Zero Trust Is More Than Just Identity & Access...What's Missing

Deciphering Zero Trust

Mark Allers
VP of Business Development, Cimcor

CIMTRAK
INTEGRITY, TRUST & RESILIENCY

Zero Trust Is More Than Just Identity & Access...

What's Missing?

1. Zero Trust Emphasizes Layer 7
2. Integrity Is a Critical Component of a Zero Trust and a Resilient Infrastructure
3. There Is No Integrity In File Integrity Monitoring (FIM)
4. Integrity Is NOT a Product It’s a Process
5. Integrity Is One of the Two Leading Indicators of a Software Supply Chain Vulnerability

Zero Trust…Why The Focus and Importance Now?

2021 set a new record with 5.9 billion accounts affected by digital thieves

TechNewWorld 2021

212 days is the average mean time to identify (MTTI) a breach

Ponemon report 2021

CAGR of Security Spend is 9.5%

CAGR of Security Breaches/Incidents is 34%

75 days is the average mean time to contain (MTTC) a breach

Ponemon report 2021

Average total cost of a ransomware breach is $4.62m

IBM 2021

Remote work has increased the average cost of a data breach by $137,000

IBM 2021

Cybercrime to cost the world $10.5 trillion annually by 2025

Cybersecurity Ventures

Nearly 1 million new malware threats released every day

CNN Business

Over 77% of organizations do not have a cyber security incident response plan

Cybint 2021

Why Start From Scratch If You Can Steal Without Consequence?

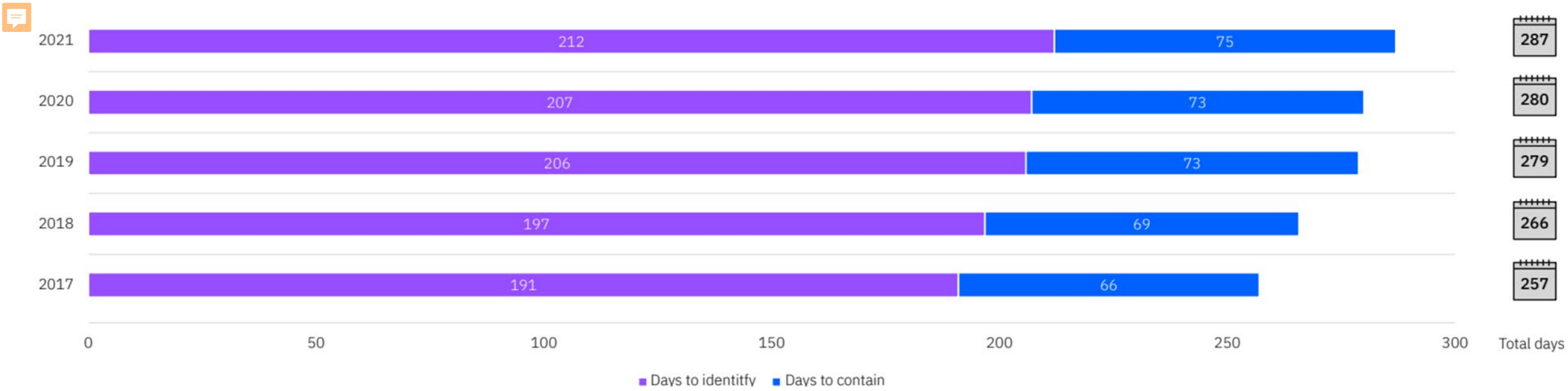
Chinese J-31

US F-35

CIMCOR

Mark's Viewpoints and Thoughts

- Zero Trust is simply the arrangement of existing controls to align and support a new architecture
- Security best practices need to become more prescriptive…a prioritized set of essential controls
- DevSecOps has a common thread to mitigate risk that is not being leveraged effectively
- Executives and boards rely upon analysts far too much
- Cyber Insurance is not in the business of helping solve or simplifying security…they are in the business of financial arbitrage between premiums and losses (evident by no due diligence requirements)
- Integrity controls reduce MTTI and MMTC
- SIEMs & SOARs need to digest integrity data to protect, detect, respond and recover (M-21-31)



Mean Time To Identify (MTTI) Meant Time To Contain (MTTC)

¾ of a Year to Identify and Contain a Breach

CIMCOR

Presidential Call To Arms

In May 2021, President Biden issued Executive Order (EO) 14028 on Improving the Nation's Cybersecurity in response to a spate of high-profile attacks targeting major technology vendors and U.S. Federal agencies. The Order focused on expanding several cybersecurity capabilities for government agencies—most notably, mandating a shift towards Zero Trust principles.

EO 14028 describes Zero Trust like this:

"The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment."

Positioning

"[...] an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented."

— Forrester, The Definition of Modern Zero Trust

"[...] an approach where implicit trust is removed from all computing infrastructure. Instead, trust levels are explicitly and continuously calculated and adapted to allow just-in-time, just-enough access to enterprise resources."

— Gartner, New to Zero Trust? Start Here

"[…] Zero Trust promotes a micro-perimeter approach based on user access, data location, and an application hosting model."

— PwC

"[..] key element of the zero trust approach is micro segmenting networks, data, applications, workloads, and other resources into individual, manageable units to contain breaches and wrap security controls at the lowest level possible."

— Deloitte

CIMCOR

Current Thinking vs Zero Trust Principals

Current Thinking

- After a single authentication, users, devices, services, and workloads are trusted to be legitimate and are granted access to a broad range of resources.
- The ubiquitous use of denylists in security tools inherently trusts that all activity is legitimate unless known to be malicious

Zero Trust (800-207)

1. Assume Breach - Organizations should assume at all times that there is a malicious presence inside their environment and implement security controls to minimize the impact.
2. Verify, Don’t Trust - Instead of assuming legitimacy, organizations should continuously verify all components within their IT infrastructure to ensure they haven’t been compromised.
3. Least Privilege - Once verified, users, devices, and services should be granted the minimum possible access required to complete their function—and for the shortest possible period. This minimizes the potential impact of malicious activity

The 7 Tenets of NIST 800-207

NIST 800-207 (the 7 Tenets)

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture (M-21-31)

Breaking Down ZT…

It's Not Just About Identity and Access!

Zero Trust Components

	Device/ Workload	Identity	Access	Transaction
User(s)	Identify & Verify User Integrity	User Authentication	Enforce Least Privileges To Data & Application (Authorization)	Manage Transaction/Content Security on a Per-Session Basis
Application(s)	Identify & Verify Workload Integrity	DevOps Authentication	Enforce Least Privileges Access To Workloads (Authorization)	Manage Transaction/Content Security on a Per-Session Basis
Infrastructure	Identify & Verify Device Integrity	Admin Authentication	Enforce Least Privileges Access To Infrastructure (Authorization)	Manage Transaction/Content Security on a Per-Session Basis
800-207 Tenants	#1, #5 #7	#1 #3	#4 #6 #7	#2

"The enterprise monitors and measures the integrity and security posture of all owned and associated assets" – Tenet #5

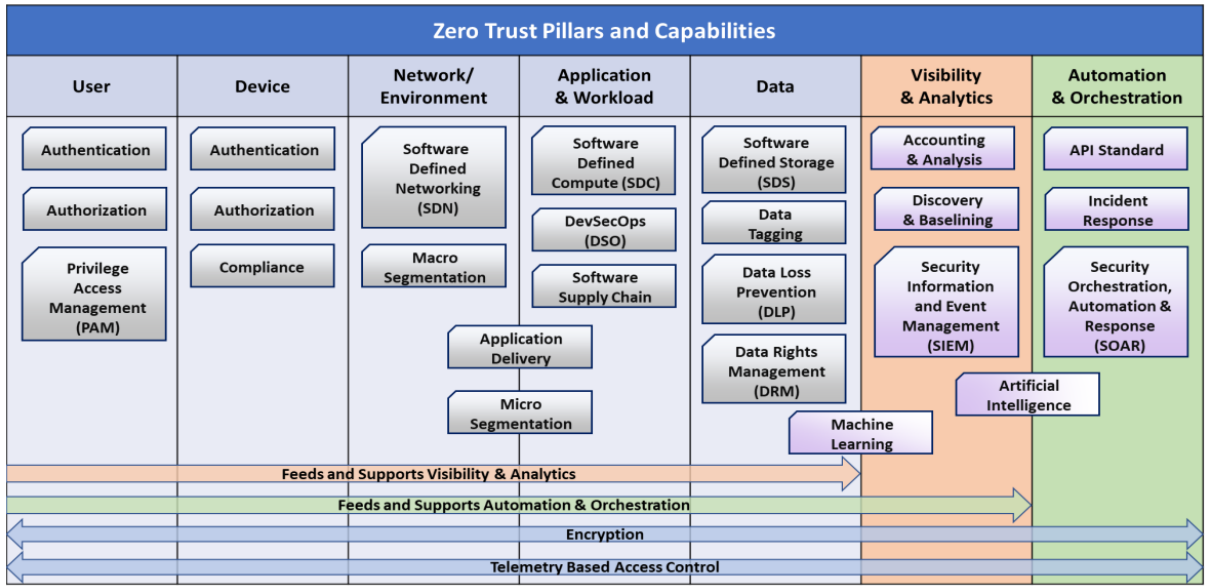
CIMCOR

DoD ZT Reference Architecture…

"Real-time attestation…of devices in an enterprise are critical functions."

"Applications and workloads include tasks on systems or services on-premises, as well as applications or services running in a cloud environment. Zero Trust workloads span the complete application stack from application layer to hypervisor. Securing and properly managing the application layer as well as compute containers and virtual machines is central to Zero Trust adoption."
"Vital, contextual details provide greater understanding of performance, behavior and activity baseline across other Zero Trust pillars. This visibility improves detection of anomalous behavior and provides the ability to make dynamic changes to security policy and real-time access decisions."

"Automated security response requires defined processes and consistent security policy enforcement across all environments in a Zero Trust enterprise to provide proactive command and control."

