

# Getting Security/Risk Right

## The Multi-Cloud Security Reference Architecture

1

*Slides by Dan Blum*

*Cybersecurity Security Strategist and Author  
November 8, 2022*

*Prepared for*

**TechVision**  
RESEARCH

*Contact me: LinkedIn, or email via  
[dan@techvisionresearch.com](mailto:dan@techvisionresearch.com)*

# Agenda

## ***What is a Security Reference Architecture?***

The Business View

Functional Views

A Business Alignment Framework

Next Steps

# What is a Reference Architecture?

Generic models or diagrams at the any architecture level that can serve as a starting point for organization-specific architectures.

Reference Architectures should:

- Fit cleanly into the big picture
- Be comprehensive enough to contain lower-level architectures, designs
- Be generic enough to be adapted to many clients, environments, contexts
- Future proof users against emerging, disruptive trends and opportunities

A Security Reference Architecture can be used to create part of an Enterprise Security Architecture

Intended audience: Security Leaders and Architects.\*

\* Although artifacts from the reference architecture aren't crafted for business leaders, they are designed to provide business-driven solutions that can be summarized or adapted for business reporting.

# Agenda

What is a Security Reference Architecture?

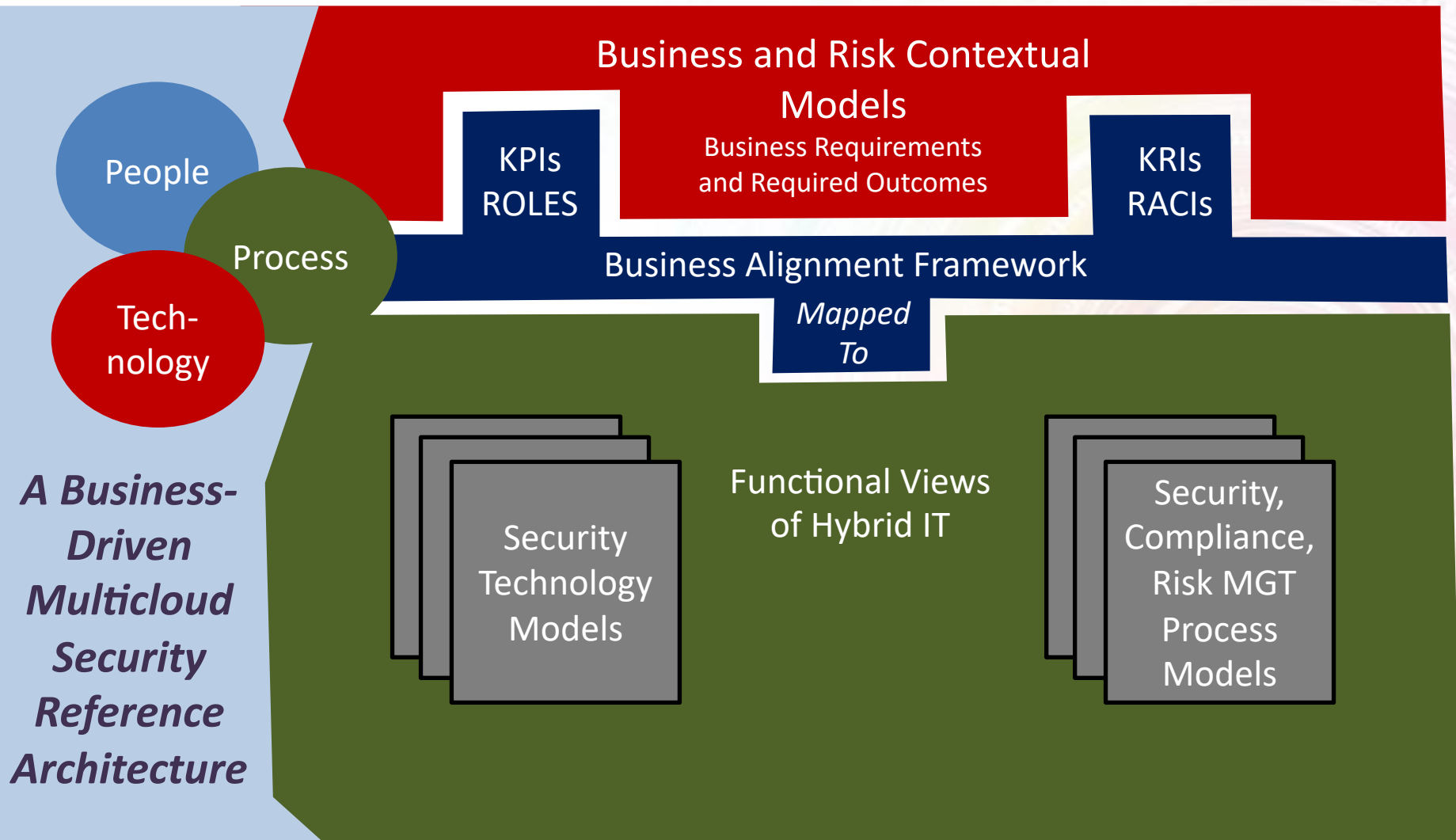
***The Business View***

Functional Views

A Business Alignment Framework

Next Steps

# Business Alignment



*Industry sector*  
*Nationalities*

# Business, Regulatory, and Risk Context

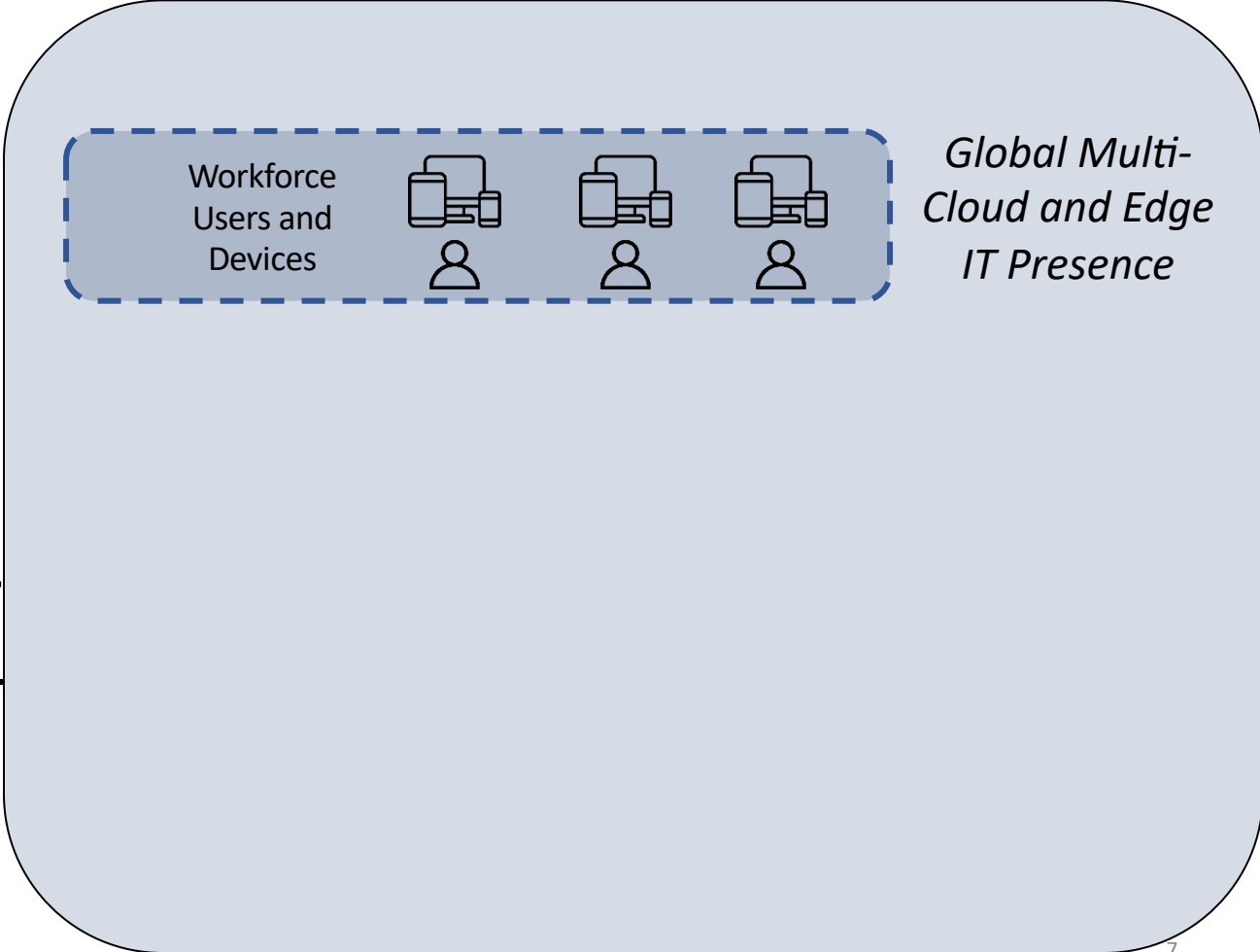
*Mission*  
*Culture*

*Drivers and Initiatives*

*Organizational Structure*

*Security Objectives*

# Business, Regulatory, and Risk Context



Industry sector  
Nationalities

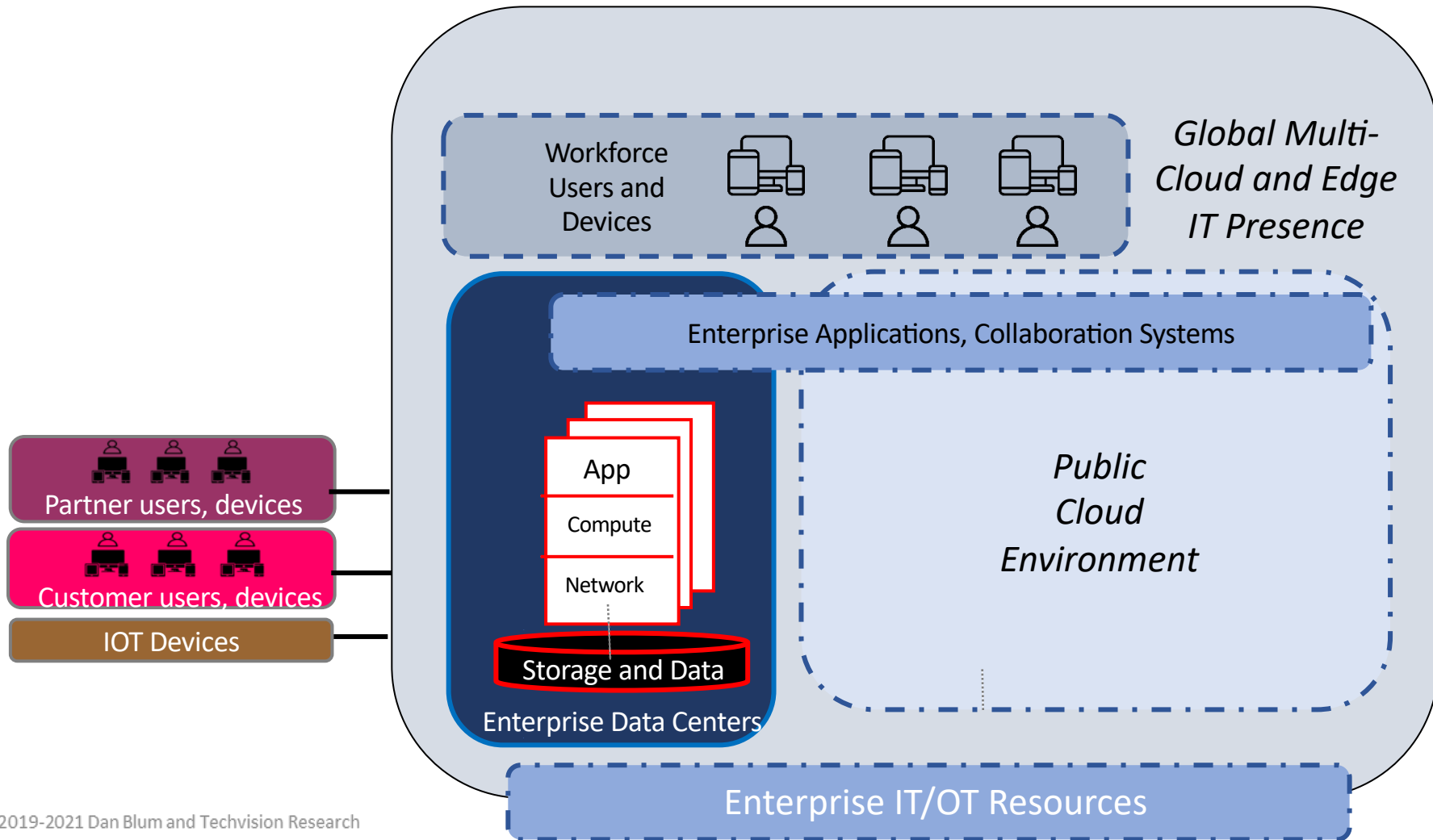
# Business, Regulatory, and Risk Context

