TechVision RESEARCH

Multicloud Cybersecurity Reference Architecture

Published 28 October 2022

Abstract

In our research reports, events, and consulting engagements, TechVision emphasizes that organizations must transform themselves into Digital Enterprises. In the wake of the pandemic, becoming a *secure* Digital Enterprise has morphed from being a "nice to have" to a matter of survival. It demands organizations develop agile and adaptive security programs and technology capabilities well-aligned to business and IT. Only though these capabilities can Digital Enterprises safely optimize responses to business opportunities, regulatory requirements, and changing IT environments or threat landscapes in today's environment.

This report provides a Multicloud Cybersecurity Reference Architecture and guidance for digital enterprises. It contains business and technical views that security teams can customize to fit their specific needs. It describes high-level functional components and capabilities, maps them to industry-standard control frameworks, and identifies the business stakeholders to align with for the purpose of adapting to local conditions. This report can be used by security/risk teams and executive leadership to get a logical understanding of security capabilities, enable cross-functional alignment of security projects or activities, measure their effectiveness, facilitate compliance towards securely supporting the digital transformation of an organization.

Authors:

Dan Blum
Principal Consulting Analyst
dan@techvisionresearch.com

Table of Contents

Executive Summary

The TechVision Research Security Reference Architecture provides guidance on identifying the business security context for an organization, and for selecting and prioritizing security-related processes and functional or technical capabilities for the IT environment. It also maps the capabilities to NIST Cybersecurity Framework (CSF) controls for convenient linkage to IT Governance, Risk, and Compliance (IT GRC) and solution architecture management tools.

The Security Reference Architecture models both security-related processes and security technologies across digital enterprises' multi-cloud and edge system IT environments. It identifies capabilities required to support distributed security systems; enterprise security operations and services; customers, partners, and suppliers; and the enterprise IT/OT environment.

The Business View of the Security Reference Architecture depicts the business context for the security program, security controls, and enterprise security infrastructure required for a Digital Enterprise.

The Functional View maps security-related technologies into those required for security management and control systems, security monitoring, incident response, vulnerability and configuration management, network security, identity and access management, and information protection. This view also shows the linkages to security-related processes, IT service management, and the enterprise IT/OT environment.

Clients can use the Reference Architecture to get a logical understanding of security capabilities, enable cross-functional alignment of security projects or activities, measure their effectiveness, and facilitate compliance as well as digital transformation of the business.

Introduction

Digital transformation is accelerating, demanding better security. The global response to the COVID-19 pandemic forced most businesses to send their staff home to "shelter in place" or shut down in-person operations such as malls, movie theaters, or manufacturing plants entirely. A great many of the business processes that continued operating did so only through digital processes and telecommuting. As CEO Satya Nadella famously said: "Microsoft has seen two years' worth of digital transformation in just two months of its third quarter (January-March period)."

Digital transformation and remote work or digital delivery models demand more cybersecurity, not just because they mean "more IT" but also "riskier IT." Technologies like mobile devices, social networks, cloud computing, artificial intelligence (AI), and the Internet of Things (IOT) have often emerged without adequate security built in. They disrupt existing security models built for older generations of technology. And as we rely more heavily on digital capabilities, this virtual world blends with physical and social realms into something new that raises risks. Just imagine digital outages or cyberattacks stopping elevators, crashing vehicles, starting fires, exploding pipelines, or turning off medical devices.

Digital transformation depends on maintaining a security program across all lines of business. The stakes have never been higher. For enterprises, cybersecurity is a fundamental requirement to realize the full benefits of cloud computing, mobility, and the Internet of Things (IoT).

In many of our research reports and events, we have described the compelling need for businesses to transform into Digital Enterprises. Being a Digital Enterprise emphasizes the requirement to be adaptive to the marketplace with enterprise-wide agility that optimizes responses to events, and opportunities. Business buyers and consumers are becoming adept at finding exactly what they want, and enterprises must become equally adept in finding, and aligning the people, knowledge and operating assets to match.

The digital transformation introduces an increasing number of cloud and device-based applications and services requiring both localized and edge computing environments in addition to large scale centralized IT infrastructure. IoT adoption creates a massively distributed and hyper-connected population of endpoints supporting interactive 'read and respond' smart services. Added to this mix are workplace changes from Collaboration and Social Tools and Drag and Drop composition of low-code and no-code localized business infrastructure by Line of Business managers all leading to an increasingly distributed enterprise.