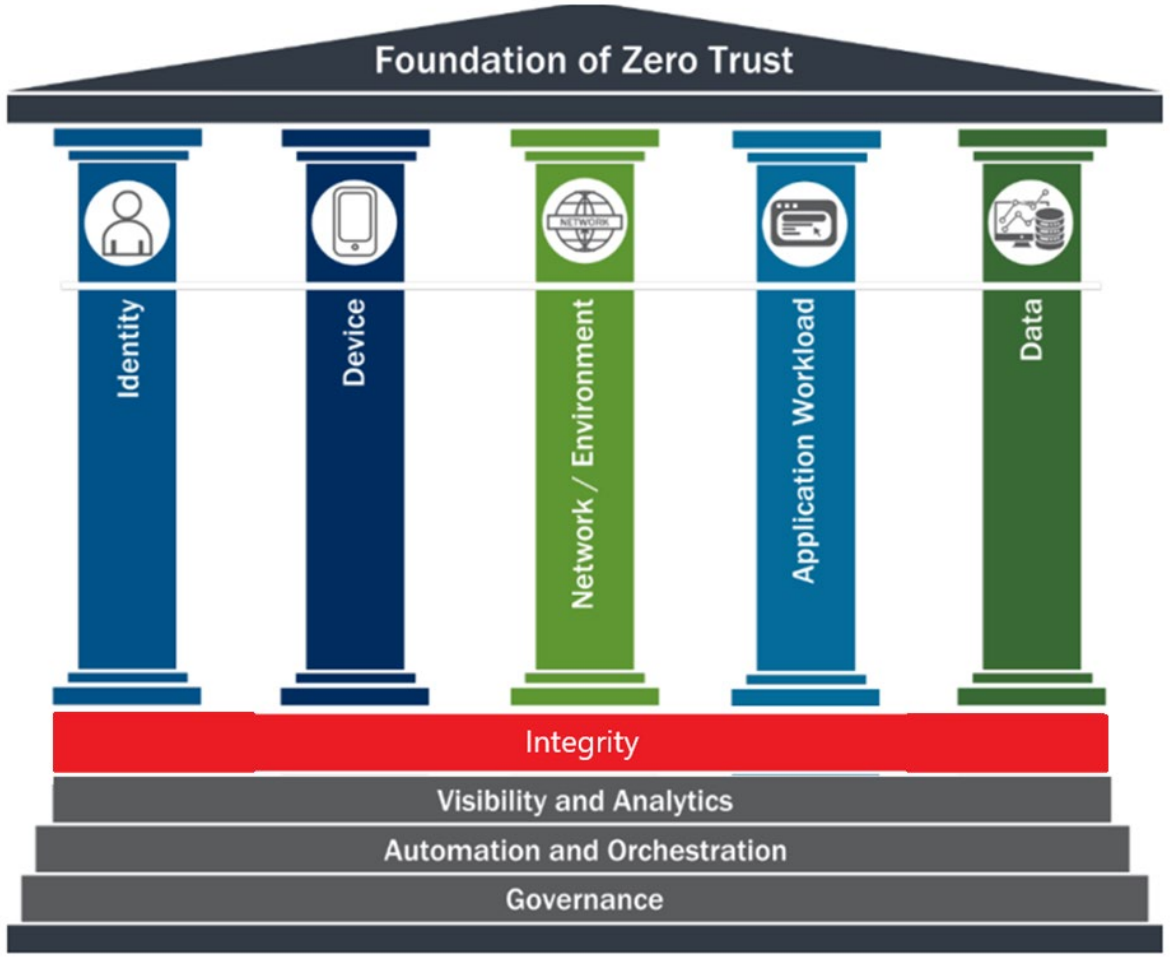


CIMCOR

CISA Zero Trust Maturity Model…

"The Zero Trust Maturity Model entails not just validating the identity of users, but also ensuring the **integrity** of the devices they use to access services and data. Agencies need to manage the security of these devices, ensuring a baseline of device security protections and visibility into the devices themselves."

"This endpoint focus allows for device compliance and **integrity** to be included as part of the access control decisions for services and data."



CIMCOR

What Is The Definition of Integrity?

SANS CIA Triad

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle.

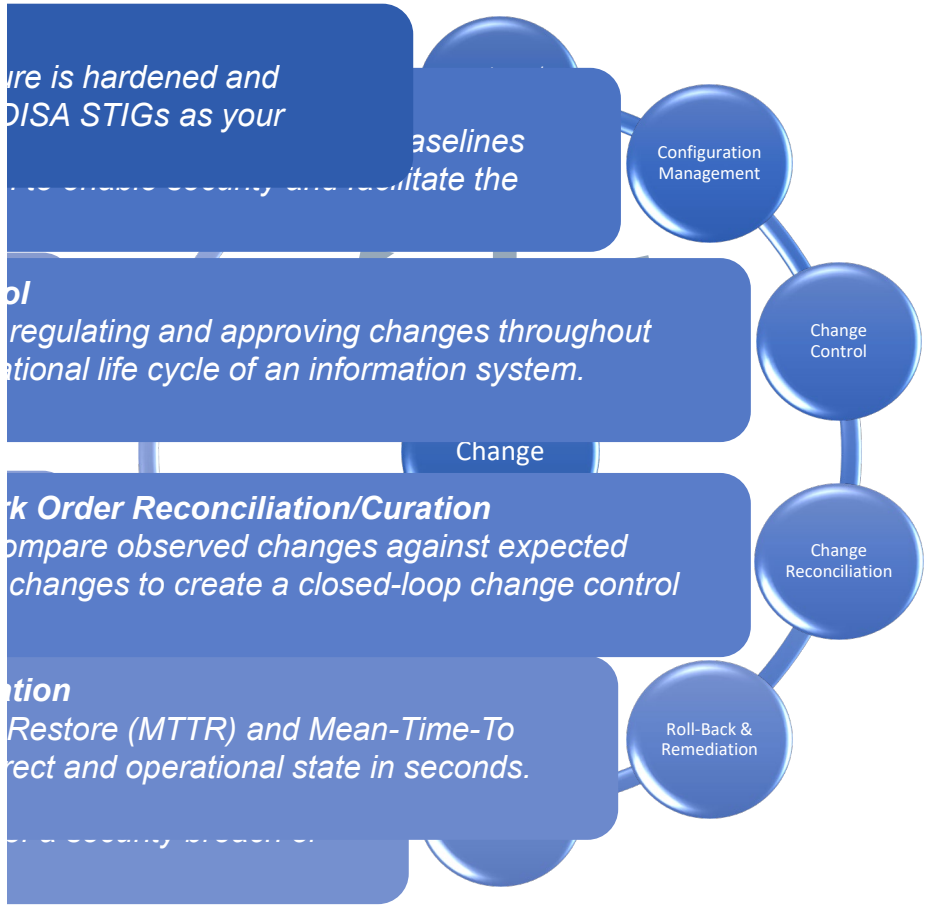
Integrity Is More Than Simply Detecting Change In The Case of FIM!

Integrity is the confidence and certainty that the appropriate controls and compliance requirements are in place to ensure the accuracy and consistency of data throughout its entire life-cycle of operation.

DEFINING INTEGRITY

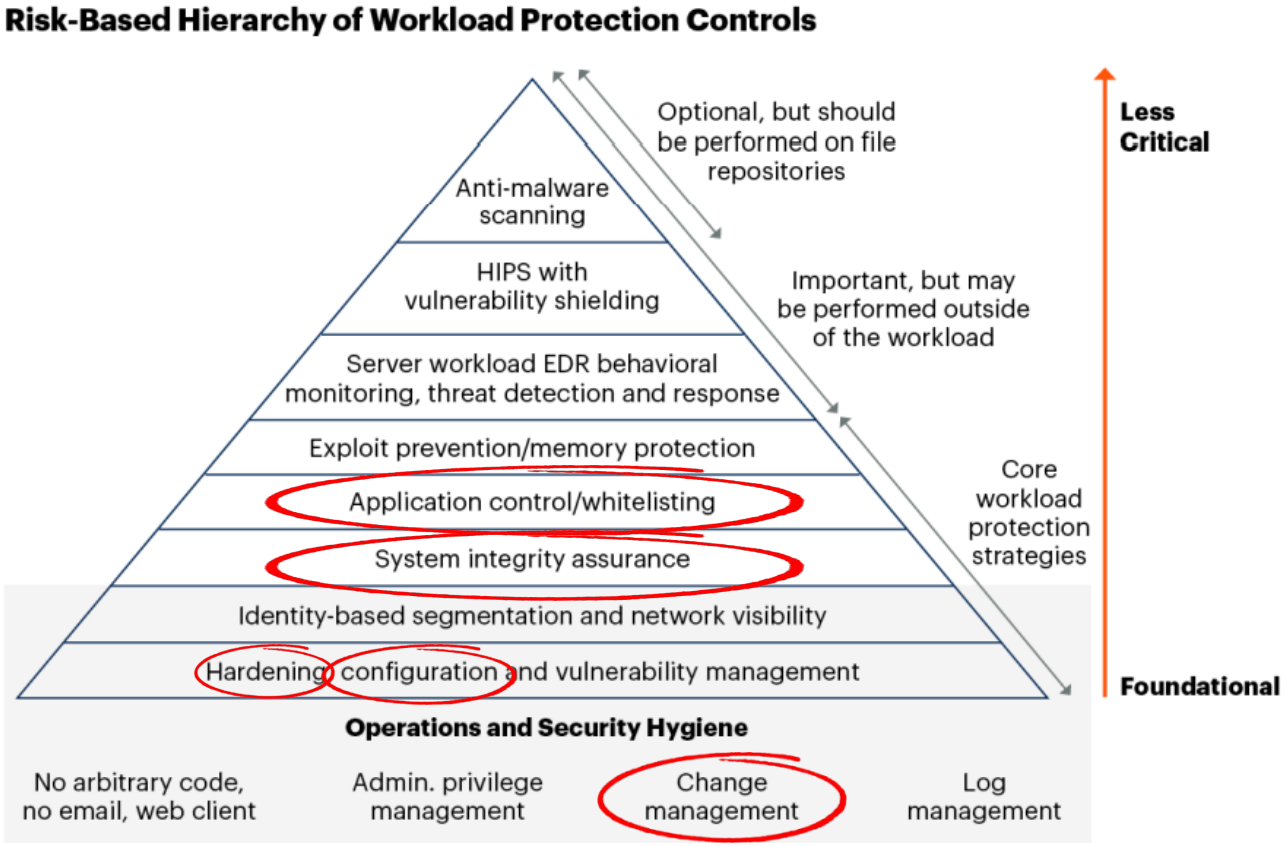
9 Controls & 1 Workflow Enables Device/Workload Integrity

egrity oring	System Integrity Assurance
	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓



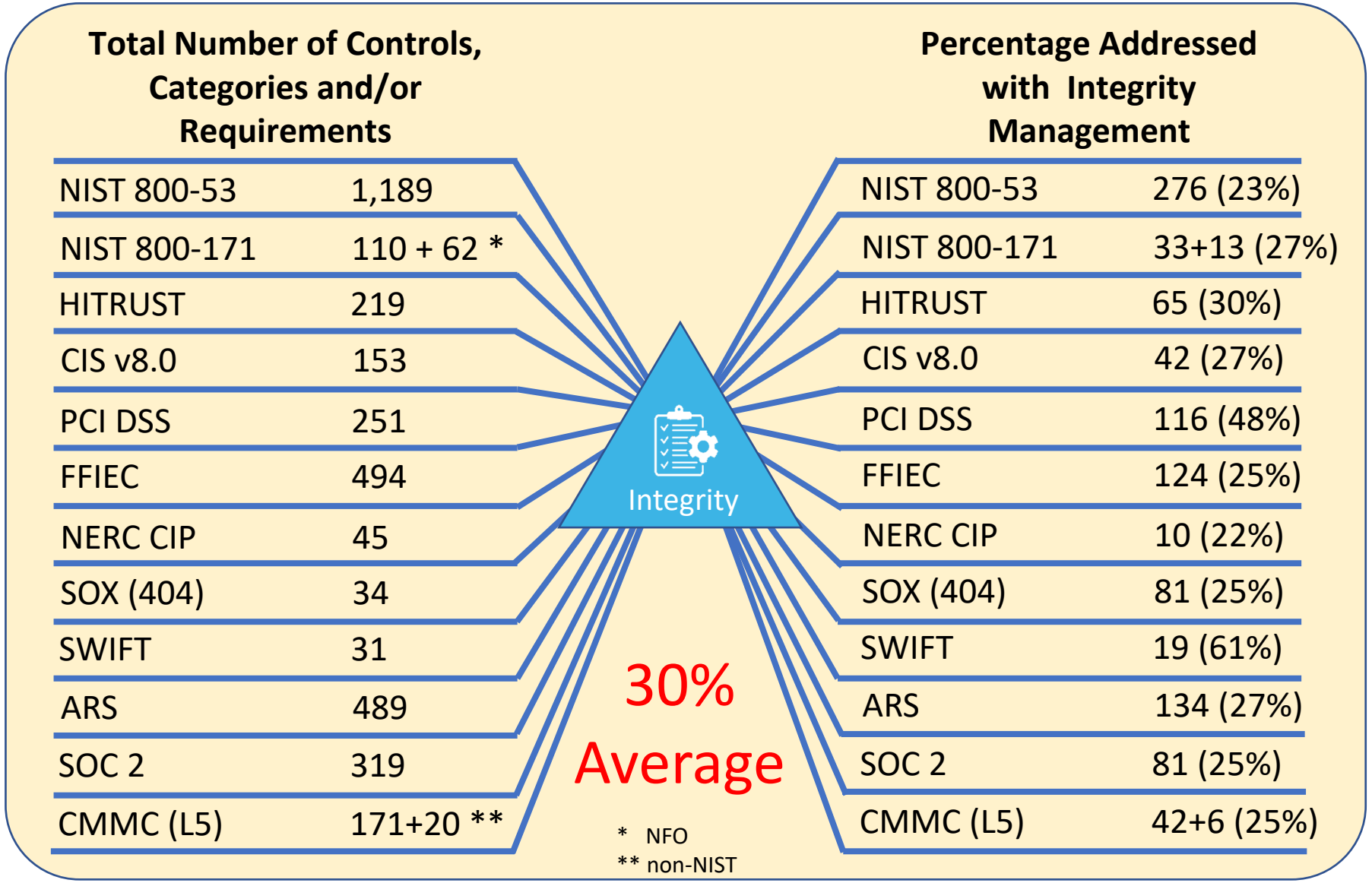
CIMCOR

Gartner's CWPP/WPP



CIMCOR

Evidence of Integrity - Compliance & Best Practices Crosswalks



CIMCOR

Evidence of Integrity Controls in PCI DSS

PCI DSS Requirements v3.2

Requirement 1 — Install and maintain a firewall configuration to protect cardholder data

#	Integrity
1.1	✓
1.1.1	✓
1.1.2	
1.1.3	
1.1.4	
1.1.5	✓
1.1.6	✓
1.1.7	✓
1.2.1	
1.2.2	✓
1.2.3	✓
1.3	
1.3.1	✓
1.3.2	
1.3.3	
1.3.4	
1.3.5	
1.3.6	
1.3.7	
1.4	✓
1.5	✓

Requirement 2 — Do not use vendor-supplied defaults for system passwords and other security parameters

#	Integrity
2.1	
2.1.1	
2.2	✓
2.2.1	
2.2.2	✓
2.2.3	
2.2.4	✓
2.2.5	✓
2.3	✓
2.4	✓
2.5	✓
2.6	

Requirement 3 — Protect stored cardholder data

#	Integrity
3.1	
3.2	
3.2.1	
3.2.2	
3.2.3	
3.3	
3.4	
3.4.1	
3.5.1	
3.5.2	
3.5.3	
3.5.4	
3.6.1	✓
3.6.2	✓
3.6.3	✓
3.6.4	
3.6.5	
3.6.6	
3.6.7	
3.6.8	
3.7	✓

Requirement 4 — Encrypt transmission of cardholder data across open, public networks

#	Integrity
4.1	
4.1.1	
4.2	
4.3	

Requirement 5 — Use and regularly update anti-virus software or programs

#	Integrity
5.1	
5.1.1	✓
5.1.2	✓
5.2	
5.3	✓
5.4	✓

Requirement 6 — Develop and maintain secure systems and applications

#	Integrity
6.1	✓
6.2	
6.3	✓
6.3.1	
6.3.2	
6.4	✓
6.4.1	✓
6.4.2	
6.4.3	
6.4.4	
6.4.5	
6.4.5.1	
6.4.5.2	✓
6.4.5.3	
6.4.5.4	✓
6.4.6	✓
6.5	
6.5.1	
6.5.2	
6.5.3	
6.5.4	
6.5.5	
6.5.6	
6.5.7	
6.5.8	
6.5.9	
6.5.10	
6.6.	✓
6.7	✓

Requirement 7 — Restrict access to cardholder data by business need to know

#	Integrity
7.1.1	✓
7.1.2	✓
7.1.3	✓
7.1.4	✓
7.2.1	✓
7.2.2	✓
7.2.3	✓
7.3	✓

Requirement 8 — Assign a unique ID to each person with computer access

#	Integrity
8.1.1	✓
8.1.2	✓
8.1.3	
8.1.4	
8.1.5	
8.1.6	
8.1.7	
8.1.8	
8.2	✓
8.2.1	✓
8.2.2	✓
8.2.3	✓
8.2.4	✓
8.2.5	✓
8.2.6	✓
8.3.1	
8.3.2	
8.4	
8.5	
8.5.1	
8.6	
8.7	✓
8.8	✓

Requirement 9 — Restrict physical access to cardholder data

#	Integrity
9.1	
9.1.1	
9.1.2	
9.1.3	
9.20	
9.3	
9.4.1	
9.4.2	
9.4.3	
9.4.4	
9.5	
9.5.1	
9.6.1	
9.6.2	
9.6.3	
9.7.1	
9.8.1	
9.8.2	
9.9.1	
9.9.2	
9.9.3	
9.10	

Requirement 10 — Track and monitor all access to network resources and cardholder data

#	Integrity
10.1	✓
10.2.1	✓
10.2.2	✓
10.2.3	✓
10.2.4	
10.2.5	✓
10.2.6	
10.2.7	✓
10.3.1	✓
10.3.2	✓
10.3.3	✓
10.3.4	✓
10.3.5	✓
10.3.6	✓
10.4	✓
10.4.1	✓
10.4.2	✓
10.4.3	✓
10.5.1	✓
10.5.2	✓
10.5.3	✓
10.5.4	✓
10.5.5	✓
10.6	✓
10.6.2	
10.6.3	✓
10.7	✓
10.8	✓
10.8.1	✓
10.9	✓

Requirement 11 — Regularly test security systems and processes

#	Integrity
11.1	
11.1.1	
11.1.2	
11.2	✓
11.2.1	✓
11.2.2	
11.2.3	✓
11.3	
11.3.1	
11.3.2	
11.3.3	
11.3.4	
11.3.4.1	
11.4	✓
11.5	✓
11.5.1	✓
11.6	✓

Requirement 12 — Maintain a policy that addresses information security for all personnel

#	Integrity
12.1	
12.1.1	
12.2	✓
12.3	✓
12.3.1	✓
12.3.2	✓
12.3.3	✓
12.3.4	✓
12.3.5	
12.3.6	
12.3.7	
12.3.8	
12.3.9	
12.3.10	✓
12.4	✓
12.4.1	✓
12.5	✓
12.5.1	✓
12.5.2	✓
12.5.3	✓
12.5.4	✓
12.5.5	✓
12.6	
12.6.1	
12.6.2	
12.7	
12.8	✓
12.8.1	
12.8.2	
12.8.3	
12.8.4	✓
12.8.5	
12.9	
12.10.1	✓
12.10.2	✓
12.10.3	✓
12.10.4	✓
12.10.5	✓
12.10.6	✓
12.11	✓
12.11.1	