Mission  
Culture

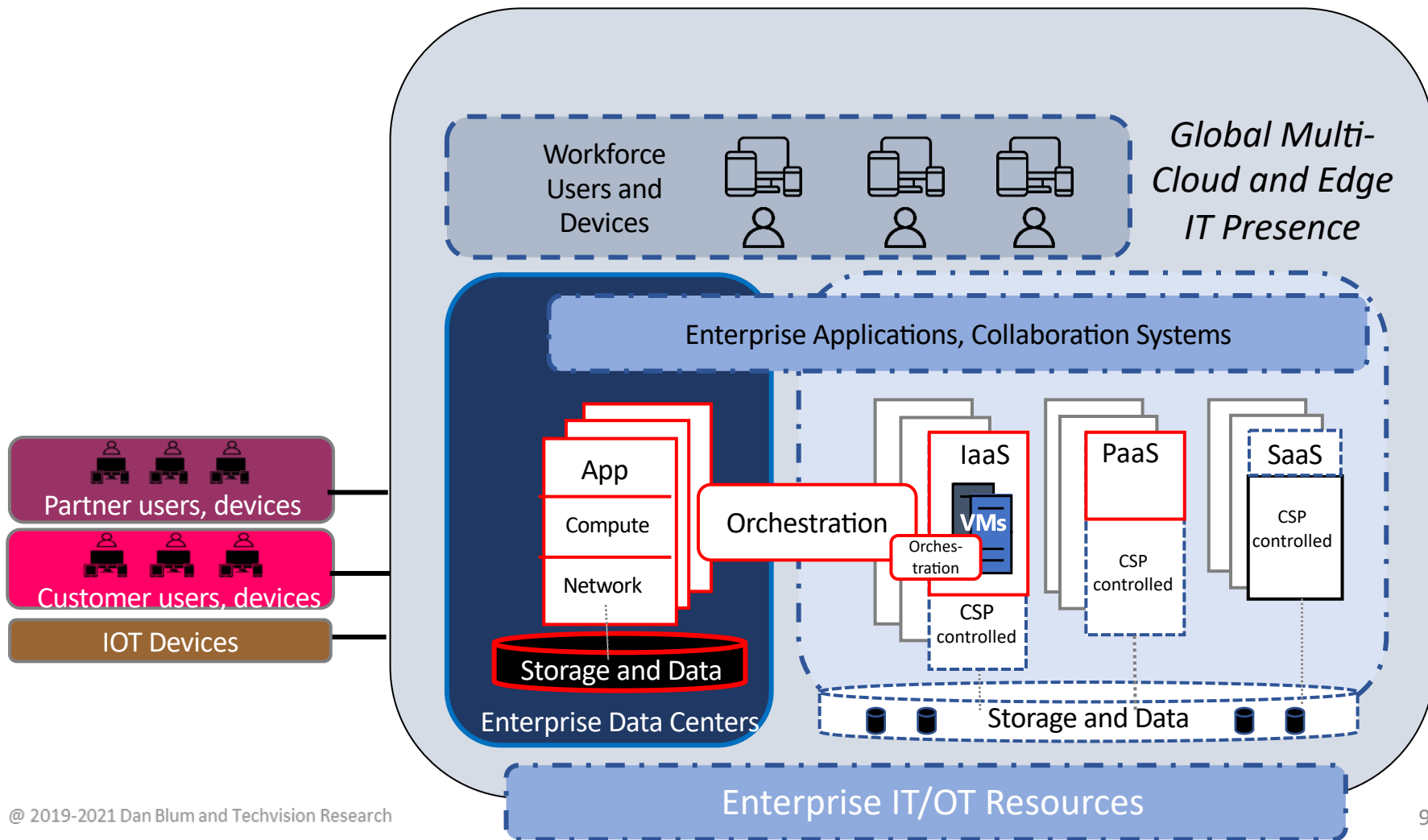
Drivers and Initiatives

Organizational Structure

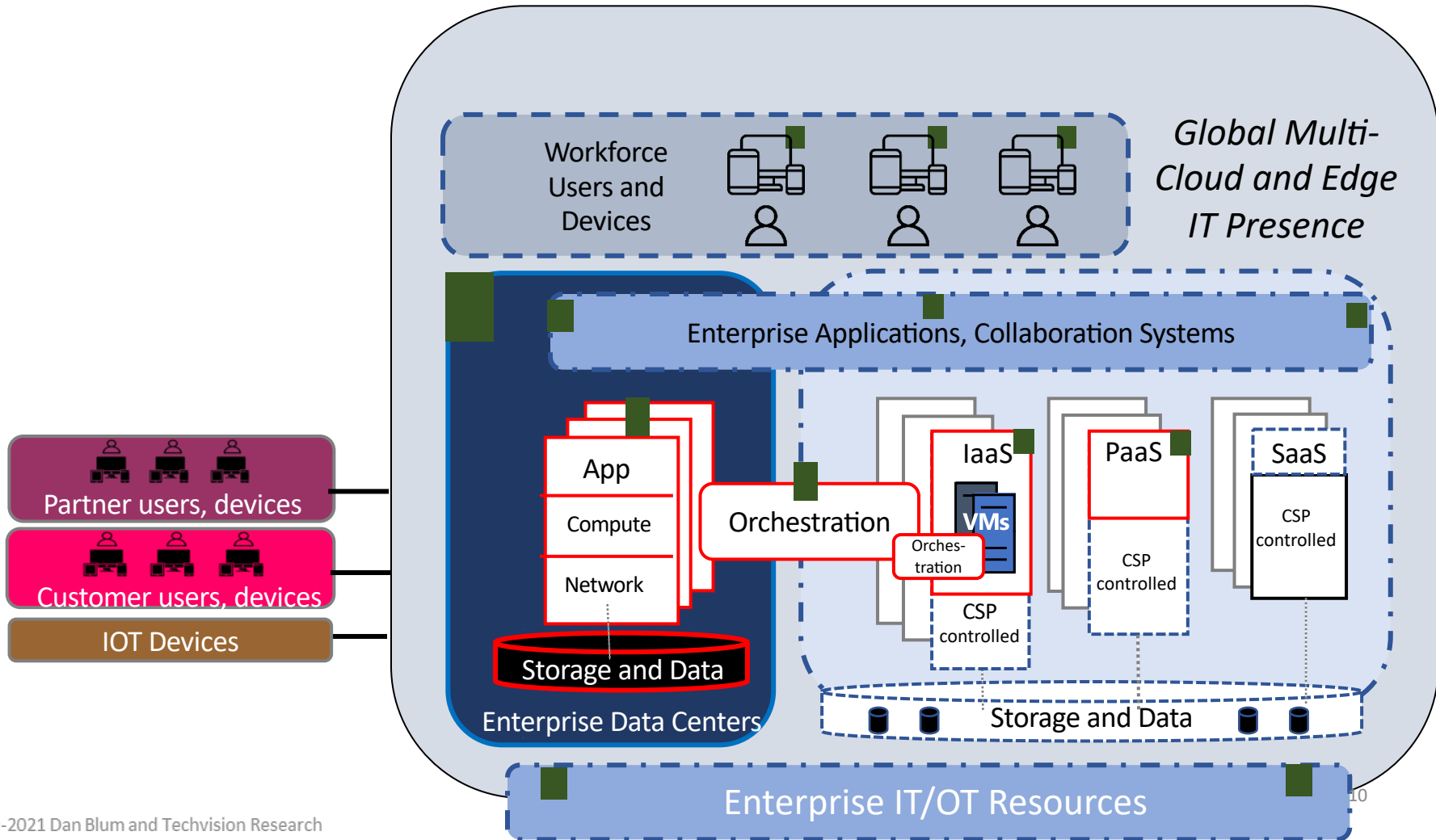
Security Objectives

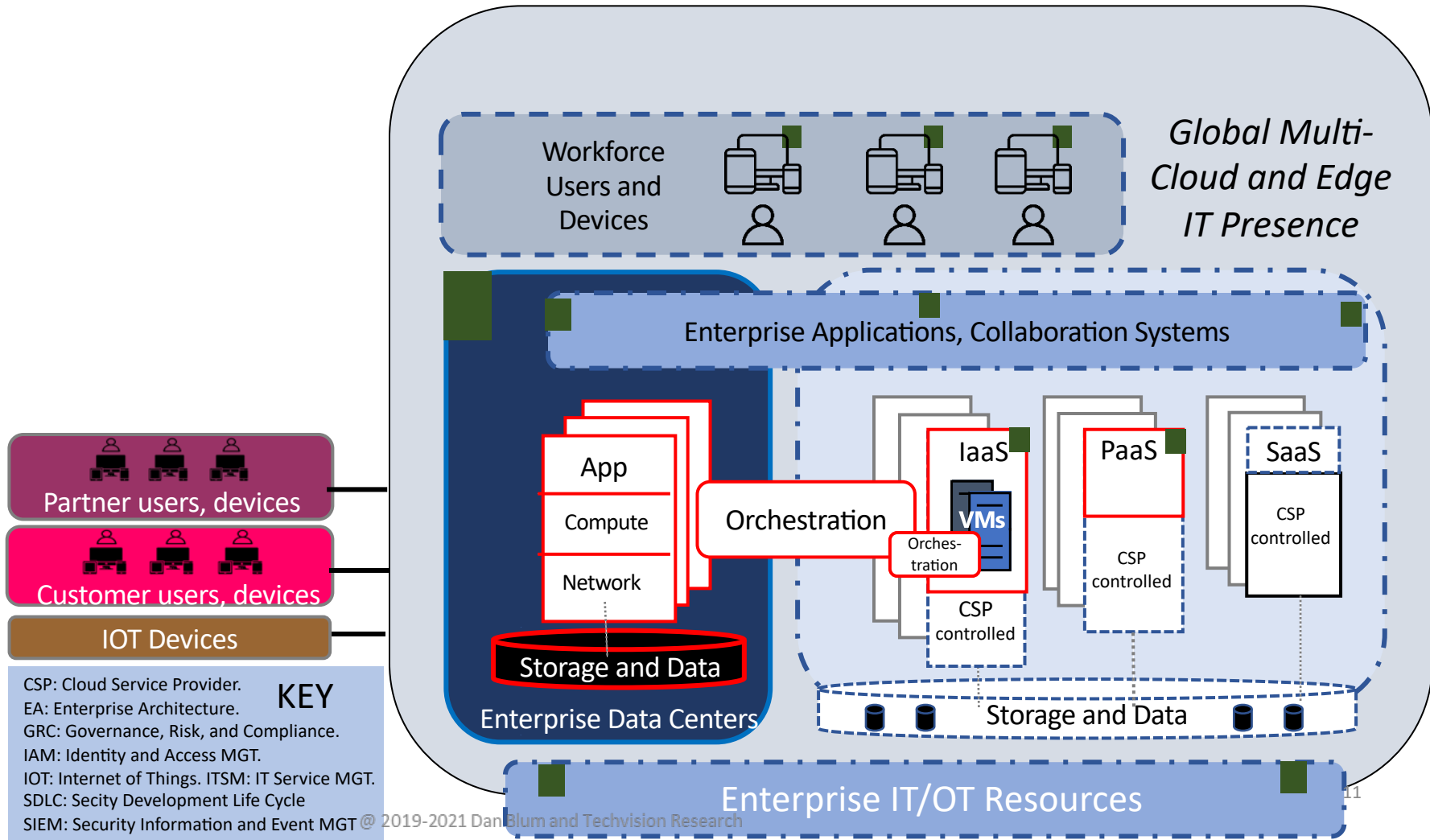
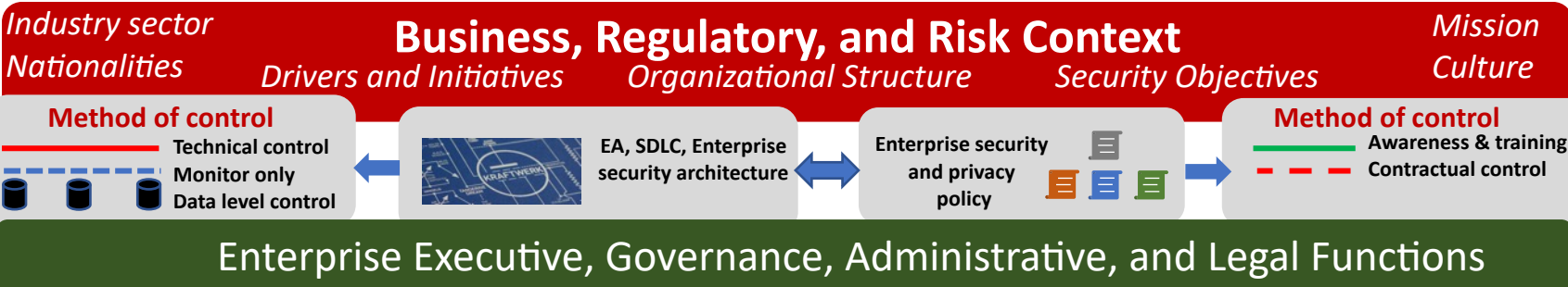




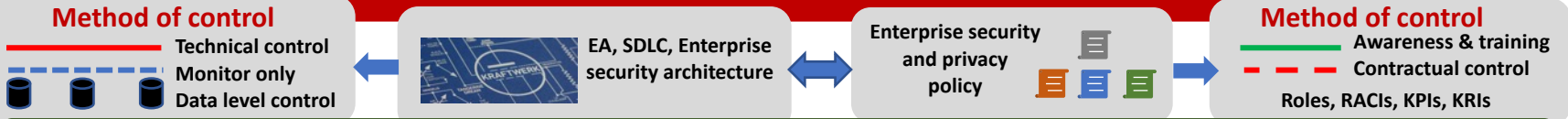