This granular, orchestrated approach to providing enterprise IT resources requires carefully constructed risk management and IT governance capabilities. It also shifts the focus of protection from the data center perimeter to the individual resources themselves – no matter where they are located. These key trends will not apply evenly to every organization but can be a starting point to consider in assessing your requirements and future state architecture. Digital enterprises must be guided by the following principles for security programs:

1. **Strategic alignment with business:** Although executive decisions on business initiatives affecting IT in any way are driving information risks, cybersecurity still isn't always considered strategic or well understood at the Executive and Board Levels. The Digital Enterprise requires security to be fully aligned with the business and IT culture, governance, and risk management processes through instrumented, quantified risk management programs.
2. **Low friction security controls:** Security programs must protect digital enterprise users, devices, and IT systems throughout the global multi-cloud and edge environment and provide a low friction user experience for end users, developers, and administrators. Key user-facing controls are transparent endpoint security and access through adaptive (aka zero trust) authentication and modern identity and access management (IAM) protocols.
3. **Automated, intelligent security services:** API's and microservices are critical to developing and adapting the tools of the Digital Enterprise. Security services must be built into DevSecOps Continuous Integration / Continuous Delivery (CI/CD) pipelines through automated processes. Security practitioners must integrate their control architecture with distributed IT environments using standard interfaces/protocols and artificial intelligence and machine learning (AI/ML) capabilities. Pervasive AI/ML can support automation and control, not just for security analytics, but also for functions such as access certification, multi-factor authentication (MFA), micro-segmentation, and more.
4. **Compliance-ready:** Continuous compliance with evolving privacy and safety regulations within the businesses' international and industry sector commercial and regulatory context.
5. **Cloud-ready or cloud-native:** With the digital transformation driving accelerated cloud migration, IT and security architectures must exhibit the five A's: agentless and scalable, API-driven, platform-agnostic, automated, and accurate.
6. **Cyber-resilient:** Lay the groundwork for sustaining a robust security program in the face of business disruption through contingency planning, incident response, and business continuity / disaster recovery (BC/DR) programs. Anticipate and detect threats or risks and respond or recover from cyberattacks with advanced security monitoring and operations.

What are Reference Architectures?

Reference architectures are standardized frameworks or technology models for a domain, sector, or field of interest. Reference models or architectures provide a common vocabulary, reusable designs, and industry best practices. They are not solution designs and as such are not meant to be implemented directly. Rather, they are used to guide more concrete efforts. Typically, a reference architecture includes common architecture principles, patterns, building blocks and standards.

Intended Audience and Title: This Security Reference Architecture is intended for security architects and security leaders. Its formal title is the Multicloud Cybersecurity Reference Architecture, and we also describe it as a Business-Driven Security Reference Architecture. It can be used to create business views of architecture and selected artifacts from a customer's work with it – such as a high level "target state" diagram – can be presented to business leaders. However, this document itself is *not* intended for direct consumption by a business-level audience.

Scope, or Level of Abstraction: Considering the broad scope of security programs and the technologies supporting them, we can understand reference architectures as tools to help develop the "Contextual", "Conceptual", and (in some cases) "Logical" levels of a full enterprise security architecture per Figure 1. It provides a very broad and comprehensive view of "how the pieces fit together" in security architecture. Those "pieces" aren't just technology capabilities but also people and process ones. Thus, it depicts how the security program will work at a high level. It indicates what technology components are to be used. But you'll have to go a level deeper in logical or solution diagrams to fully map out the implementation phase.

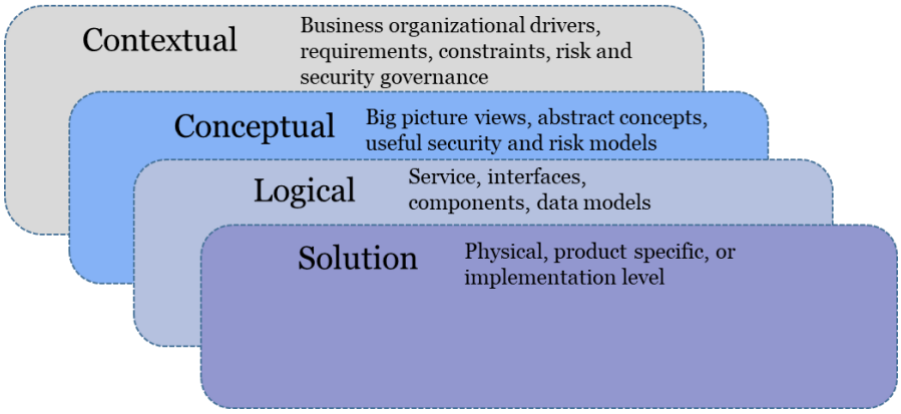

Figure 1: *A Simplified View of Enterprise Security Architecture*

Source: The four levels of enterprise security architecture are derived from Enterprise (EA) models and the Sherwood Applied Business Security Architecture (SABSA). [1]

Five Reasons to Use a Security Reference Architecture.