Appendix A1 — Additional PCI DSS Requirements for Shared Hosting Providers

#	Integrity
A1	✓
A1.1	✓
A1.2	✓
A1.3	✓
A1.4	✓

Appendix A2 — Additional PCI DSS Requirements for Entities using SSL/early TLS

#	Integrity
A2.1	
A2.2	
A3.3	

CIMCOR

Evidence of Integrity Controls in 800-53

NIST 800-53 rev5 Crosswalk To Integrity

Access Control (AC)		Awareness & Training (AT)		Audit & Accountability (AU)		Assessment, Authorization & Monitoring (CA)		Configuration Management (CM)		Contingency Planning (CP)		Identification & Authentication (IA)		Incident Response (IR)		Maintenance (MA)		Media Protection (MP)		Physical & Environmental Protection (PE)		Planning (PL)		Program Management (PM)		Personnel Security (PS)		Personally Identifiable Information Processing & Transparency (PT)		System & Services Acquisition (SA)		Risk Assessment (RA)		System & Communication Protection (SC)		System & Information Integrity (SI)		Supply Chain Risk Management (SR)	
#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#		#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity	#	Integrity
AC-1		AT-1		AU-1		CA-1		CM-1		CP-1		IA-1		IR-1		MA-1		MP-1		PE-1		PL-1		PM-1		PS-1		PT-1		SA-1		RA-1		SC-1		SI-1		SR-1	
AC-2	✓	AT-2		AU-2	✓	CA-2		CM-2	✓	CP-2		IA-2		IR-2		MA-2	✓	MP-2	✓	PE-2		PL-2		PM-2		PS-2		PT-2		SA-2		RA-2		SC-2	✓	SI-2	✓	SR-2	
AC-3	✓	AT-3		AU-3	✓	CA-3		CM-3	✓	CP-3		IA-3		IR-3		MA-3	✓	MP-3		PE-3		PL-3		PM-3		PS-3		PT-3		SA-3	✓	RA-3	✓	SC-3	✓	SI-3	✓	SR-3	✓
AC-4		AT-4		AU-4		CA-4		CM-4	✓	CP-4		IA-4		IR-4	✓	MA-4		MP-4		PE-4		PL-4		PM-4		PS-4		PT-4		SA-4	✓	RA-4		SC-4		SI-4	✓	SR-4	✓
AC-5	✓	AT-5		AU-5		CA-5		CM-5	✓	CP-5		IA-5		IR-5	✓	MA-5		MP-5		PE-5		PL-5		PM-5		PS-5		PT-5		SA-5	✓	RA-5	✓	SC-5		SI-5	✓	SR-5	✓
AC-6	✓	AT-6		AU-6	✓	CA-6		CM-6	✓	CP-6		IA-6		IR-6	✓	MA-6		MP-6		PE-6		PL-6		PM-6		PS-6		PT-6		SA-6		RA-6		SC-6		SI-6		SR-6	
AC-7				AU-7	✓	CA-7	✓	CM-7	✓	CP-7		IA-7		IR-7	✓	MA-7		MP-7		PE-7		PL-7		PM-7		PS-7		PT-7		SA-7		RA-7	✓	SC-7	✓	SI-7	✓	SR-7	
AC-8	✓			AU-8	✓	CA-8		CM-8	✓	CP-8		IA-8		IR-8				MP-8		PE-8		PL-8		PM-8		PS-8		PT-8		SA-8	✓	RA-8		SC-8	✓	SI-8		SR-8	
AC-9				AU-9		CA-9		CM-9		CP-9	✓	IA-9		IR-9						PE-9		PL-9		PM-9		PS-9				SA-9	✓	RA-9		SC-9		SI-9		SR-9	✓
AC-10				AU-10				CM-10		CP-10	✓	IA-10								PE-10		PL-10		PM-10						SA-10	✓	RA-10		SC-10		SI-10		SR-10	✓
AC-11				AU-11				CM-11	✓	CP-11		IA-11								PE-11		PL-11		PM-11						SA-11	✓			SC-11		SI-11	✓	SR-11	✓
AC-12				AU-12				CM-12	✓	CP-12		IA-12								PE-12				PM-12						SA-12				SC-12	✓	SI-12	✓	SR-12	
AC-13				AU-13				CM-13		CP-13										PE-13				PM-13						SA-13				SC-13	✓	SI-13			
AC-14				AU-14				CM-14												PE-14				PM-14						SA-14				SC-14		SI-14	✓		
AC-15				AU-15																PE-15				PM-15						SA-15	✓			SC-15		SI-15	✓		
AC-16	✓			AU-16																PE-16				PM-16						SA-16				SC-16	✓	SI-16			
AC-17																				PE-17				PM-17						SA-17				SC-17		SI-17			
AC-18																				PE-18				PM-18						SA-18				SC-18		SI-18			
AC-19																				PE-19				PM-19						SA-19				SC-19		SI-19			
AC-20																				PE-20				PM-20						SA-20				SC-20		SI-20			
AC-21	✓																			PE-21				PM-21						SA-21				SC-21		SI-21	✓		
AC-22																				PE-22				PM-22						SA-22				SC-22		SI-22			
AC-23																				PE-23				PM-23						SA-23				SC-23		SI-23			
AC-24																								PM-24										SC-24	✓				
AC-25	✓																							PM-25										SC-25					
																								PM-26										SC-26	✓				
																								PM-27										SC-27					
																								PM-28										SC-28	✓				
																								PM-29										SC-29					
																								PM-30										SC-30					
																								PM-31										SC-31					
																								PM-32										SC-32					
																																		SC-33					
																																		SC-34	✓				
																																		SC-35					
																																		SC-36	✓				
																																		SC-37					
																																		SC-38					
																																		SC-39					
																																		SC-40					
																																		SC-41					
																																		SC-42	✓				
																																		SC-43					
																																		SC-44					
																																		SC-45					
																																		SC-46					
																																		SC-47					
																																		SC-48					
																																		SC-49					
																																		SC-50					
																																		SC-51					

✓ Integrity Enables

CIMCOR

All frameworks are very ***descriptive***

Whereas a best practices framework like CIS is ***prescriptive*** and aligns with Zero Trust…tells you what to do and in what order

20 of the 56 (36%) of IG1 controls are Integrity controls

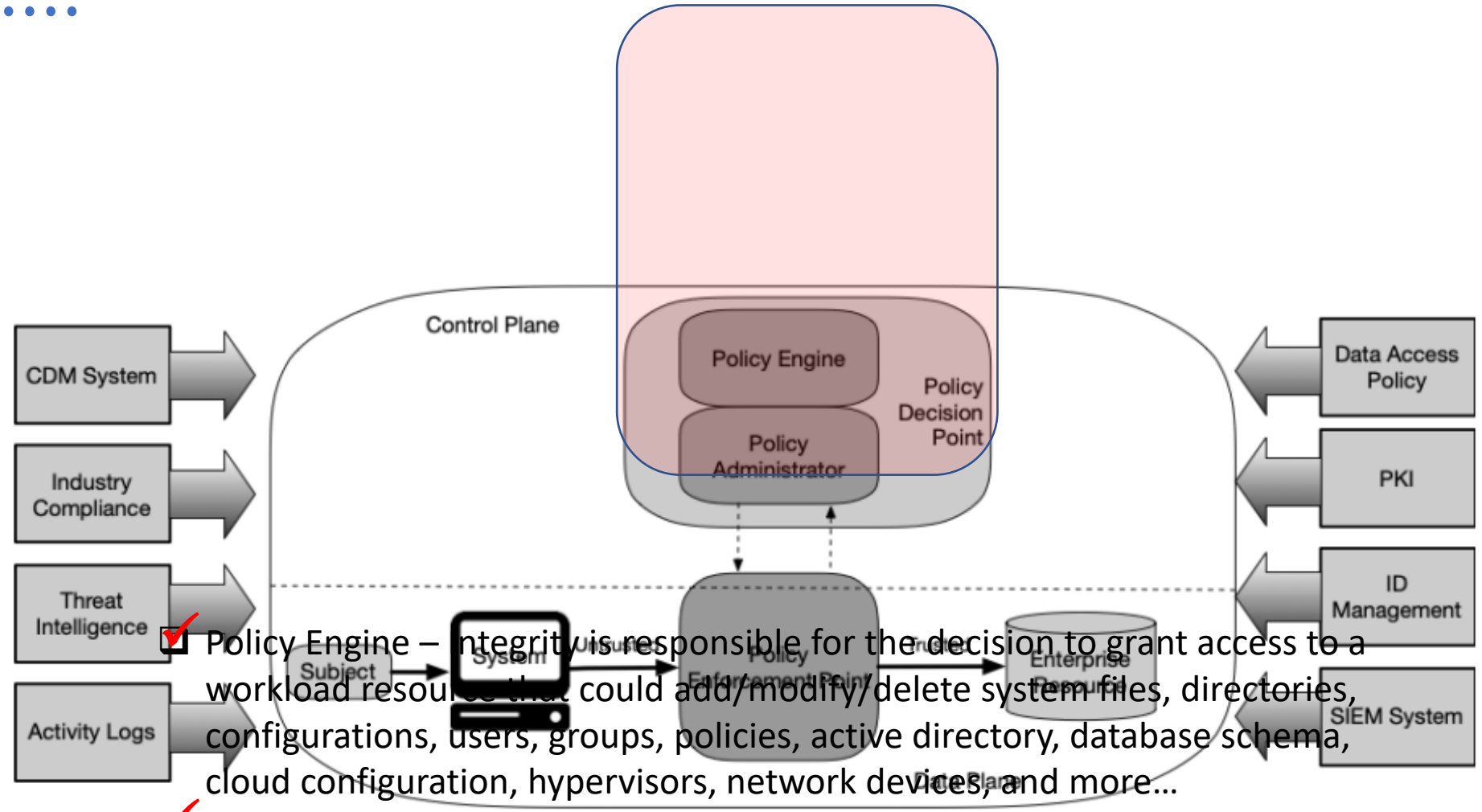
11 of the 56 (20%) are Access & Identity controls

CIMCOR

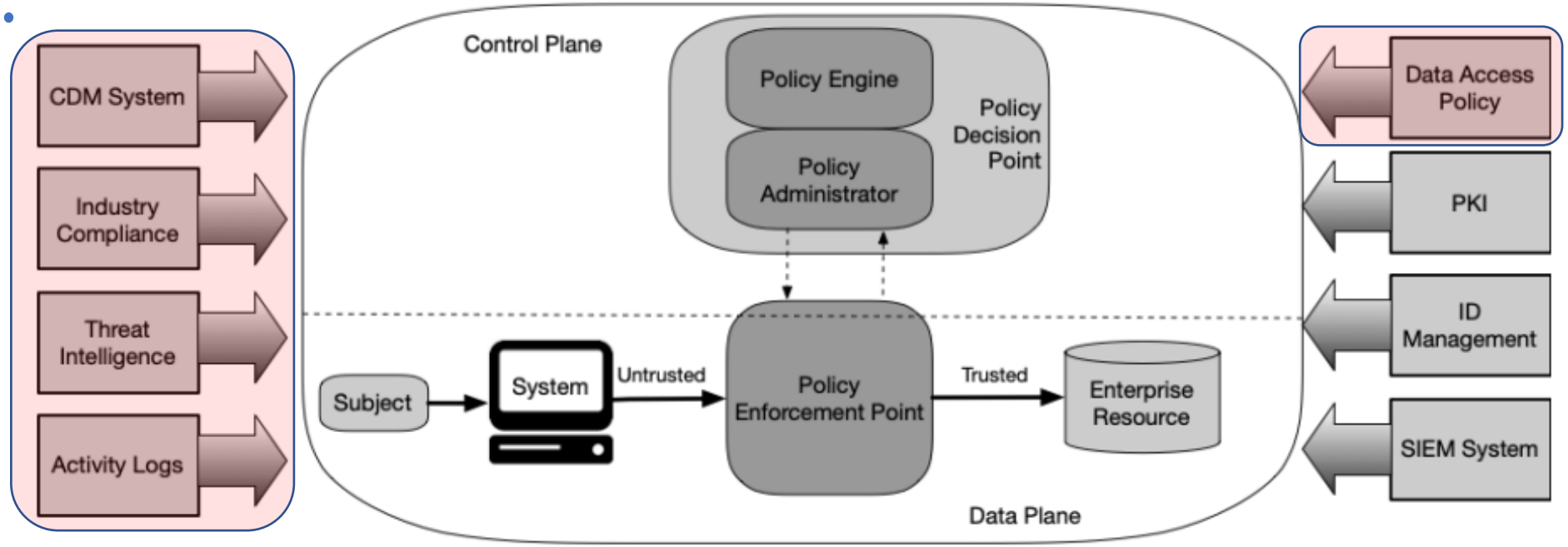
So How Does Zero Trust Align w/ CIS Controls…