# Business, Regulatory, and Risk Context



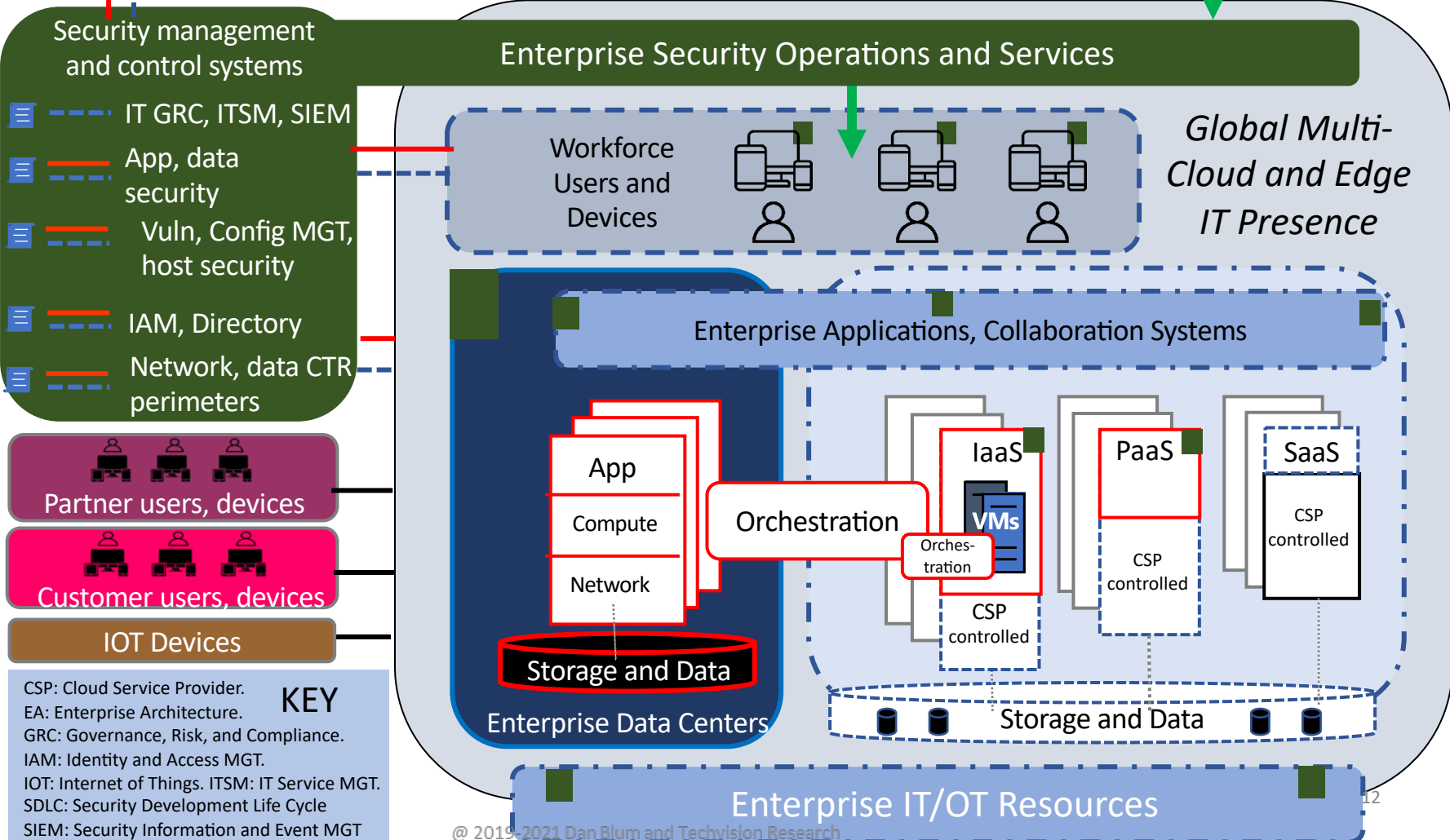


**Business, Regulatory, and Risk Context**



**Enterprise Executive, Governance, Administrative, and Legal Functions**

*Risk, Compliance, Incident, Situation reporting*



# Agenda

What is a Security Reference Architecture?