Why would you want to use a reference architecture? Here are five reasons why adopting a security reference architecture is a good thing.

1. **It helps you to get a logical understanding of security programs and technologies.** It provides a structure for taking your architecture governance model to the next level of detail regarding security. And it empowers customers with a vendor-neutral way of describing and specifying their security requirements.
2. **It supports digital transformation.** For many enterprises, transformation means their value chain is being redistributed among partners, service providers, and customers. If all parties speak the same language, use similar architecture frameworks or standards, and recognize the same boundaries between functions, processes and/or services, it will be

[1] "Enterprise Security Architecture: A Business-Driven Approach," John Sherwood, Andrew Clark, David Lynas, CMP Books, 2005

much easier to relate or recombine their elements in new ways.

3. **It encourages cross-functional alignment.** It does this by enabling security teams to agree with business and IT stakeholders on the business risk justification and functional requirements for a future state capability, its interfaces, and concept of operations in advance. The architecture or design of any controls can also be tuned to meet all stakeholders' assurance, compliance, usability or productivity, market, and customer needs.
4. **It facilitates measurement.** Often, the differences between companies or lines of business (LOB) are not in the design of their security-related processes, but in the execution. Using reference designs makes it much easier for customers to define for themselves "what good looks like," and to compare progress and execution results with others.
5. **It is important for regulatory compliance.** Often, reference architectures are prescribed (or at least strongly recommended) by regulators. For example, in the EU General Data Protection Regulation (GDPR) privacy protection principles, practices and processes are standardized and mandated. This leads to audit requirements and business reporting standards that are supported by a proper reference architecture.

The Multicloud Cybersecurity Reference Architecture

The reference architecture models the security-related processes and technical capabilities needed to meet current and future state business and IT requirements. It provides a high-level business view of the capabilities as well as more detailed functional views. Within these views it embeds additional views that show the high-level relationship between cybersecurity and the:

- Business and regulatory context
- Information technology (IT) capabilities
- Security programs and technologies

The reference architecture describes security people, process, and technology capabilities in terms of control domains that are mapped to the NIST Cybersecurity Framework. Also, we provide a Business Alignment Framework to associate capabilities or controls with security-related business roles and responsibilities within an organization. Figure 2 illustrates the overall structure of the reference architecture.

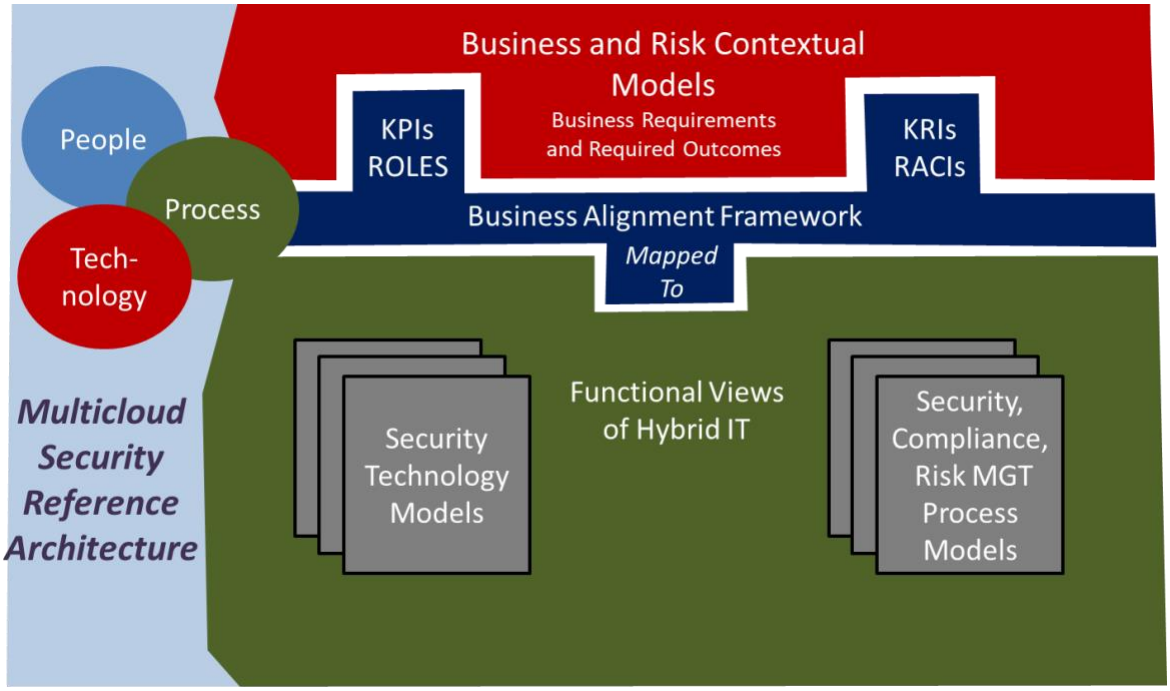

Figure 2: *Overview of the Multicloud Cybersecurity Reference Architecture*

A Business-Driven IT and Security Reference Architecture

Figure 3 illustrates how the business context relates to the IT and security program capabilities required for a Digital Enterprise. This includes:

