TechVision RESEARCH

Security Reference Architecture

Published 29 November 2020

Abstract

In our research reports, events, and consulting engagements, TechVision emphasizes that organizations must transform themselves into Digital Enterprises. Becoming a *secure* Digital Enterprise demands organizations develop agile and adaptive security programs and technology capabilities well-aligned to business and IT. These capabilities will enable Digital Enterprises to safely optimize responses to business opportunities, regulatory requirements, and changing IT environments or threat landscapes.

This report provides a Security Reference Architecture and guidance for secure 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.

Authors:

Dan Blum
Principal Consulting Analyst
dan@techvisionresearch.com

Table of Contents

Executive Summary

This document is a summary of the full TechVision Research Security Reference Architecture, which we have developed to help create better security programs and future-proofed, business-aligned security architectures and solutions in Digital Enterprises.

In many of our research reports and events, we have described the compelling need for businesses to transform into Digital Enterprises. For most types of organizations, becoming a digital enterprise depends adaptive to the marketplace with enterprise-wide agility that optimizes responses to events, and opportunities while still maintaining a security program calibrated to enterprise risks across all lines of business. The digital enterprise security program must also support the following principles:

1. Strategic alignment with business
2. Low friction security controls
3. Automated, intelligent security services
4. Compliance-readiness
5. Cloud-ready or cloud-native
6. Cyber-resilient

The TechVision Research Security Reference Architecture provides guidance on identifying the business security context for a digital enterprise, and for selecting and prioritizing security-related processes and functional or technical capabilities to 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.

What are Reference Architectures?

Reference architectures are standardized frameworks or technology models for a domain, sector, or field of interest. They aren't solution designs, but instead typically identify common architecture principles, patterns, building blocks and standards.

Considering the broad scope of security programs and the technologies supporting them, we can understand reference architectures as existing at the "Conceptual" or "Logical" levels of a full Enterprise Architecture (EA) aligned security architecture (aka "enterprise security architecture).

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
2. It supports digital transformation
3. It encourages cross-functional alignment
4. It facilitates measurement
5. It is important for regulatory compliance

The TechVision Research Security Reference Architecture

The Security Reference architecture models the security-related processes and technical capabilities needed to meet current and future state business and IT requirements. It provides three primary views:

- A high-level Business View mapping security to the digital enterprise environment
- Functional View of security-related process capabilities
- Functional View of security technology capabilities

In addition, the Reference Architecture maps capabilities within the three views to 20 functional domains which it in turn aligns with standard security control frameworks via the NIST Cybersecurity Framework model.

Business View of Capabilities

The Business View of the Security Reference Architecture (Figure 1) identifies the business context for the security program, security controls, and enterprise security infrastructure 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 1) 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.