The Business View

***Functional Views***

A Business Alignment Framework

Next Steps

# Security Related Processes View

## Enterprise Security-Related Processes

## Process View

Risk Management  
Business Continuity MGT

Compliance, Assurance, Audit MGT  
(for GDPR, CCPA, FINRA, SOX...)

Security  
Program MGT

Asset  
MGT

Security  
Monitoring

IT Service & Change Management

Incident  
Response

Vendor and  
Supplier MGT

System, Vuln,  
Config MGT

Configuration  
MGT

Vulnerability  
MGT

Network  
security

Network  
MGT

Network  
Security  
Testing

Workforce  
Users and  
Devices



Desktop  
and mobile  
device  
MGT

Global Multi-  
Cloud and Edge  
IT Presence

Enterprise Applications,  
Collaboration Systems

App portfolio MGT, appsec testing  
and QA, component LCM

App

Compute

Network

IT Operations  
management,  
testing, DevSecOps

IaaS



CSP  
controlled

PaaS

CSP  
controlled

SaaS

CSP  
controlled

Enterprise Data Centers

Storage & Backups MGT



Facilities  
MGT

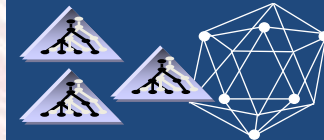
Enterprise IT/OT Resources

Operational  
Technology (OT)  
MGT processes

Identity and  
Access MGT

User identity life  
cycle MGT

Access MGT &  
Certification

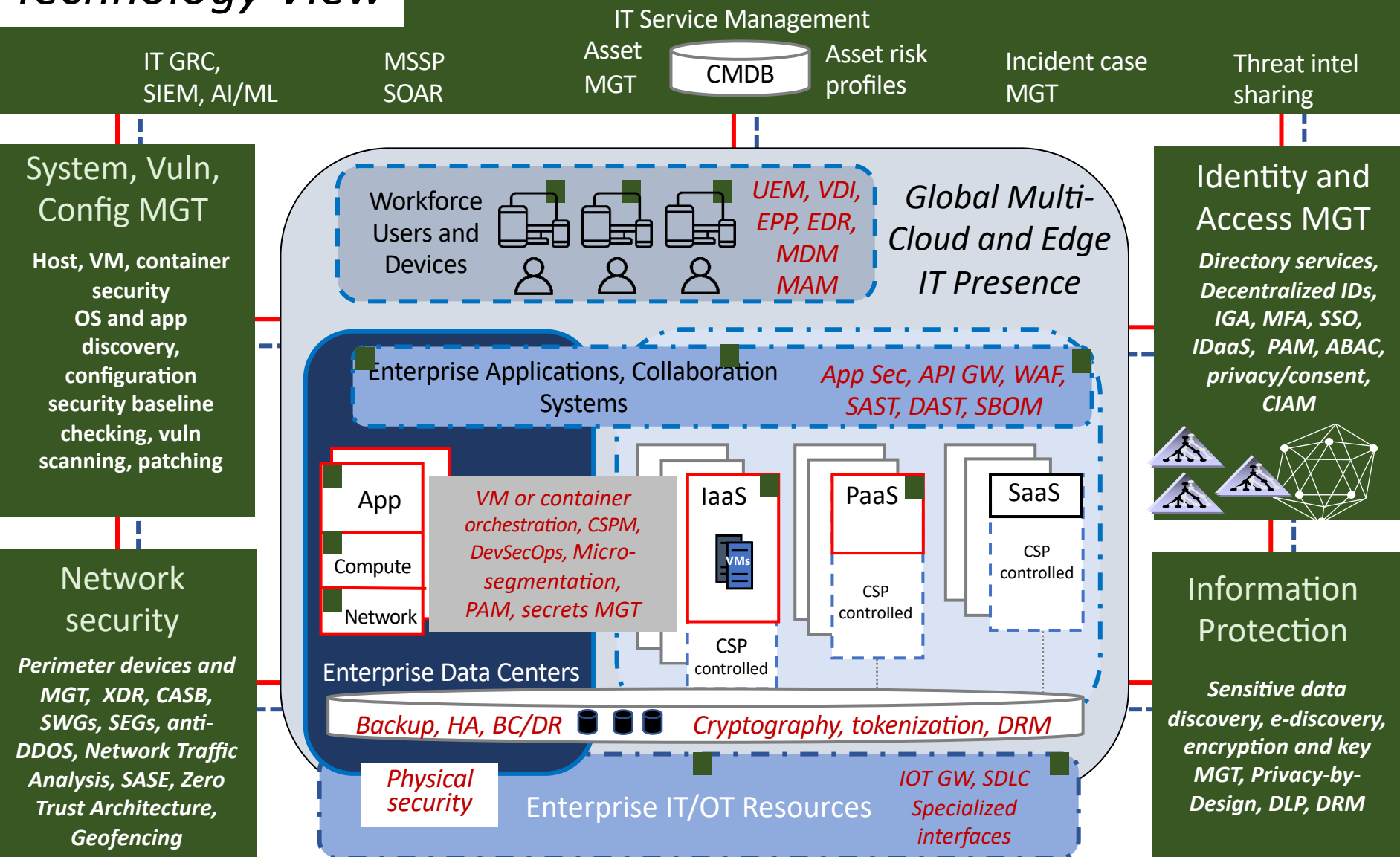


Information  
Protection

Data governance,  
information  
classification,  
e-discovery

# Technology View

## Enterprise Security Operations and Services

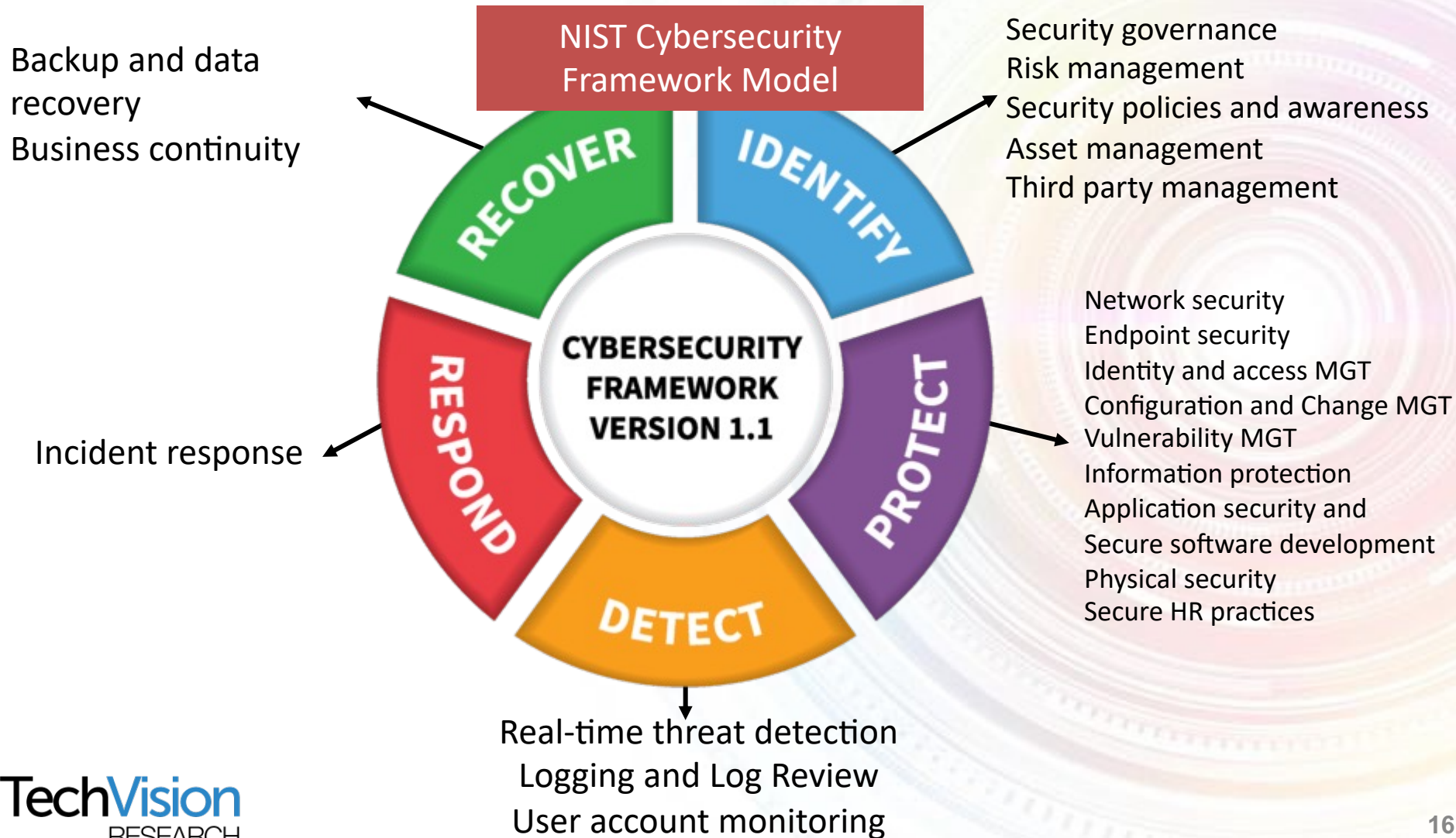


**KEY**

- AI/ML: Artificial Intelligence, Machine Learning
- CASB: Cloud Access Security Broker
- CIAM: Consumer IAM
- CMDB: Configuration MGT Database
- CSPM: Cloud Security Posture MGT
- DDOS: Distributed denial of service
- DLP: Data Loss Protection
- DRM: Digital Rights MGT
- EPP: Endpoint Protection Platform