- The business strategy, regulatory, risk, and capabilities context within which the organization's IT environment exists, and the security program operates.
- The enterprise executive, governance, administrative functions that control the security program, or with which the security program must align.
- Defined and authorized security program, governance, and risk management processes overseeing security policy, controls, and awareness.
- The global, multi-cloud and edge IT presence that provides all business IT capabilities for workforce users, business processes, customers, suppliers, partners, and the enterprise IT/OT resources.
- Distributed security capabilities (represented by the dark green squares in Figure 3) indicate the logical location of security controls through the hybrid multi-cloud stack (aka "digital estate.")
- The enterprise security operations and services as well as security control systems needed to provide centralized, or logically consistent, management over the distributed security capabilities.

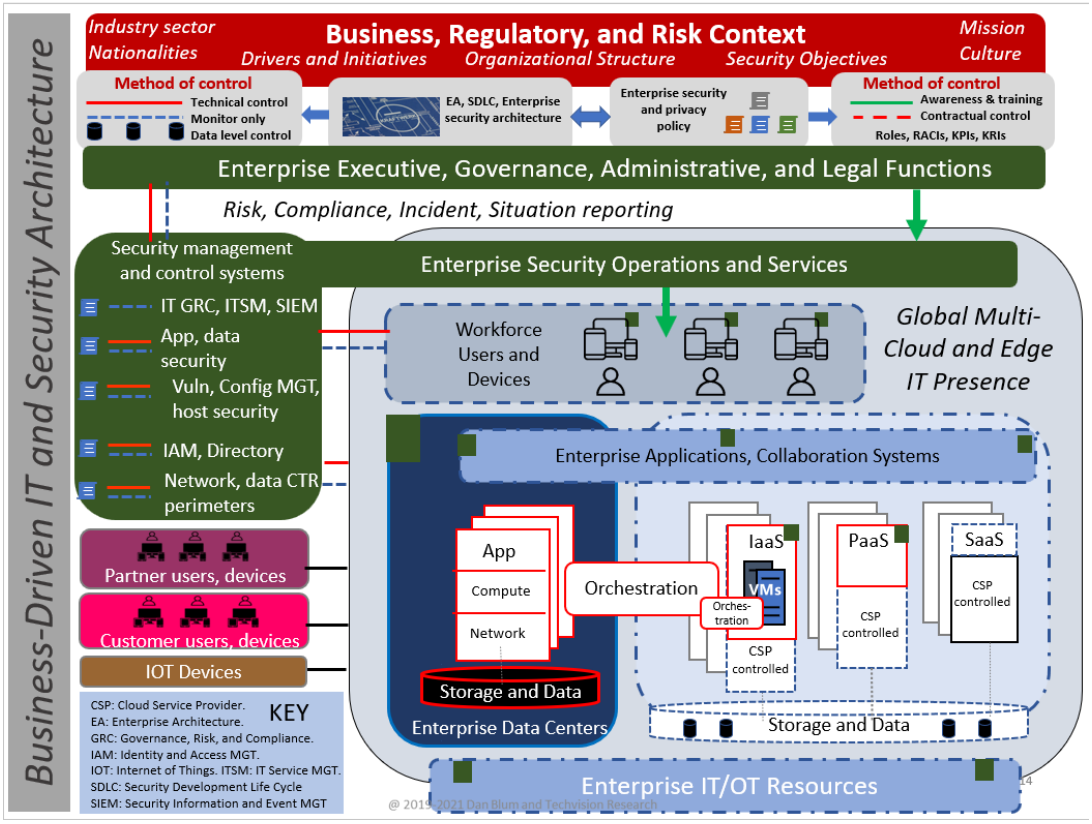

Figure 3: *Business-Driven IT and Security Reference Architecture*

Business Context

An organization's IT environment and security program always operate within a business context. Context can differ across vertical industries, national cultures, and it changes with business strategies and capabilities. For example, a traditional bank in a developing country operates very differently from a fast-growing retailer in the same country, and both bear scant resemblance to a large or mid-sized business or IT service provider in the U.S. Yet all have the same kinds of security objectives related to maintaining availability, confidentiality, integrity, privacy, and safety.