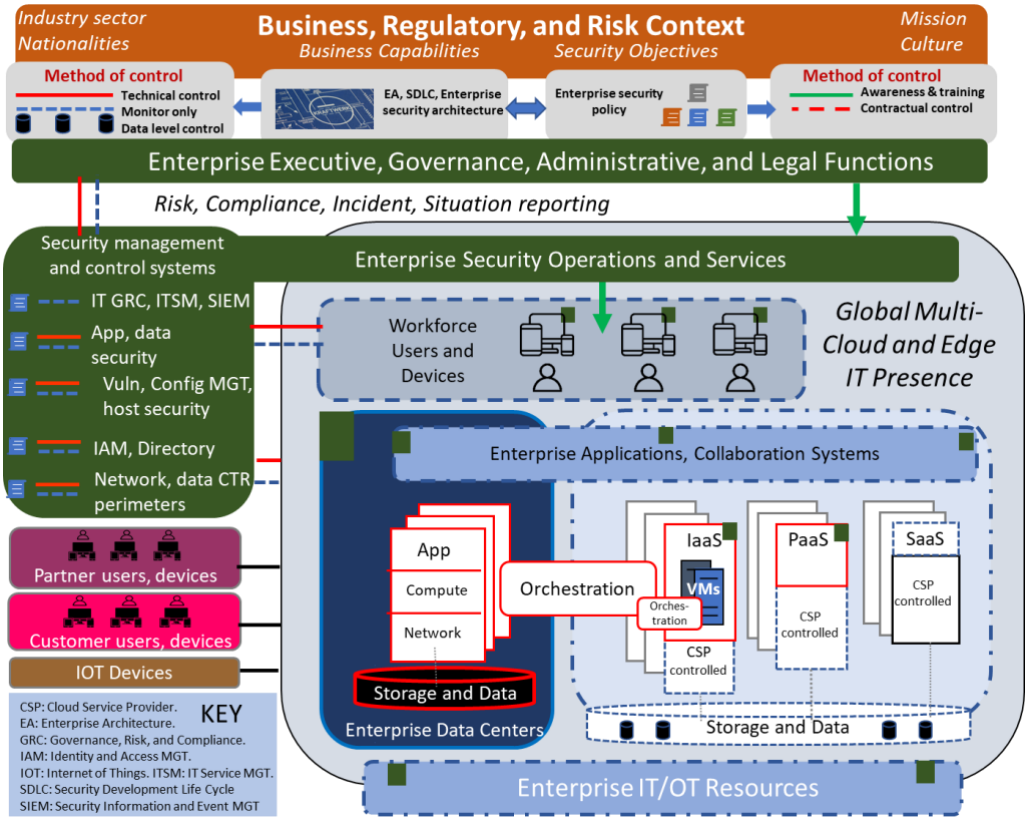

Figure 1: *Security Reference Architecture Business View*

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. The business-level Security Reference Architecture diagram identifies:

- Technical control, including the ability to actively control the operation of IT resources
- Monitoring (detective only) controls
- Data level controls: Controls on the data itself
- Awareness and training controls: Controls or programs to influence people's security 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 Multi-Cloud 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 1's global multi-cloud 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 busines obtains risk, compliance, incident, and situation reporting and can translate security policy into operation and deployment.
- System, vulnerability, and configuration management controls protect endpoint devices, business applications, and compute infrastructure.
- Identity and access management (IAM) and directory services control accounts, credentials, security-related roles, and permissions or privileges through the digital estate.
- Cloud networking and data center perimeter security demarcates logical or physical boundaries for enterprise resources, 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 2 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[1] and 27002[2] standards as well as to NIST's own drill down on control standards (NIST 800-53)[3] and ISACA's COBIT.[4]

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.