- EDTR: Endpoint Detection Threat Response. GRC: Governance, Risk & Compliance
- IGA: Identity Governance & Admin
- MAM: Mobile Application MGT
- MDM: Mobile Device MGT
- MFA: Multi-Factor Authentication
- SAST/DAST: Static/Dynamic Security Analysis & Testing
- SASE: Service Access Service Edge
- SBOM: Software Bill of Materials
- SEGs: Secure Email Gateways
- SIEM: Security Information and Event MGT
- SLCM: Security Life Cycle Config MGT
- SWGs: Secure Web Gateways
- UEM: Unified Endpoint MGT
- VDI: Virtual Desktop I/F
- WAF: Web app FW
- XDR: Extended detection & response



# Map Functional Control Domains to NIST CSF





# Mapping Ref Arch Controls to NIST CSF

Business-Level Capability	Functional Domains	NIST CSF Controls
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
Enterprise security policy security and awareness	Security policy and awareness	ID.GV-1: Organizational policy PR.AT: all 5 Awareness and training controls
Software (or security) life cycle management	Secure software development	PR.AC-4: Access control (for applications) PR.AC-5: Network segregation PR.AT-1, 2: User awareness, training PR.DS-7: Separate development from production PR.IP-2: Implement secure SDLC PR.IP-12: Vulnerability management plan
Contractual control	Third party management, Secure HR practices	ID.SC: supply chain risk PR.IP-11: Cybersecurity included in HR practices
Managing the global, multi-cloud IT presence	Asset management	ID.AM 1-6: physical systems, software, applications, data discovered and assigned resource owners ID.RA-1: Identity asset vulnerabilities PR.DS-3: Assets managed
Maintaining availability	Backup, Recovery, Business Continuity	RC.RP-1: Recovery plan executed (Business Impact Analysis)

# Agenda

What is a Security Reference Architecture?