Enterprise Executive, Governance, Administrative Functions

These functions control the security program and/or the security program must align with them. For example, the Chief Counsel's Legal organization typically sets the direction on privacy law compliance programs which can have significant impact on security policy and operations. Business and IT governance or administration functions control Enterprise Architecture and the Software Development Life Cycle (SDLC). They also should influence and be aligned with enterprise security policy and architecture.

Security Program – Methods of Control

Security programs exist to manage risk in large part through people, process, and technology controls. Figure 3 identifies:

- Technical control, including the ability to actively control the operation of IT resources
- Monitoring (detection only) controls
- Data level controls: Controls on the data itself
- Awareness and training controls: Controls or programs to influence people's security-related behavior
- Contractual controls on employees, contractors, third parties, and other stakeholders

External Users and Devices

Includes partners' users and their devices, customers and their devices, and Internet of Things (IoT) devices that the enterprise interacts with but doesn't employ, sell, own, or manage.

Global Multicloud and Edge IT Presence

Provides all business IT capabilities for workforce users, business processes, customers, suppliers, partners, and the enterprise IT/OT resources. Consists of:

- Workforce users and devices (some managed, others unmanaged bring-your-own-device (BYOD) equipment)
- Enterprise applications and collaboration systems
- Enterprise Data Centers containing physical and virtual servers and networks as well as storage and data
- Public cloud services from cloud service providers (CSPs)
    - Infrastructure-as-a-service (IaaS) environments
    - Platform-as-a-service (PaaS) environments
    - Software-as-a-service (SaaS) applications
    - Note: Business Process-as-a-Service (BPaaS) and other AASs such as identity-as-a-service (IDaaS) aren't shown, but are important variants or specialties of the main three CSP delivery formats
- Enterprise IoT resources such as industrial, medical, or transportation devices; remotely managed devices sold to customers; and office devices such as printers or projectors.

Distributed Security Capabilities

The small green squares within Figure 3's global multicloud and edge IT presence box denote the logical location of security controls throughout the digital estate. Such controls may take the form of agent software, plug-ins, or shims but can also be provided by instrumentation built in at the native solution layer. For example, APIs or standard interfaces can expose native security functionality at the OS, application, or cloud solution layer for enterprise security control. This enterprise security control of the distributed security capabilities comes from the big green boxes, or the enterprise security operations and services described next.

Enterprise Security Operations and Services

Includes security teams, processes, and equipment as well as security management and control systems that provide centralized, or logically consistent, management over the distributed security capabilities in the global multi-cloud and edge IT presence. Some of the major security management and control systems at the business level include:

- IT Governance risk and compliance (IT GRC) and Security Information and Event Management (SIEM) through which the business obtains risk, compliance, incident, and situation reporting that can translate security policy into operation and deployment.
- System, vulnerability, and configuration management controls that protect endpoint devices, business applications, and compute infrastructure.
- Identity and access management (IAM) and directory services that control accounts, credentials, security-related roles, and permissions or privileges through the digital estate.
- Cloud networking and data center perimeter security that demarcates logical or physical boundaries for enterprise resources, and controls and monitors network traffic flows.

Security Architecture and Control Frameworks

It is important for any Security Reference Architecture – which operates at the conceptual or logical level - to align with industry standard risk management and control frameworks. Because IT GRC tools also reference these frameworks, the frameworks can serve as linkage, or integration points between the Security Reference Architecture and security solution level architectures such as Active Directory domain designs, Splunk log collection and normalization schemas, Kubernetes and Docker container deployment patterns, etc.

Figure 4 identifies 20 functional control domains used in the Security Reference Architecture and maps them to the NIST CSF control categories. The NIST CSF in turn maps these domains to the ISO 27001[2] and 27002[3] standards as well as to NIST's own drill down on control standards (NIST 800-53)[4] and ISACA's COBIT.[5]

TechVision Research customers using any of these control frameworks can in turn map from the Security Reference Architecture to their IT GRC tools (from RSA, IBM, SAP, ServiceNow, MetricStream, etc.) or solution architecture management tools such as PlanView or Flexera.