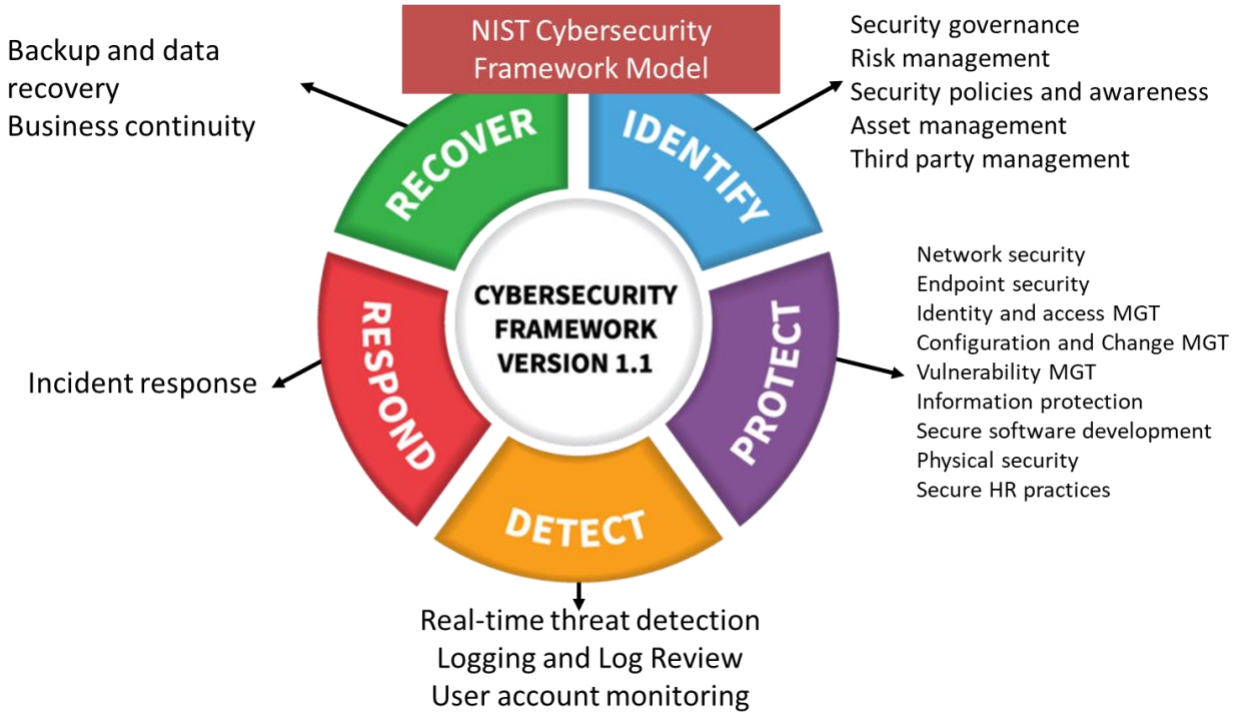

Figure 2: Security Reference Architecture Functional Domains

Source: Adapted from Figure 6-1 in "Rational Cybersecurity for Business" (available for complimentary download)[5] Chapter 6, "Establish a Control Baseline" explores a similar control model from the business alignment perspective in detail.

[1] International Standard ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition), ISO/IEC, 2013
[2] International Standard ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls, ISO/IEC, 2013
[3] "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
[4] "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
[5] "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

Security Related Processes

Security programs must be provided through security-related processes. Figure 3 diagrams key security processes that support or drive the technologies shown later, in Figure 4. 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.

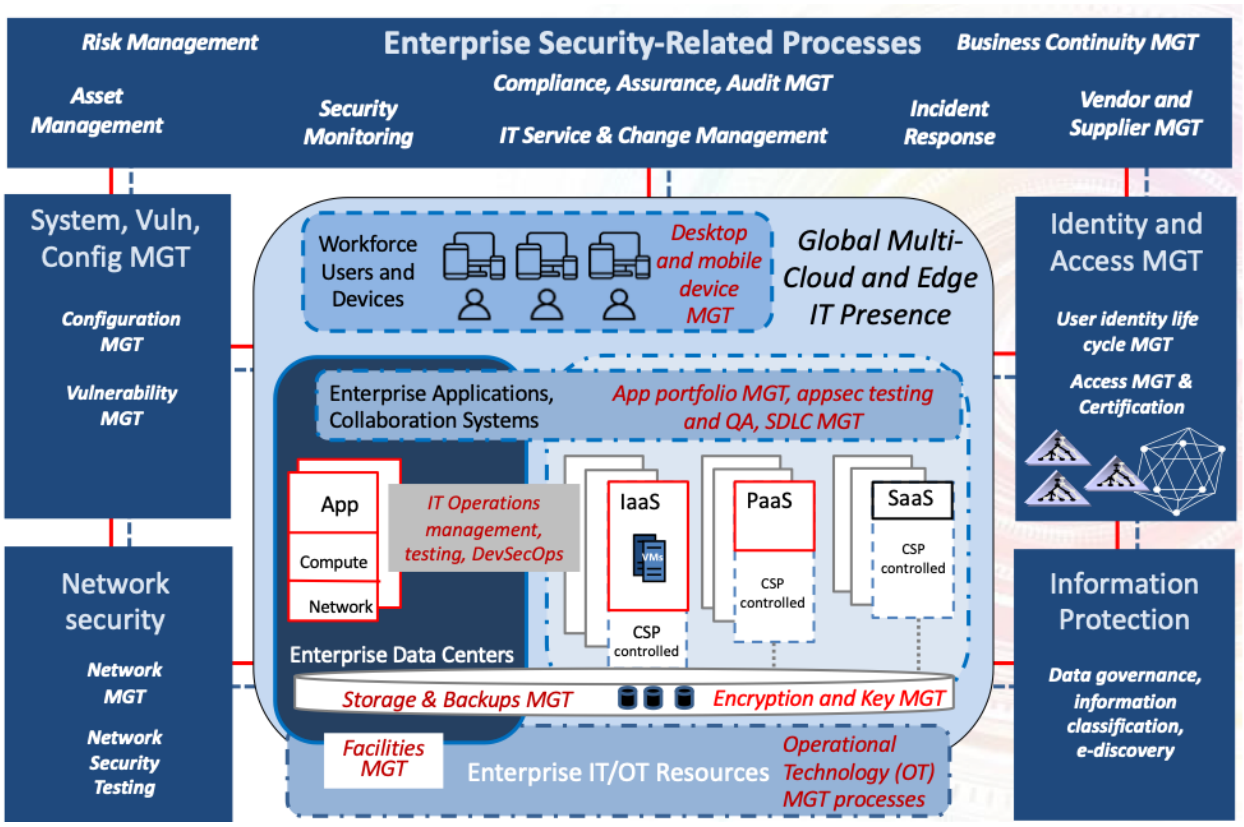

Figure 3: *Security-Related Processes View*

To make the linkage between security-related processes, functional control domains, controls, and stakeholders, the full version of the TechVision Research Security Reference Architecture provides two appendices and seven tables mapping to detailed security controls via the 20 functional control domains and the NIST CSF.