Zero Trust Components				
	Device/ Workload	Identity	Access	Transaction
User(s)	Identify & Verify User Integrity	User Authentication	Enforce Least Privileges To Data & Application (Authorization)	Manage Transaction/Content Security on a Per-Session Basis
Application(s)	Identify & Verify Workload Integrity	DevOps Authentication	Enforce Least Privileges Access To Workloads (Authorization)	Manage Transaction/Content Security on a Per-Session Basis
			Enforce Least	Manage

CIMCOR

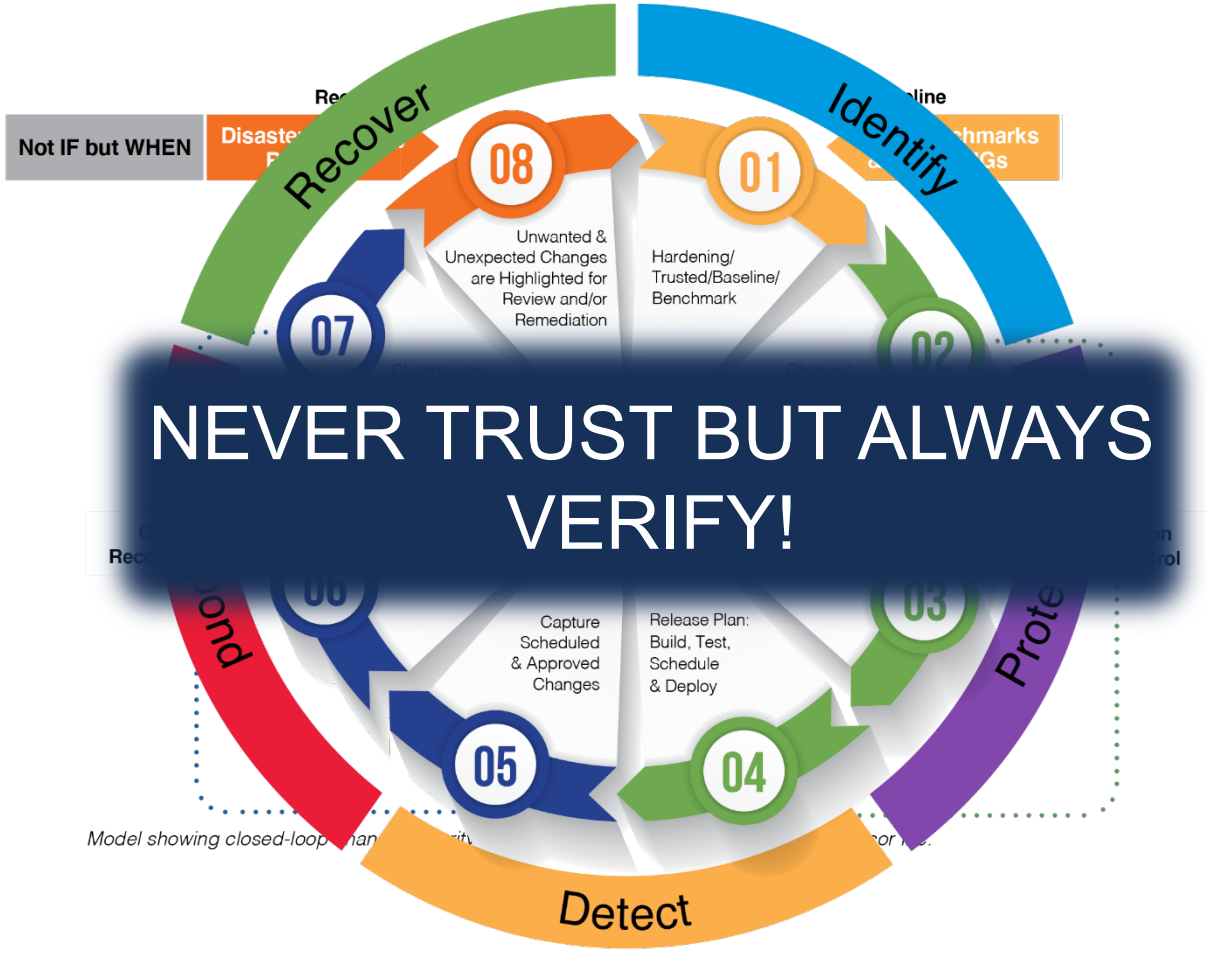


- ☑ Policy Engine – Integrity is responsible for the decision to grant access to a workload resource that could add/modify/delete system files, directories, configurations, users, groups, policies, active directory, database schema, cloud configuration, hypervisors, network devices, and more…
- ☑ Policy Administrator – Integrity provides a workflow and process for change control, change prevention, and roll-back capability to ensure system integrity assurance.
- ☑ Policy Enforcement Point – Ultimately responsible for enabling and monitoring in real-time the integrity of an enterprise resource.



- ☑ CDM System – There is an integrity management platform that has received Continuous Diagnostics & Mitigation (CDM) approval.
- ☑ Industry Compliance – Integrity platforms should provide the necessary evidence for 800-53, PCI, CMMC, HITRUST, SWIFT, and dozens of other compliance mandates.
- ☑ Threat Intelligence – Integrity platforms should digest STIX & TAXII feeds to analyze and evaluate real-time security decisions and vulnerability risks.
- ☑ Activity Logs – Integrity platforms should provide in real-time a comprehensive view of all change activities and processes with an ability to restore unwanted or unexpected changes back to a known and trusted state of operation.
- ☑ Data Access Policy – Integrity platforms should provide granular detail of who made changes and what process/approval was linked to that authorized change.

Integrity Is Not a Product… It's a Process… Feedback Loop

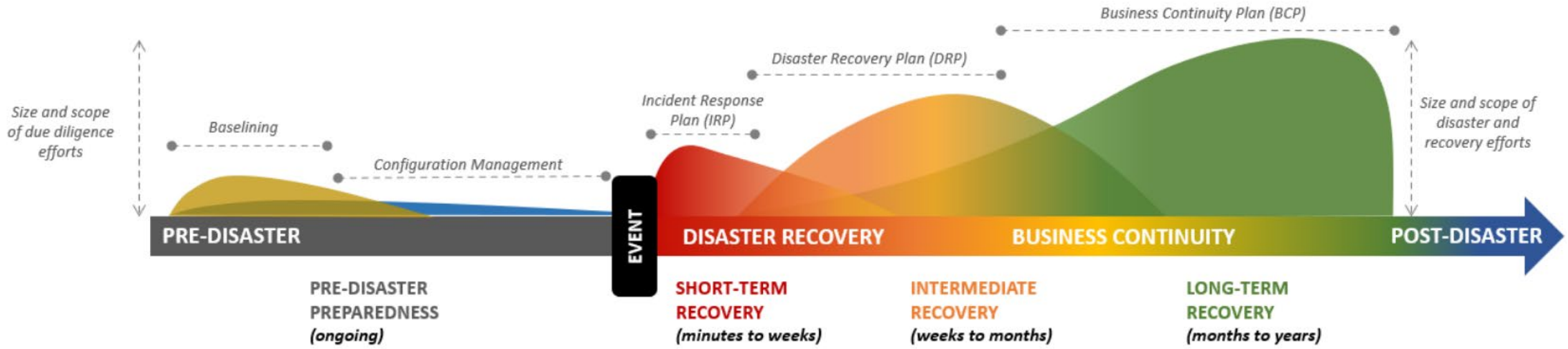


91% of all security breaches can be auto-detected with the proper deployment of three controls…configuration management, change management, and release management *