---

[2] International Standard ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition), ISO/IEC, 2013
[3] International Standard ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls, ISO/IEC, 2013
[4] "NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, NIST, April 16, 2018. Accessed at http://dx.doi.org/10.6028/NIST.SP.800-53r4, April 2013
[5] "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT", ISACA, 2012. accessed at http://www.isaca.org/cobit/Pages/CobitFramework.aspx

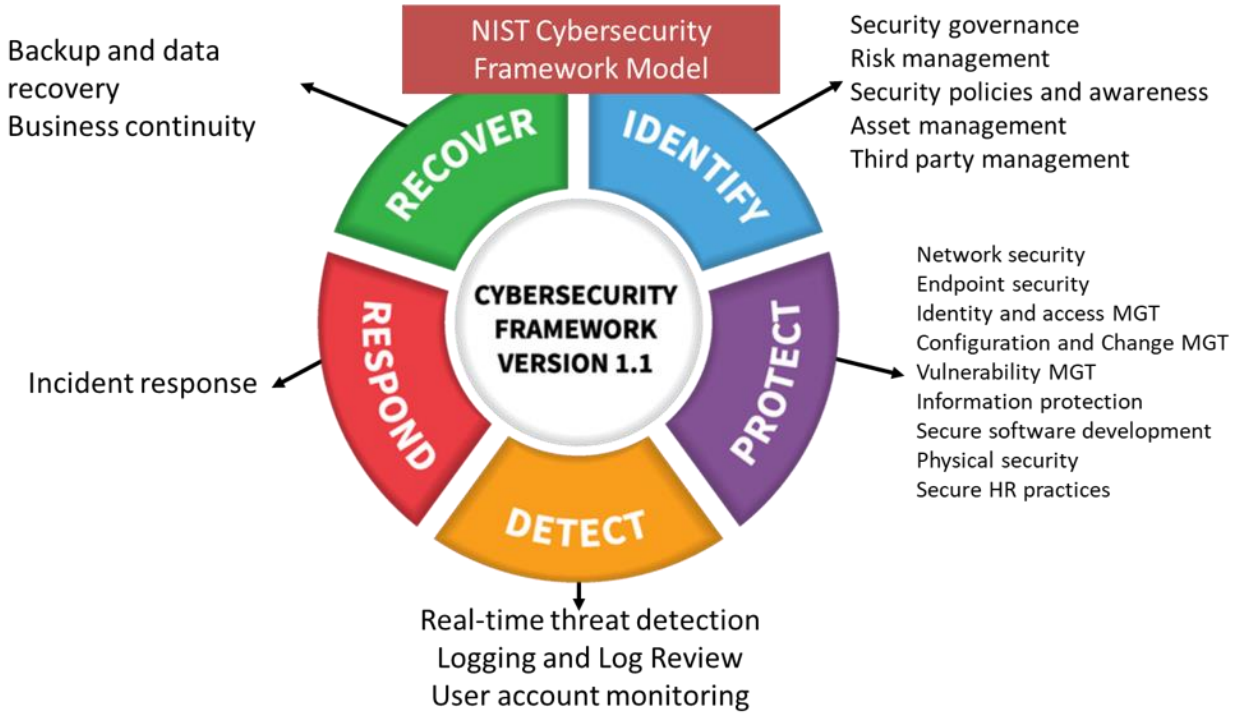

Figure 4: *Security Reference Architecture Functional Domains*

Source: Adapted from Figure 7-1 in "Rational Cybersecurity for Business" (available for complimentary download)[6] Chapter 6, "Establish a Control Baseline" explores a similar control model from the business alignment perspective in detail.

Selecting and Aligning Controls

Table 1 maps selected business-level capabilities to functional security domains and the high-level NIST CSF controls. Additional business level capabilities are described as security-related processes in a subsequent section. Note that each NIST CSF control is tagged with the following category coding from the CSF model: ID (identify), PR (protect), DE (detect), RS (respond), RC (recover). Also, because aligning security controls with the business at the governance level is just as critical as getting the technology right, Table 8 in the Business Alignment Framework section provides a detailed mapping from key business stakeholders to each functional control domain. TechVision Research clients can work with the Reference Architecture and Table 8 to make the connection from architecture to operations.

[6] "Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment," by Dan Blum, 2020, published by Apress, available at: https://www.apress.com/gp/book/9781484259511

Business-Level Capability	Functional Domains	NIST CSF Controls
Interpreting the business regulatory and risk context	Security governance, risk management	• ID.GOV: All 4 controls • ID.BE: Business environment • ID.RA: Risk assessment • ID.RM: Risk management • ID.SC: Supply chain risk
Organizational policies	Security policy and awareness	• ID.GV-1: Organizational policy • PR.AT: all 5 Awareness and training controls
Contractual control	Third party (vendor and supplier) management, Secure HR practices	• ID.SC: Supply chain risk • PR.IP-11: Cybersecurity included in HR practices

Table 1: *Business-Level Security Controls Mapping to NIST CSF*

The next level of the Security Reference Architecture shows security-related process and technology capabilities in greater detail as illustrated in Figure 5 and 6.