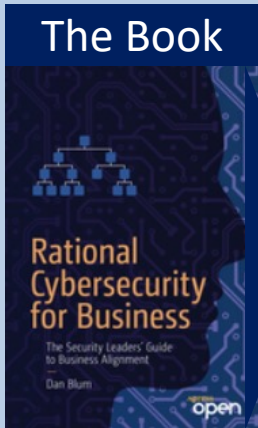
The Business View

Functional Views

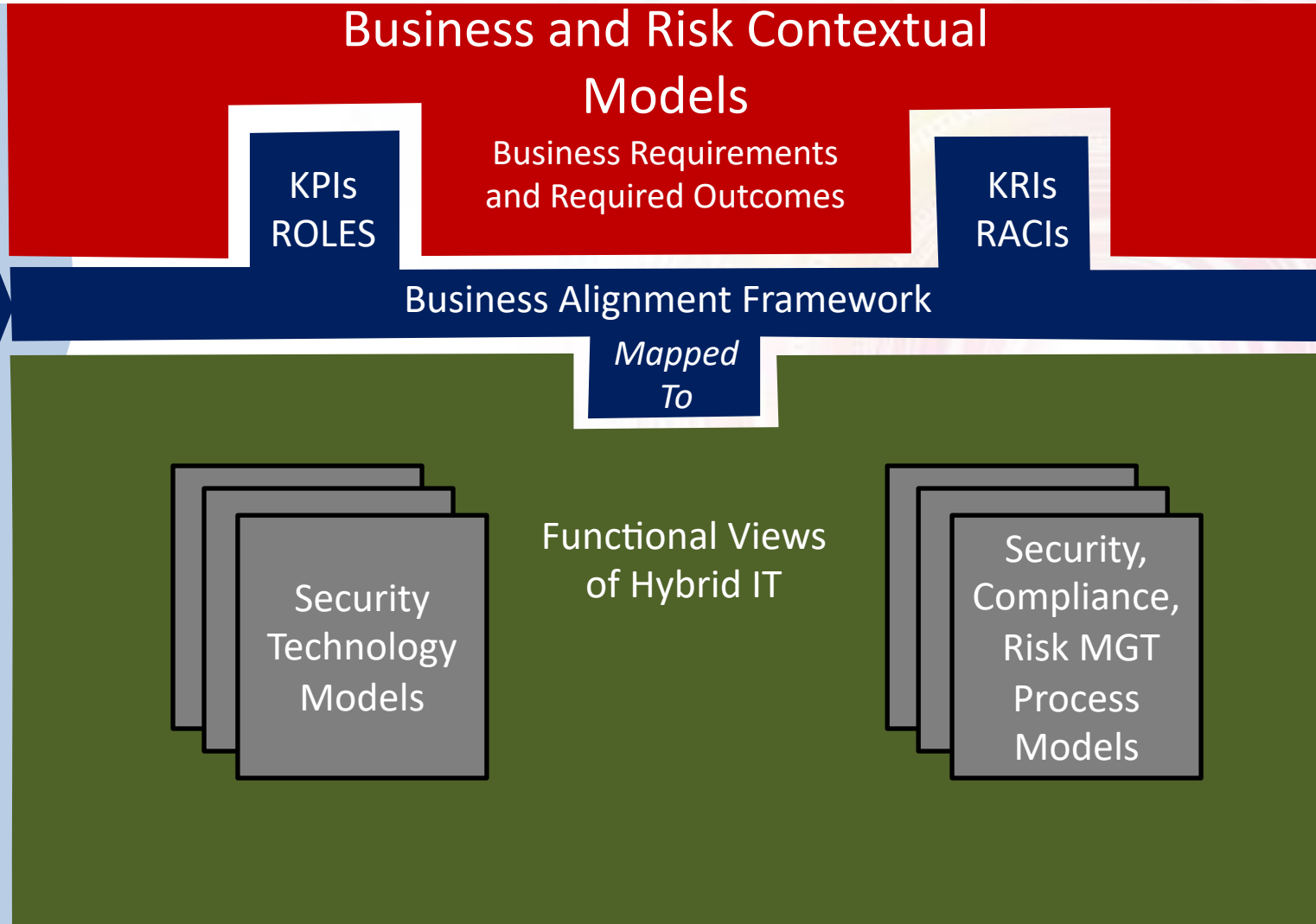
***A Business Alignment Framework***

Next Steps

# The Security Leader's Guide to Business Alignment

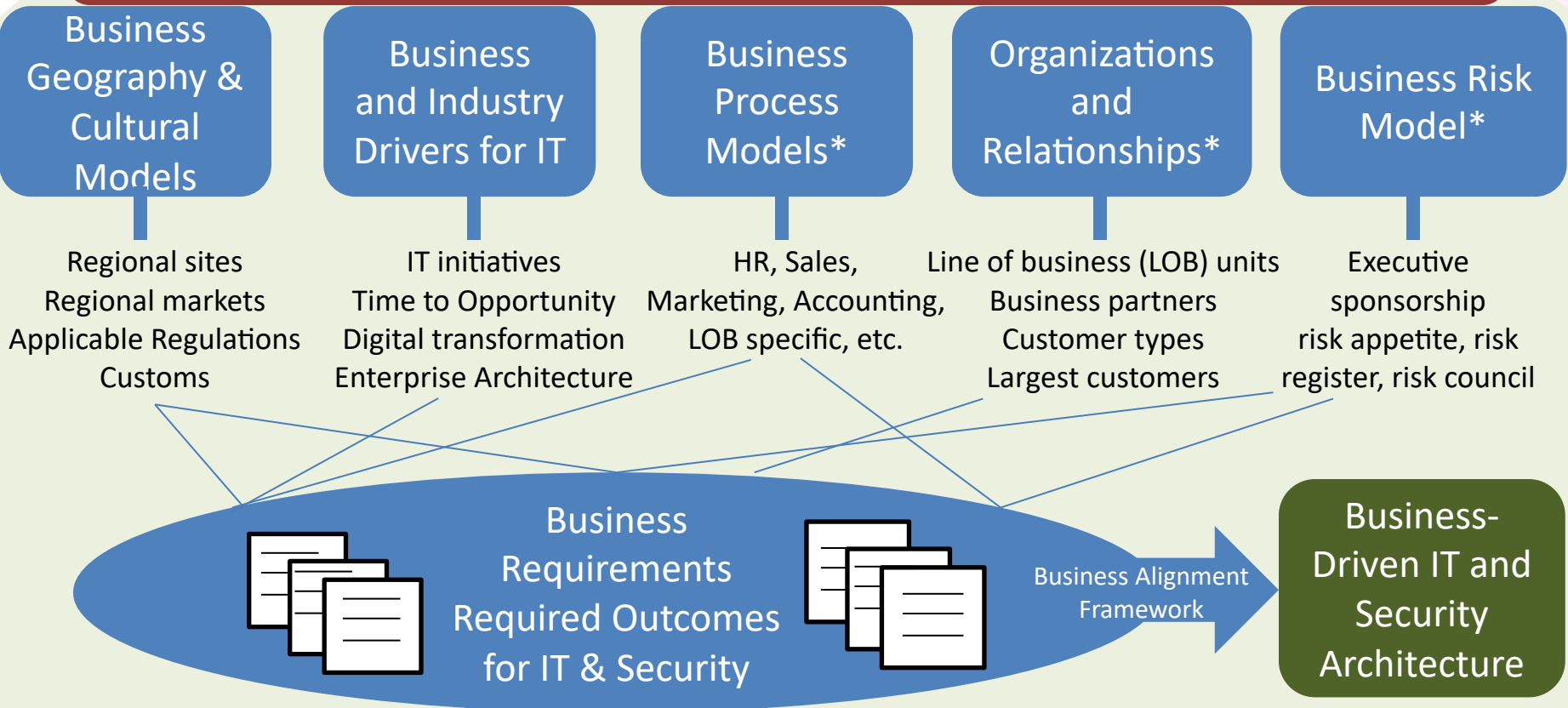


*Multicloud  
Security  
Reference  
Architecture*



# Business View

## Business, Regulatory, and Risk Context



\* Asterisked items also included in the “Enterprise Security Architecture: A Business-Driven Approach”

By John Sherwood, Andrew Clark, and David Lynas

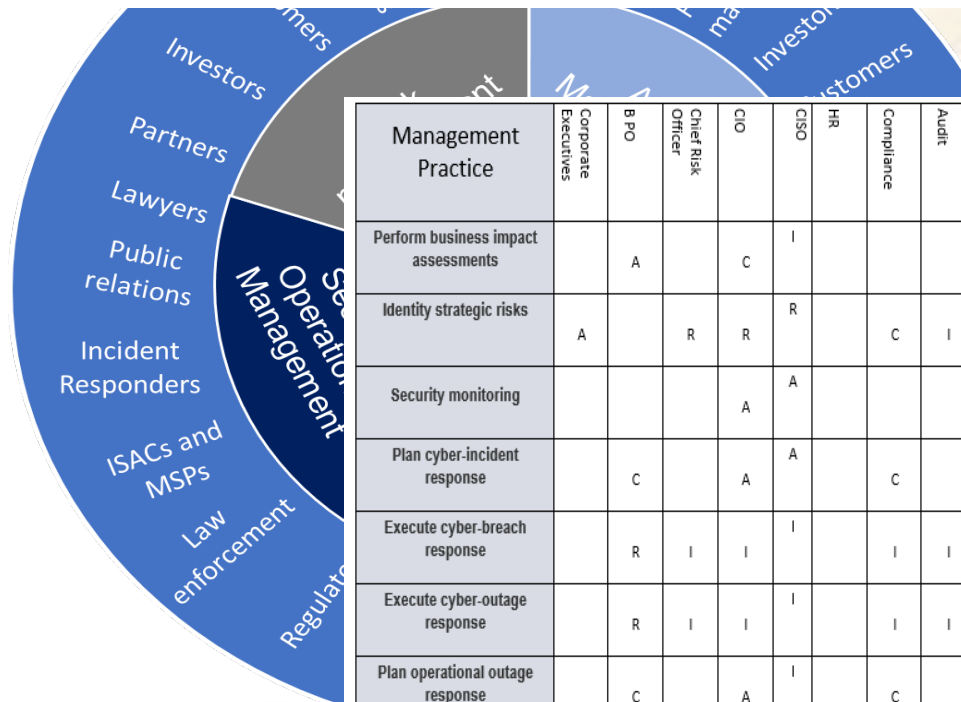
@ 2020-2022 Techvision Research

# Cybersecurity Roles in Many Departments



2-3

*Understand and get general agreement on which persons or departments fulfill security-related roles. Describe these roles and responsibilities in policy as a starting point for security governance.*