* IT Process Institute

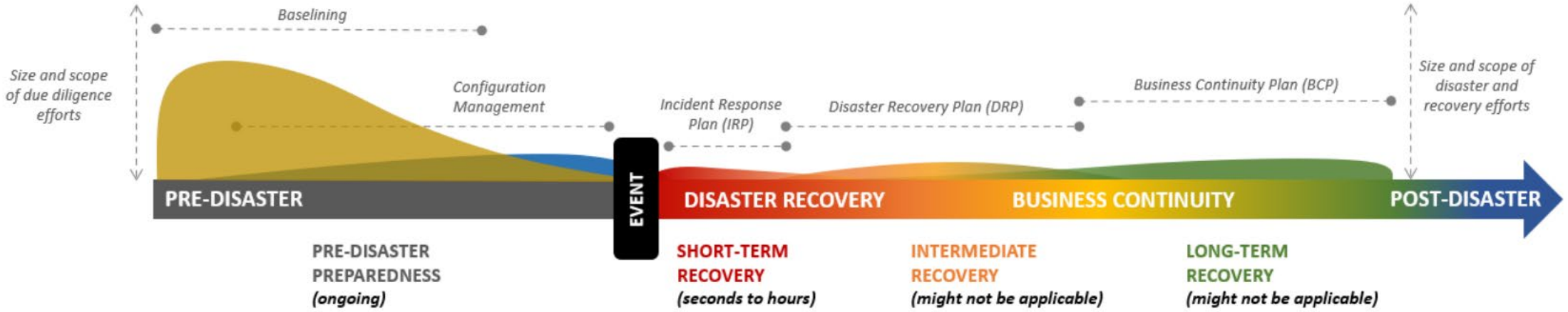
CIMCOR

REACTIVE-FOCUSED SECURITY OPERATIONS



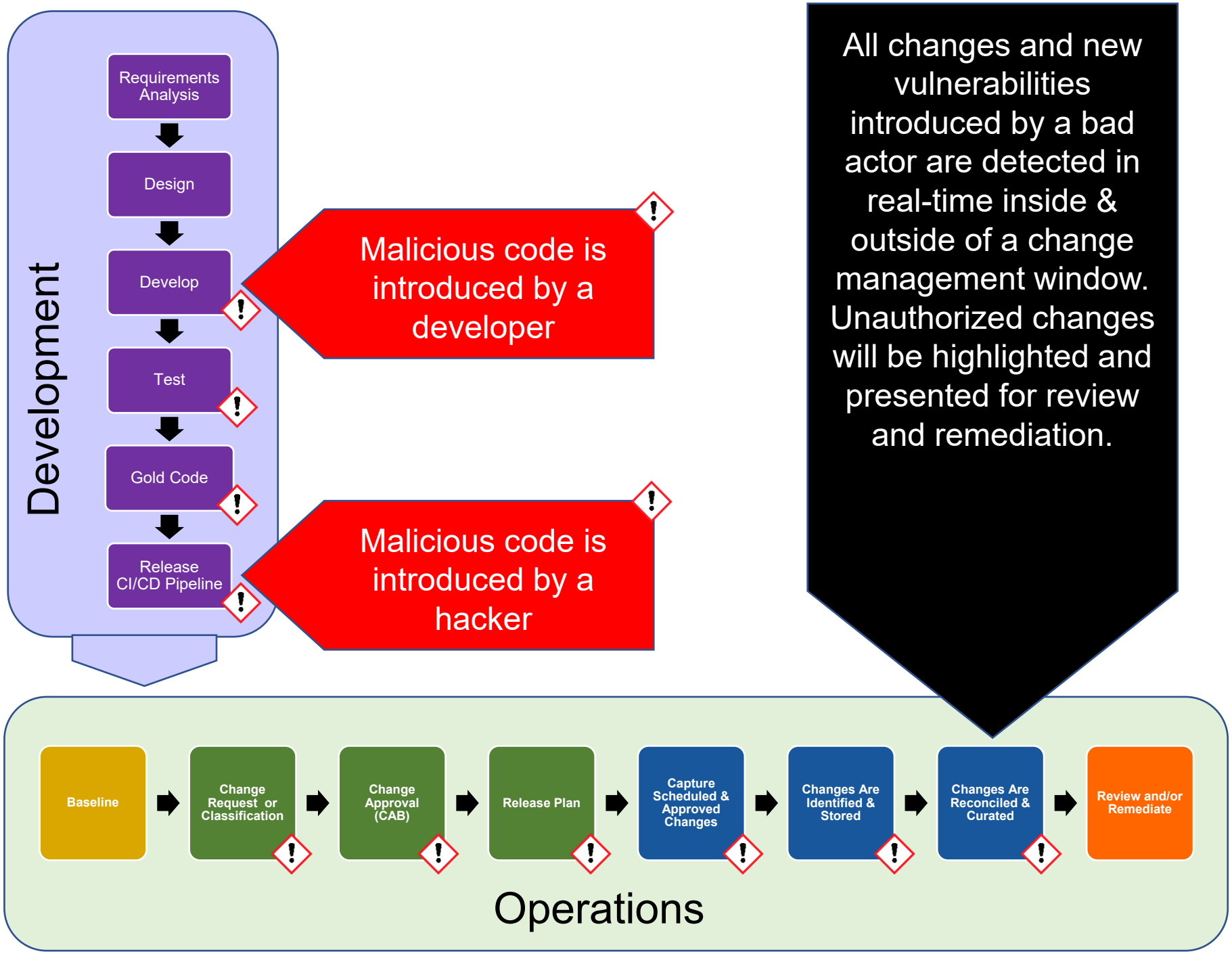
- Effort is on the “right side” of an incident or event – it is reactive. Baselining and configuration management on the “left side” of an incident or event is often compliance-focused and are not directly tied to response/recovery operations.
- The traditional, reactive model has minimal focus on baselining and configuration management.
- When an incident occurs, there are structured plans to respond that span from minutes to years in duration:
  - Incident Response Plan (IRP)
  - Disaster Recovery Plan (DRP)
  - Business Continuity Plan (BCP)
- Expense is primarily associated with event detection, response, remediation and recovery operations.

RESILIENT-FOCUSED SECURITY OPERATIONS



- Effort is on the “left side” of an incident or event - prevention-focused. An increased effort on the “left side”, will result in a decreased operational impact on the “right side” of the event occurrence.
- There is significant effort placed on baselining and automating configuration and change management operations.
- When an incident occurs, the automated remediation actions minimize impact and the necessity to activate IRPs, DRPs and BCPs.
- Expense is primarily associated with tightly-controlled configuration and change management practices.

How Does Integrity Positively Impact Dev & Supply Chain



CIMCOR

What Does Integrity Helps Solve

- It is the evidence to verify that your workload is running in an expected state
- Cornerstone for a resilient infrastructure
- Minimizes cost and risk that impact IRP, DRP, and BCP
- Leading indicator to identify a security breach/incident
- Leading indicator you have a software vulnerability
- Leading indicator you have drifted from a state of being compliant
- Addresses Ransomware for ZTA - you can still encrypt the encrypted!
- Critical to achieving a Zero Trust framework

M-22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

2. Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.

4. Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

5. Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

M-22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Devices

- Vision - Agencies maintain a complete inventory of every device authorized and operated for official business and can prevent, detect, and respond to incidents on those devices.

Actions (2)

- ✓ Inventorying Assets (#1)
- ✓ Government-wide endpoint detection and response (#2)
- ❑ Recovery

Applications and Workloads

- Vison - Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

Actions (6)

- ✓ Immutable workloads (#6)
- ❑ Recovery

Immutable workloads and applications refers to deployed servers or VMs that are never modified after deployment without proper authority and attestation for change.

Data

- Vison - Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing.

Actions (4)

- ✓ Automating security responses (#2)
- ✓ Auditing access to sensitive data in the cloud (#3)
- ✓ Timely access to logs (#4)
- ❑ Recovery

CIMCOR

M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Integrity Controls Are What Give SIEMs/SOARs Their Most Critical Data

- Data that gets loaded to the SIEM is what gives it value. There are a lot of bad data sources, and most data cannot easily be classified binary as good or bad.
  - Integrity alerts are BINARY and provides clear context of unwanted, unexpected and unauthorized activity throughout your enterprise.
- SIEM's can be associated with "noise". Alert fatigue has become a major SIEM problem with organizations receiving an average of 17,000 malware alerts per week.
  - Integrity platforms provides precise and actionable data when integrity and compliance drift occurs throughout your infrastructure. Integrity management practices reduces change noise as much as 95% leaving concise details of unknown, unwanted and unexpected activity.
- Integrity and compliance drift is certain to occur though circumvented or malicious additions, modifications and deletions of data throughout the lifecycle of its operation.
  - Integrity platforms can provide roll-back and remediation capability. Whether it's the restoration of a failed service, configurations, port setting, etc…integrity platforms can roll-back to any number of trusted and operation states as it stores the appropriate files in compressed and encrypted formats.

M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Integrity Controls Are What Give SIEMs/SOARs Their Most Critical Data & Remediation Capabilities

- SIEMs and SOAR's have no remediation capability other than invoking a command to reprovision through a back-up vendor(s).
  - Roll-back and remediation through integrity practices is very different than reprovisioning. Reprovisioning through back-up vendors requires blowing away the OS and Applications and rebuilding from scratch which requires time, energy, and effort whereas Integrity Management can simply restore to any number of previous trusted baselines in seconds.
- SIEMs and SOAR's can not prevent change(s).
  - Designating a change management officer is becoming a popular security practice for mature IT environment. Integrity platforms can restrict authorized changes…even for those that have system admin rights.

M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Appendix A: Implementation and Centralized Access Requirements

Event Forwarding

- Agencies shall forward all required logging data, in near real- time9 and on an automated basis, to centralized systems responsible for security, information, and event monitoring (SIEM); bulk storage; and other analytical workflows or services.

Protecting and Validating Log Information

- To ensure data integrity, logging facilities and log information must be protected by cryptographic methods from tampering and unauthorized access. Agencies shall protect and monitor the integrity of their logs and systems producing logs by:
  - Using integrity-verification mechanisms to detect unauthorized changes to event logging configuration and log files that are no longer being written to or are considered closed.
  - Conducting integrity checks periodically and upon access against the log hashes throughout their retention period.

User behavior Monitoring – Planning

- User behavioral analytics allow for early detection of malicious behavior.

Logging Orchestration, Automation, and Response –Planning

- Federal agencies shall maintain and manage logs by leveraging the additional logging to develop automated hunt and incident response playbooks. Such playbooks shall take advantage of Security, Orchestration, Automation, and Response (SOAR) capabilities.

Application Container Security, Operations, and Management

- Container security and monitoring tools should be integrated with security information and event management (SIEM) tools to ensure container-related events are captured by the enterprise.

M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Appendix C: Logging Requirements – Technical Details

System Configuration and Performance
- Configuration
- Configuration Changes

Network Device Infrastructure (Access, Authorization, and Accounting)
- Changes to, or Attempts to Change, System Security Settings and Controls

Operating Systems & Cloud Environments
- System Configuration

Database Level
- Changes to the Database Structure
- Changes to User Roles or Database Permissions
- Database Configuration

Virtualization System
- System Configuration o Changes to Security Configuration (Success/Failure)
- Changes to Hypervisor
- Changes to VMS
- Changes Made within VMS

Container - Supply Chain
- Log Changes / Deltas Between

Container - Image
- Hash of the Binary
- Hash of the Executables
- Filesystem Changes

Container – Engine
- Configuration Log
- Registration Changes

Container - OS
- System Configuration
  - Changes to Security
  - Configuration (Success/Failure)
  - Audit Log Cleared
  - Changes to Accounts User or Group Management Changes
  - Scheduled Task Changes

CIMCOR

Parting Thoughts & Perspective

Managing from a good or expected state provides a unique ability to pinpoint and highlight everything that is unknown, unwanted, and unexpected!

Our bodies don't have a blacklist or a threat profile to identify when there's a problem. We have white blood cells that flow continuously through our bloodstream to fight viruses, bacteria, and other foreign invaders that threaten our health. They know and understand what is good and identify and attack anything that is unknown and unwanted. They are the baseline to our health.

If our bodies operated like today's security, we would cease to exist as a civilization!