Functional View of Technologies and Capabilities

Figure 4 provides a functional view of security-related technologies or capabilities. This view is similar to a Technical Reference Model in an EA framework.

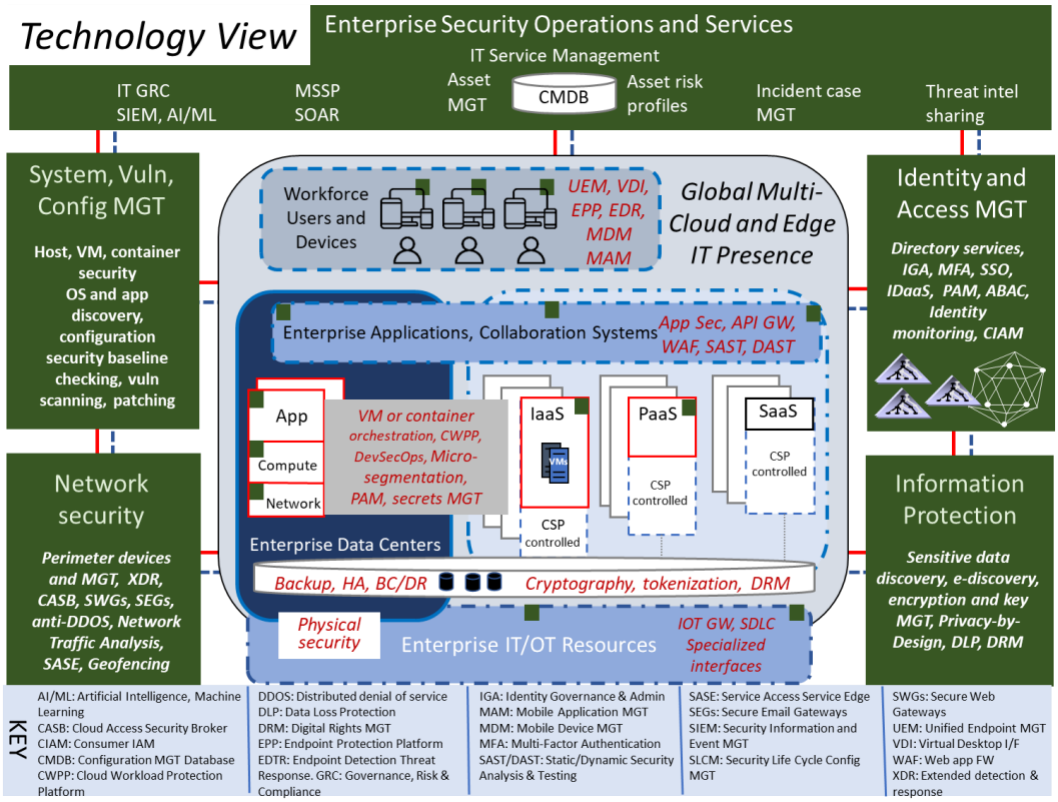

Figure 4: *Security Reference Architecture Technology View*

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)

Conclusion and Next Steps

Organizations need tools to identity their business security context, select and prioritize security-related processes and functional or technical capabilities, and put them into operation. The TechVision Research Security Reference Architecture identifies many security-related processes

and technology capabilities, puts them into a business and IT context, maps them to industry-standard control frameworks, and provides high level implementation guidance.

The full version of the Reference Architecture:

- Drill downs into the functional capabilities identified in Figures 3 and 4
- Maps the functional capabilities to the NIST CSF control map
- Maps the functional capabilities to a Stakeholder Map for business alignment
- Explains how to use the Security Reference Architecture to develop and operationalize a security strategy and architecture that fits your business
- Lays out two appendices and seven tables that map identified capabilities to detailed security controls via the NIST CSF

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 is an internationally recognized strategist in cybersecurity and risk management with over 30 years of experience in IT, security, risk, and privacy. His forthcoming 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.