Security Related Processes

Security programs must be provided through security-related processes and coordinated through their own Security Program Management process and tools. Figure 5 diagrams key security processes that support or drive the technologies shown later, in Figure 6. These processes are highly inter-related. For example, Risk Management assesses some of the business's top risks by analyzing risks to its most critical assets as identified in a Business Control Management (BCM) Business Impact Assessment's (BIA) inter-dependency analysis. The BIA sub-process, in turn, cannot be performed without obtaining input from the Asset Management process or system.

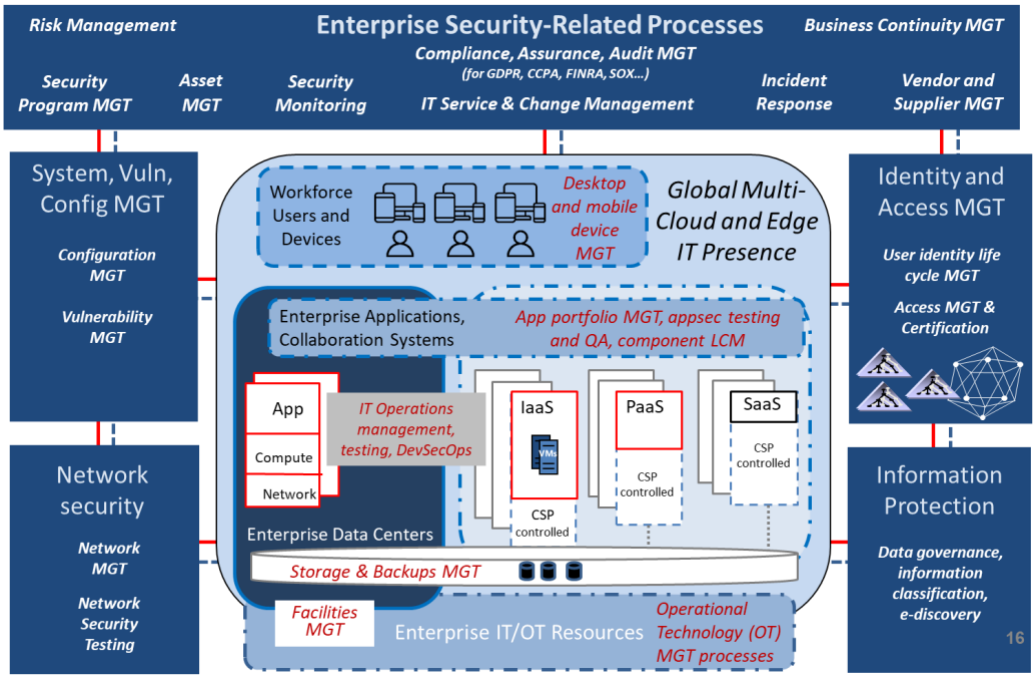

Figure 5: *Security-Related Processes View*

To make the linkage between security-related processes, functional control domains, controls, and stakeholders:

- Table 8 in the Business Alignment Framework section maps each functional control domain to the types of business stakeholders that, in many organizations, must be engaged in planning and delivering the required capabilities.
- Table 9 in the Business Alignment Framework section maps the security-related processes into functional control domains.
- The subsequent section - Functional View of Technologies and Capabilities - map the functional control domains to NIST CSF controls.

Functional View of Technologies and Capabilities

Figure 6 provides a functional view of security-related technologies or capabilities. This view is similar to a Technical Reference Model in an EA framework.