Don’t Let Bright Shiny Objects Distract Us From Solving The Problems of Security & Zero Trust

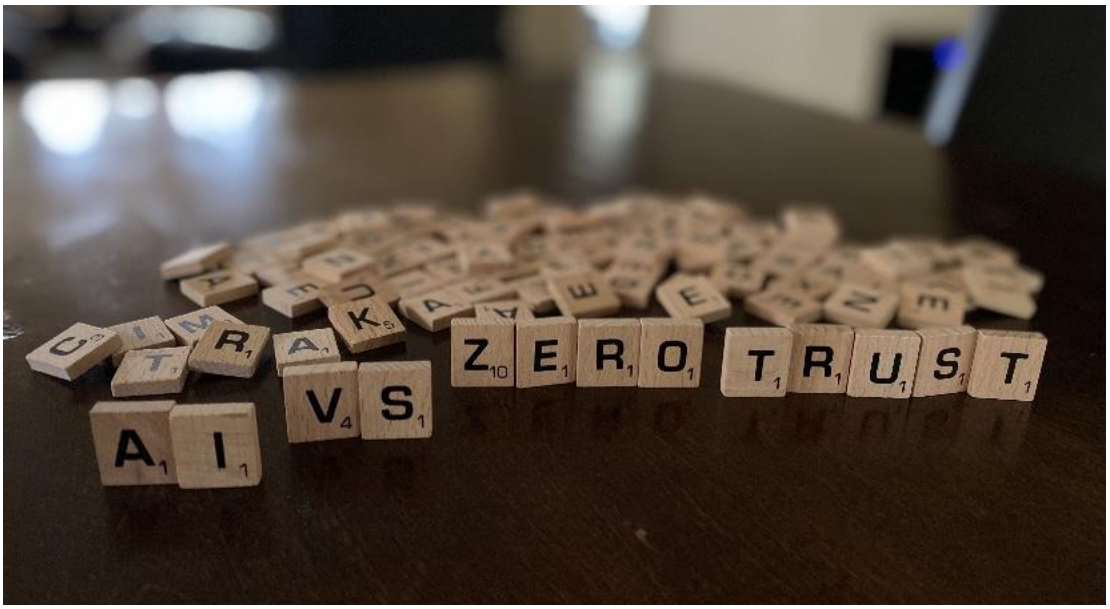
Focus On What Matters…It May Be Boring and Not Sexy…But It’s Proven

Get Back To Basics and Align With Those Controls That Provide The Greatest Value To Zero Trust!

Q&A

Mark Allers
VP of Business Development – Cimcor
Allers.Mark@cimcor.com

CIMCOR



Security: Artificial Intelligence (AI) vs. Zero Trust

Mark Allers, VP of Business Development, Cimcor

AI works via a set of probabilities. When an AI algorithm provides a recommendation, under the hood, the algorithm will make a determination such as 'this file has been classified and has a 29% chance of being malware'. What is the suitable threshold to raise concern to the security engineer? 40% chance? 90% chance? The AI is never 100% sure if something is good or bad unless it has already seen it. All AI is based on machine learning algorithms. This means that to classify a piece of information or make a recommendation, it must be trained on a training dataset of historical information. This entails training the machine learning (ML) algorithm on a training dataset of old or previously seen malware in the cybersecurity field. The ML algorithm attempts to create a model that can accurately classify this old malware with a high level of accuracy (high probability of classifying the historical malware correctly). This is an incredible feat of engineering, but this is also the Achilles heel of AI.

It does a great job of classifying information that it has been trained on and even information similar to data that it has been trained on. However, it often does a terrible job classifying brand new and novel or unique techniques. So, if there is an entirely new piece of malware created and not based on old malware techniques, then it is highly likely that the AI will not correctly detect anything wrong. Another concern scenario is that, sometimes, hackers target a specific organization. In this case, every step by the hacker is custom…once again bypassing most AIs because it will not be similar to anything it has been previously trained. In other words, advanced Zero-Day attacks and customized attacks will very likely bypass detection by even the best AI algorithms.

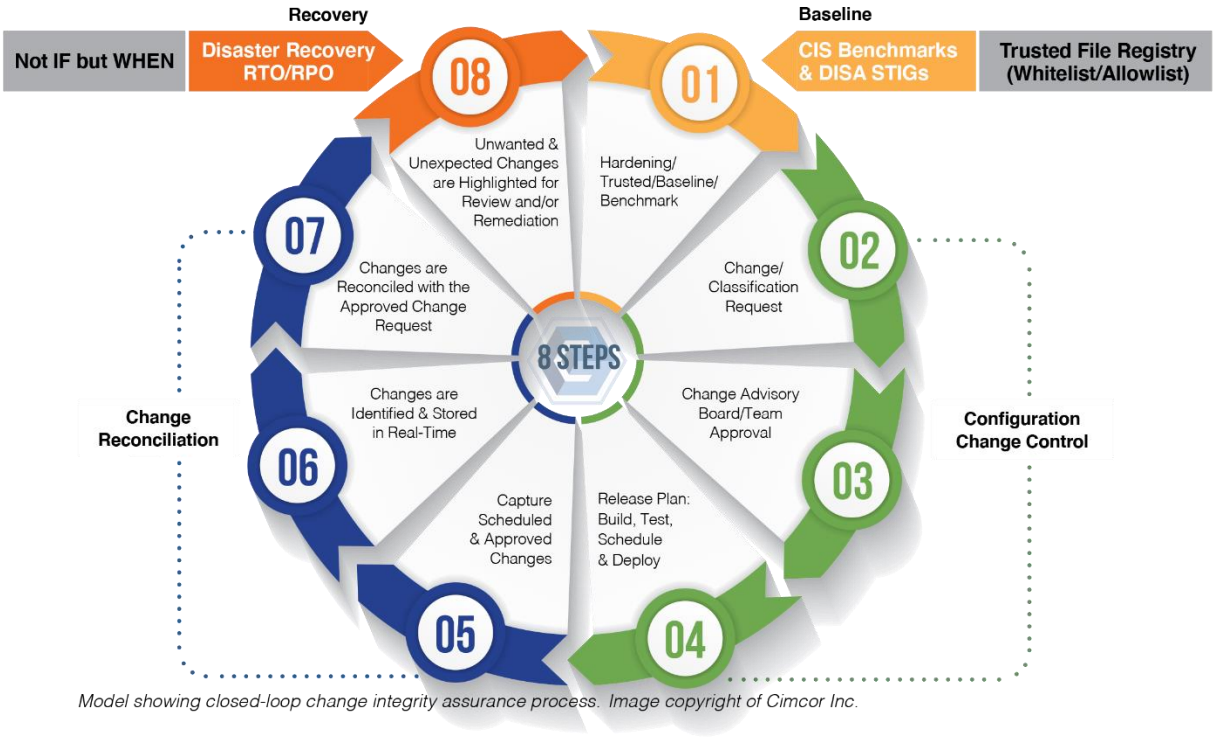
Never trust but always verify!

In contrast, the precise, deterministic, evidence-based method implemented by a System Integrity Assurance solution is effective both for known threats, new threats, and zero-day

attacks. An AI will assume that the file or change is good unless something bad is identified via an AI algorithm and has a `probability of malware` that exceeds a certain confidence threshold. System Integrity Assurance does just the opposite. It will always assume that the file or change is 100% invalid/bad unless a clear audit trail provides non-repudiation data/evidence. The bottom line… an AI will catch new malware and unexpected changes `sometimes,` and System Integrity Assurance will catch new malware and unexpected changes `all the time.`

CimTrak is System Integrity Assurance

The core mission of CimTrak is to identify changes and categorize those changes as good or bad. This is done based on a zero-trust-based philosophy. If there is not a clear audit trail related to the change, it will be considered harmful. If a clear audit trail is found, the change can be classified as good. In CimTrak, this audit trail is based on digital signatures, authoritative baselines based on one-way hash algorithms, hash-based whitelist technology, and a workflow that has coupled the necessary detective controls to create a closed-loop environment for change. This means that when CimTrak indicates that a file is `good,` it is definitely good, and if it indicates that the file is `bad,` that means there is no `proof` that the file or the change is authorized. This is a very deterministic and transparent way of differentiating good changes from bad.



Model showing closed-loop change integrity assurance process. Image copyright of Cimcor Inc.

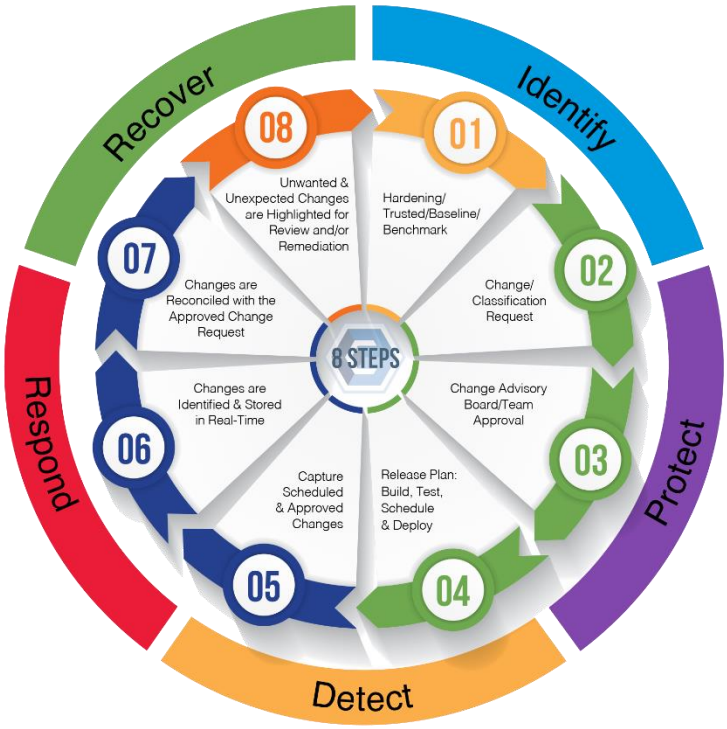
It is invaluable to users to know, without a doubt, if a change is authorized or not. If a new piece of malware is created today and targeted to a system protected by CimTrak, it would detect it. Why? Because there is no proof, there is no audit trail for that malware that would be classified as unauthorized. The result is a clear, binary view of the disposition of changes. CimTrak identifies, prohibits, and remediates unauthorized modifications of files, directories, and configurations and uses the same methodology to manage users, groups, policies, active directories, database schemas, cloud configurations, hypervisors, network devices, and more…

Complicate to profit, simplify to results!

The importance of change control can be seen in several best practices and compliance mandates ranging from NIST 800-53, HITRUST, PCI DSS, HIPAA, ITIL, CIS, CMMC, and dozens of others. Change control and configuration management have even been linked to statistics stating that 91% of all security breaches could be autodetected if these controls were in place and set up correctly.

All security issues start with a change or a need for change.

So, what does this mean relative to something as specific as ransomware? Currently, the industry is addressing the symptom and not the problem. Organizations are focused on the topic of how they must remediate when critical files have been encrypted/changed (symptom) as opposed to detecting and preventing the malicious payload from being delivered and installed (problem), which by definition is a change (addition/modification/deletion) that is not authorized. Don't get me wrong, remediation is essential. Still, it is the last resort of a workflow that follows the five functional requirements of the NIST Cybersecurity Framework (CSF) of identify, protect, detect, respond, and then recover if and when necessary.



