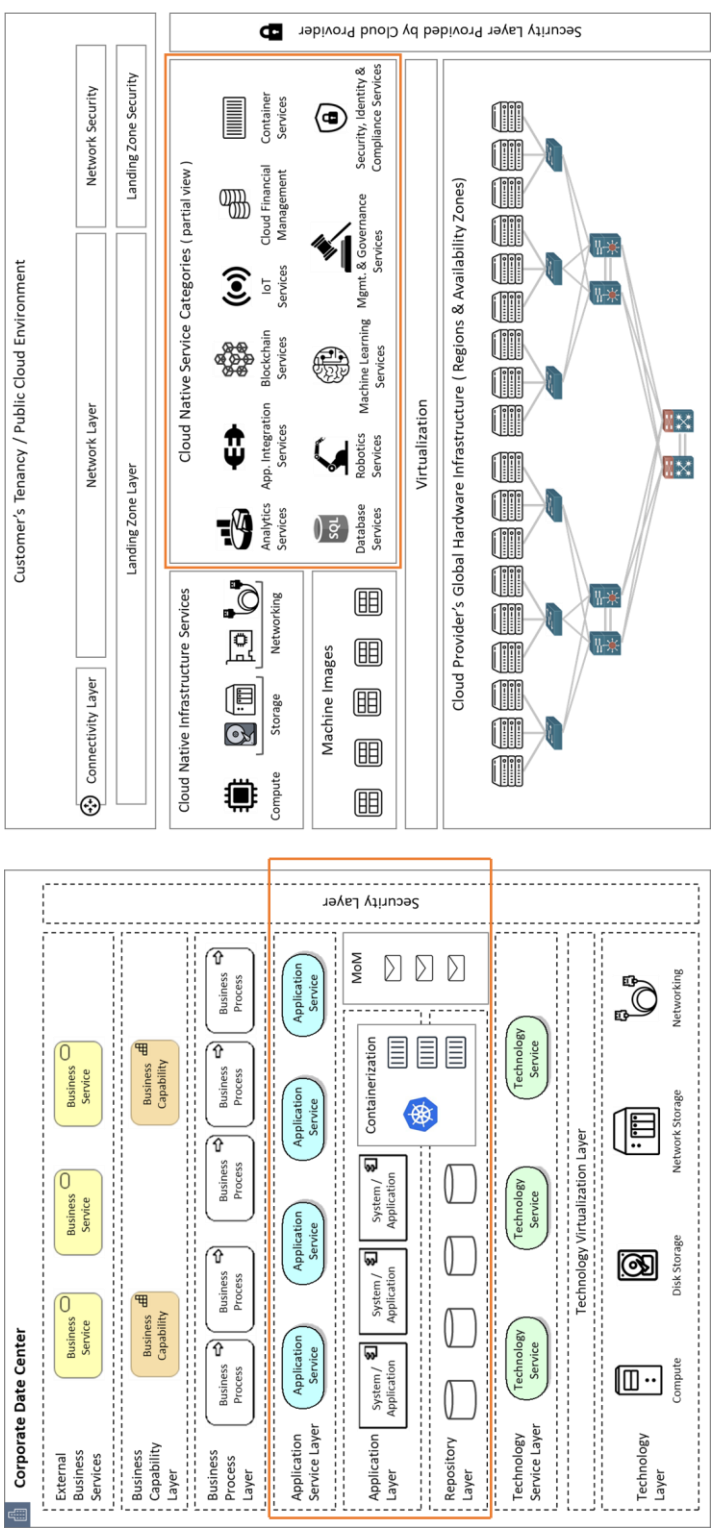


Figure 53

6. References

[1] The Open Group, ArchiMate® 3.2 Specification Web site, *Capability definition*. Available at https://pubs.opengroup.org/architecture/archimate3-doc/ch-Strategy-Layer.html#sec-Capability

[2] Cornell University, Legal Information Institute, *Entity definition*. Available at https://www.law.cornell.edu/wex/entity

[3] Cornell University, Legal Information Institute, *Natural Person definition*. Available at https://www.law.cornell.edu/wex/natural_person