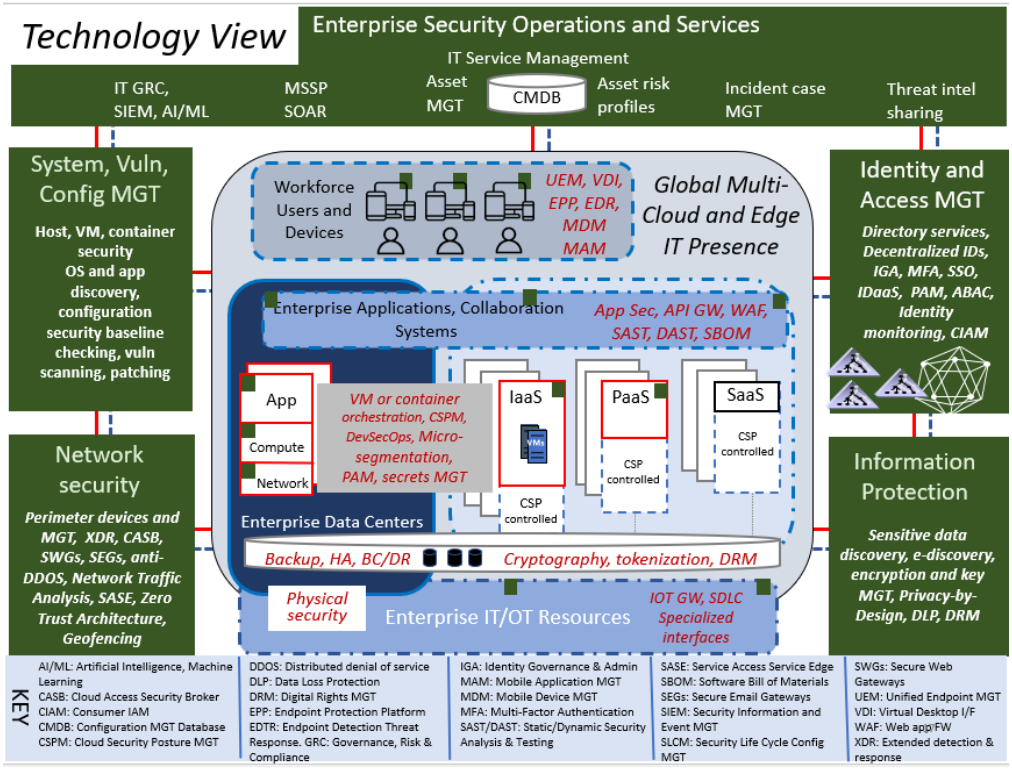

Figure 6: *Security Reference Architecture Technology View*

From this level, practitioners can navigate deeper into the functional requirements for:

- Distributed security controls throughout the multi-cloud environment
- Enterprise security operations and services
- Security management and control systems for
    - IT risk and security service management
    - Real-time threat, anomaly, and control deficiency monitoring and analytics
    - Host security, vulnerability, and configuration management
    - Risk, compliance, and incident reporting
    - Network and data center protection
    - Application security
    - Information protection
    - Identity and access management (IAM)

Distributed Security Controls throughout the Multicloud Environment

Distributed security controls are required to protect the multi-cloud environment at all points. They are managed by third party service providers, decentralized IT teams, business units, or users but can also be inventoried, monitored, or even directly controlled through local APIs or interfaces from the enterprise level.

Digital enterprises must make architectural decisions about when to insert enterprise-level controls into the multi-cloud environment and/or how to manage or instrument native cloud and OS-level security controls.

The families of distributed security controls used throughout the digital estate include:

- Unified endpoint management and security
- Compute infrastructure security
- Enterprise application and collaboration system security
- Information and storage level security
- Enterprise IOT security

About TechVision

World-class research requires world-class consulting analysts, and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skillsets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Dan Blum, Principal Consulting Analyst at TechVision Research, is an internationally recognized strategist in cybersecurity and risk management with over 30 years of experience in IT, security, risk, and privacy. His book "Rational Cybersecurity for Business" is a Security Leaders' Guide to Business Alignment. He was a Golden Quill Award winning VP and Distinguished Analyst at Gartner, Inc., has served as the security leader at several startups and consulting companies, and has advised 100s of large corporations, universities and government organizations. Mr. Blum is a frequent speaker at industry events and participates in industry groups such as ISACA, FAIR Institute, IDPro, ISSA, CSA, and the Kantara Initiative.

A Founding Member of the Kantara Initiative's IDPro group and honored as a "Privacy by Design Ambassador", Mr. Blum has also authored two books, written for numerous publications, and participated in standards or industry groups such as ISACA, the FAIR Institute, IDPro, CSA, OASIS, Open ID Foundation, and others.

Mr. Blum's career has encompassed a wide gamut of experience. He has written countless research reports and has led consulting projects in North America and Europe, spanning Financial Services, Insurance and Manufacturing, Health Care, Higher Education, and the Public Sector.

During his tenure at Gartner, Mr. Blum held VP positions as a Distinguished Analyst and Agenda Manager with the Security and Risk Management Strategies analyst team. He led the effort to enhance and improve the Security Reference Architecture acquired from Burton Group. He managed successive cloud security track programs at the Gartner Catalyst conferences and spoke at Gartner Security Summit and other events. He also served as the Cloud Security Research lead at Gartner for Technical Professionals.

At Burton Group, Mr. Blum filled multiple roles over a 10-year period, initially serving as Senior VP and Consulting Practice Manager, then as Research Director for the Identity and Privacy Strategies team. He authored, co-authored, or directed all the initial identity Reference Architecture content and also co-founded the Burton Group's Security and Risk Management Strategies research service beginning in 2004.