Management Practice	Corporate Executives	B PO	Chief Risk Officer	CIO	CISO	HR	Compliance	Audit	Chief Privacy Officer	CSIRT manager	Security Ops Manager	CTO / Dev	IT operations	Service Manager	Business continuity	FA / ARB
Perform business impact assessments		A		C	I					I		C	R		C	
Identify strategic risks	A		R	R	R		C	I	C	I	I	I	I	I	I	I
Security monitoring				A	A					C	R					
Plan cyber-incident response		C		A	A		C		C	R	R	C		R		C
Execute cyber-breach response		R	I	I	I		I	I		R	R		C			
Execute cyber-outage response		R	I	I	I		I	I		R	R		R	A	C	
Plan operational outage response		C		A	I		C			C	C	R	R	R	R	C
Execute operational outage response		R	I	I			I	I	C	I	I	R	R	A	R	

# Align Business Functions to Control Domains

## Excerpt

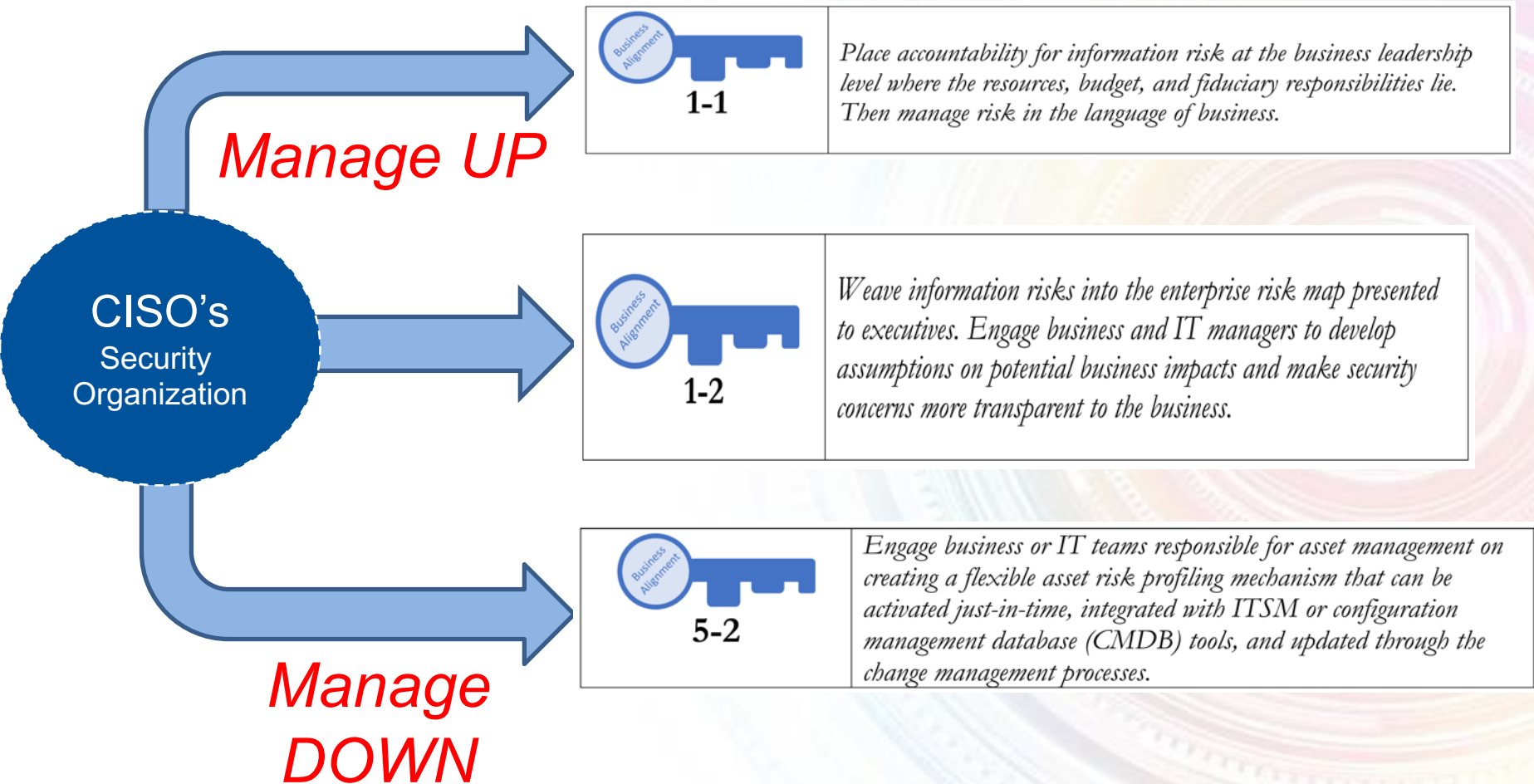
CHAPTER 6 ESTABLISH A CONTROL BASELINE

*Table 6-3. Master Table for Aligning Business Functions to Control Domains*


<b>Business Function</b>	<b>Control Domain Inter-Dependencies</b>
Internal marketing team	Security policy and awareness
IT asset management	Asset inventory
Legal team	Secure HR practices, logging and log review, user account monitoring, incident response, business continuity
Network management team	Security zoning
Procurement and/or vendor management	Third-party management, security zoning, access management and authorization, data protection, incident response, backup and data recovery
Public relations	Incident response
UAT team	Security policy and awareness





# Manage Risk In the Language of Business



# Keys to Business Alignment in the Multicloud Environment

 <p>7-4</p>	<p><i>Work with forward-thinking IT leaders seeking to establish IT as a broker in the cloud environment.</i></p>
--	---

 <p>7-5</p>	<p><i>Work with third party management to develop a portfolio process for managing the risk and utility of third parties.</i></p>
--	---

 <p>7-6</p>	<p><i>Empower developers to easily perform security-related tasks (DevSecOps) as part of their normal workflow and/ or cross-fertilize security staff or expertise into the development organization.</i></p>
---	---



# Agenda

What is a Security Reference Architecture?  
The Business View  
Functional Views  
A Business Alignment Framework  
***Next Steps***

# Next Steps: Fitting the Reference Architecture to Your Business and Security Program

## Plan

Develop Business Requirements. Work with stakeholders to:

- **Identify:** What capabilities from the Ref Arch to select and prioritize for security program and deployment plans?
- **Discover:** Which capabilities are in place, which are not?
- **Assess:** Maturity, or effectiveness, risk-appropriateness of existing solutions
- **Align:** Security-related Roles, RACIs, KPIs, and KRIs

## Do

Acquire, Build, or Implement

## Check

Validate Readiness with stakeholders, test capabilities

## Act

Deploy solutions

# Additional Recommendations

## Digital Transformation

- Align cybersecurity risk management and governance with business drivers and required business outcomes

## Multicloud Environments

- Mature third party management systems
- Implement distributed IAM, data discovery

## Expanding Risk Matrix

- Develop agile risk management processes
- Pursue zero trust, cybersecurity mesh architectures

## Cybersecurity Skills Shortage

- Position security as “coach” to business, IT staff
- Establish security championship programs

# Conclusion

- The Security Reference Architecture can help clients advance many initiatives, from a full Enterprise Security Architecture to individual security projects
- Use it as a yardstick to tell you “what good looks like” or to identify what components you need to work on
- TechVision Research will be drilling down into the Reference Architecture’s high-level capabilities in future documents
- TechVision Consulting can help clients apply the Reference Architecture through custom engagements