[4] Orbus Software, *BPMN 2.0 Task Types Explained (2023)*. Available at https://www.orbussoftware.com/resources/research-library/detail/bpmn-20-task-types-explained

[5] Object Management Group, *Business Motivation Model v1.3 (2015)*. Available at https://www.omg.org/spec/BMM/1.3/PDF

[6] The Open Group, TOGAG® Series Guide, *Business Capabilities, v2 (2022)*. Available at https://pubs.opengroup.org/togaf-standard/business-architecture/business-capabilities.html

[7] Patricia Guevara, *Understanding the Essence of Cybersecurity Governance to Organizations (2024)*. Available at https://safetyculture.com/topics/cyber-security/cybersecurity-governance/

[8] ISACA Interactive Glossary. Available at https://www.isaca.org/resources/glossary#glossc

[9] Carol; Woody, Ph.D., Rita Creel, *What is Cybersecurity Engineering? And Why Do I need it? (2020)*. Available at https://insights.sei.cmu.edu/documents/5688/2020_018_101_650083.pdf

[10] Kayly Lange, *What Is SecOps? Security Operations Defined (2024)*. Available at https://www.splunk.com/en_us/blog/learn/secops-security-operations.html

[11] Lark Editorial Team, *Cyber Operations (2024)*. Available at https://www.larksuite.com/en_us/topics/cybersecurity-glossary/cyber-operations

[12] The Open Group, Open Enterprise Security Architecture (O-ESA), *The Enterprise Security System Desing Model (2011)*. Available at https://pubs.opengroup.org/security/o-esa/#_Toc291061699

[13] Anderson Technologies, *What Is a Cybersecurity Audit: A Comprehensive Step-by-Step Guide*. Available at https://andersontech.com/resources/learn/what-is-cybersecurity-audit/

[14] The Open Group, The TOGAF® Standard, v9.2, *Architecture definition*. Available at https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html

[15] Sunil Arora, *From Chaos to Confidence: The Indispensable Role of Security Architecture (2023)*. Available at https://www.isaca.org/resources/news-and-trends/industry-news/2023/from-chaos-to-confidence-the-indispensable-role-of-security-architecture

[16] Graham Budd, Forbes Technology Council, Resilience As A Competitive Advantage (2020). Available at https://www.forbes.com/councils/forbestechcouncil/2020/12/09/resilience-as-a-competitive-advantage/

[17] Mary K. Pratt, *The undeniable benefits of making cyber resiliency the new standard* (2023). Available at https://www.csoonline.com/article/654891/the-undeniable-benefits-of-making-cyber-resiliency-the-new-standard.html

[18] Sivan Tehila, Forbes Technology Council, *Cybersecurity As A Strategic Investment: How ROI Optimization Can Lead To A More Secure Future (2023)*. Available at https://www.forbes.com/councils/forbestechcouncil/2023/08/16/cybersecurity-as-a-strategic-investment-how-roi-optimization-can-lead-to-a-more-secure-future/

[19] Joseph Nocera, *Cyber & Privacy Innovation Institute Leader, PwC, Get smart on cyber investment strategies (2022)*. Available at https://www.pwc.com/us/en/tech-effect/cybersecurity/cyber-investment-strategies.html

[20] Paul Proctor, David Furlonger, Gartner, *2024 Growth Agenda: Align Cybersecurity Investments With Business Growth (2024)*. Available at https://www.gartner.com/document/5500295

[21] Dr. S. Rajalakshmi, *The Intersection of Fintech, Regtech, and Cybersecurity: Challenges and Opportunities (2023)*. Available at https://ijisrt.com/assets/upload/files/IJISRT23APR1735.pdf

[22] Benny Firmansyah, Arry Akhmad Arman, *Generic Solution Architecture Design of Regulatory Technology (2023)*. Available at https://pdfs.semanticscholar.org/29e8/527a3600b2c4361b748f91bd1792f003cf9b.pdf

[23] FINRA, Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry (2018). Available at https://www.finra.org/sites/default/files/2018_RegTech_Report.pdf