CIMCOR

The Authoritative Guide to System Integrity Assurance

SYSTEM INTEGRITY ASSURANCE is the confidence and certainty that the appropriate security controls and compliance requirements are in place to ensure the accuracy and consistency of data throughout its entire life-cycle of operation.

Contents

Introduction

The Importance of Change Management

Why FIM Hasn't Solved Cybersecurity Problems

Conclusion

Introduction

Executive Summary

Despite constantly rising cybersecurity spending, data breaches and security incidents are rising by the year. Despite vendor-prompted calls to invest in more flashy tools and solutions, this is not a problem that organizations can spend their way out of.

Instead, organizations should focus on getting the basics right and maintaining integrity across their entire IT environment. This is what File Integrity Monitoring (FIM) tools were designed to help with—but their promise was never realized.

FIM has a bad name in the cybersecurity industry, mainly because FIM tools don't deliver on their claims or promises. Instead of maintaining integrity, they have become 'shelfware' for most organizations as they are simply too noisy and cumbersome to be useful.

In short, these tools fail to deliver integrity, instead providing nothing more than change monitoring detection.

This white paper will examine how moving away from change monitoring and towards system integrity assurance can significantly help organizations improve cybersecurity outcomes, proactively respond to security threats, reduce the time and effort needed to maintain and demonstrate compliance and employ a zero trust security practice.

Key Learning Points

- Cybersecurity teams are stuck in reactive mode, drowning under a constantly growing pile of alerts—and the prevailing approach to cybersecurity isn't doing anything to help.
- To reverse the current trends, organizations need to re-evaluate the fundamental principles of cybersecurity.
- While flashy tools get more attention, industry experts understand that fundamentals like system integrity, configuration, and change management are more important.
- Change management, a core IT practice, is critical to cybersecurity. Tracking and (where necessary) remediating change in real-time cuts off many security incidents at the source.
- By focusing on maintaining integrity across an IT environment, organizations can drastically improve cybersecurity outcomes while cutting out 95% of change noise.
- When cybersecurity controls and policies are effective, well-enforced, verifiable, and regularly reported, demonstrating compliance ceases to be a drain on time and resources.

Security and Compliance: We're Going the Wrong Way

In 2011, the cybersecurity market was valued at around $60 billion[1] in annual spending. In 2021, it's expected to reach $150.4 billion.[2] That's a Compound Annual Growth Rate (CAGR) of 9.63% over a decade, and there's no sign of spending slowing down.

From 2020 to 2027/28, analysts expect the CAGR of global cybersecurity spending to continue at a rate of 9.4%[3], 10.9%[4], or 12.5%[5], depending on which source you trust.

With all that spending, you'd expect the rate of security incidents and data breaches to fall—but they haven't. The number of recorded breaches is rising year by year. The number of breached records hit a new high during Q1 2021[6], and nobody expects them to fall in the coming years.

When it comes to our ability to identify and contain breaches, there's more bad news.

Between 2015 – 2020, the Mean Time To Identify (MTTI) security breaches remained static at 206 days, while the Mean Time To Contain (MTTC) a breach rose from 69 days to 73 days. That makes the average time needed to identify and contain a security breach an incredible 279 days.[7]

What Can We Learn From This?

Despite a huge rise in cybersecurity spending, threat actors are getting better, faster than we are.

From this, we can deduce two lessons:

1. Today's approach to cybersecurity isn't working.
2. Organizations can't spend their way out of the problem.

And, perhaps the situation is even worse. Increasing cybersecurity budgets and spending creates a false sense of security that comes crashing down when an organization is inevitably breached.

You've probably heard the oft-repeated phrase, "it's not **if** but **when** your organization is breached." While it may seem self-serving for cybersecurity vendors to repeat this over-and-over, it's a truism—and the data above makes it abundantly clear.

[1] https://www.ifsecglobal.com/uncategorized/pwc-report-global-spending-on-cyber-security-to-hit-60-billion-by-year-end/

[2] https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-management

[3] https://www.alliedmarketresearch.com/cyber-security-market

[4] https://www.grandviewresearch.com/industry-analysis/cyber-security-market

[5] https://www.globenewswire.com/news-release/2021/03/17/2194254/0/en/Global-Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html

[6] https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q1-2021

[7] https://www.ibm.com/uk-en/security/data-breach

The 'Fog of More'

We can all agree that no organization can do everything when it comes to cybersecurity. The available systems, controls, and processes are simply too expansive (and expensive) to even contemplate the idea. This leaves organizations trying to figure out which controls to implement with their limited human and budget resources.

This is where we run into a serious problem that most organizations haven't yet solved. Tony Sager, SVP and Chief Evangelist at The Center for Internet Security (CIS), explains[8]:

> *Defenders lose because they are overwhelmed. There's too much advice and too many consultants, tools, compliance requirements, and marketing messages to process. They don't know where to start, and that makes them susceptible to any message or tool that claims to solve their problems.*

With so much choice, many cybersecurity leaders (and their teams) become paralyzed. They do their best to prioritize budgets and energy, but the outcomes don't match their efforts.

Security is Stuck in 'Reactive Mode'

When you're at war, reacting to your enemy is the worst position to be in. However, that's how most cybersecurity teams are forced to operate.

Perimeter defense tools like firewalls and IDS/IPS tools do an essential but incomplete job. The predominant approach to cybersecurity relies heavily on reactive monitoring and incident response, hoping to head off each threat before it does serious harm.

Worse, many cybersecurity teams are over-reliant on individual 'security heroes' to fight threats. This is a poor use of resources, and it's also a dangerous and potentially costly position. Being reliant on individuals creates a huge weakness—what if that person isn't in the office or leaves the organization for a new opportunity?

The fact is that no cybersecurity team should be reliant on individuals—and everybody knows it. What they really need is the proper machinery in place to prevent threats at their source with only limited human involvement.

All of this brings us to an inevitable conclusion:

To reverse the current trends surrounding cybersecurity spending and outcomes, we need to re-evaluate the fundamental principles of cybersecurity.

> *Never permit your enemy to gain an advantage over you in any way. You can be sure your enemy is thinking likewise; either you lead the enemy, or he will lead you.*
>
> **— Miyamoto Musashi,**
> The Book of Five Rings

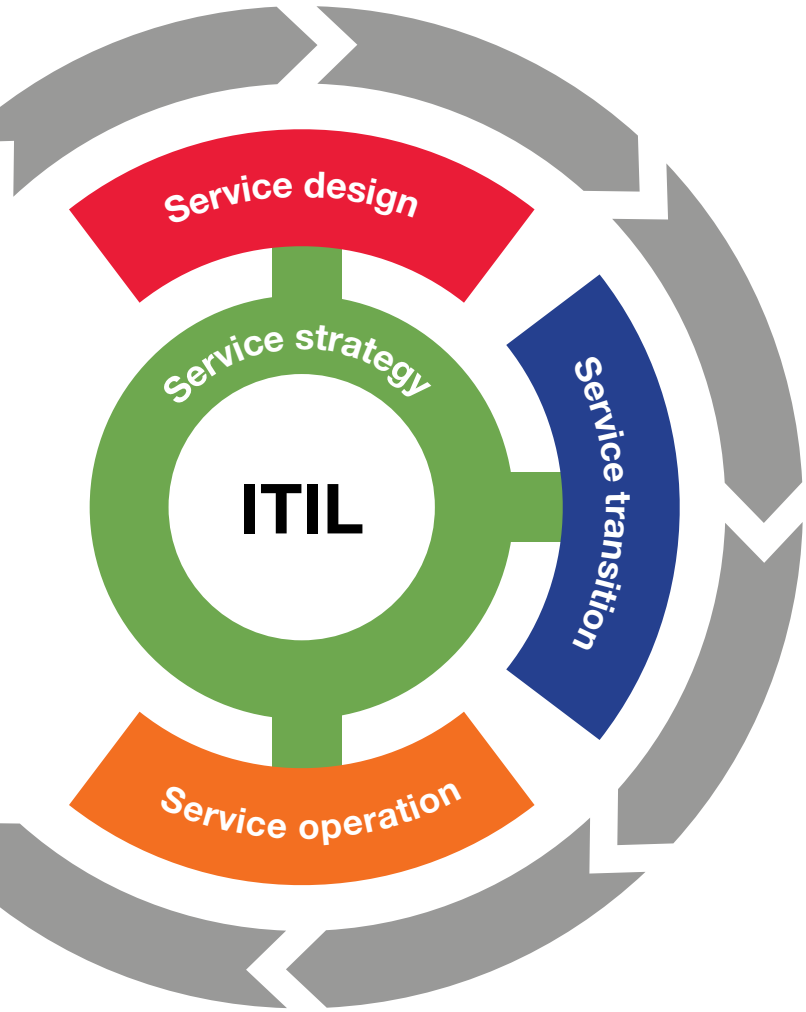
[8] https://www.youtube.com/watch?v=OZLO-xekp3o

What Can Cybersecurity Learn from IT?

Historically, there has been plenty of negativity and friction between IT operations and cybersecurity teams. However, as an industry, we need to accept a simple fact. IT departments have been around a lot longer than cybersecurity teams, and their processes are more mature.

Consider one of the most prominent frameworks for IT service management (ITSM): the IT Infrastructure Library (ITIL). Developed in the 1980s by the UK Government, ITIL has evolved into the most comprehensive set of IT practices ever devised. It's more widely[9] used than any other framework, and even Microsoft used it as the basis[10] for its Microsoft Operations Framework (MOF).

To see what cybersecurity teams can learn from it, consider the ITIL Life Cycle's five principles:



Service strategy defines the perspective, position, plans, and patterns a service provider needs to execute in order to meet business outcomes.

Service design includes the design of services, governing practices, processes, and policies required to realize the strategy.

Service transition ensures new, modified, or retired services meet business expectations.

Service operation coordinates actions and processes to deliver and manage services at agreed levels. It also manages the technology used to deliver and support services.

Continual service improvement ensures services are aligned with changing business needs by identifying and implementing IT service improvements.

Note[11]: These definitions have been slightly condensed for brevity. You can find full definitions in the ITIL® glossary and abbreviations, 2011. Source: AXELOS, ITIL v.3 (2011)

[9] https://www.peoplecert.org/itil-certification-family

[10] https://www.itilnews.com/index.php?pagename=ITIL_V3_and_Microsoft_Operational_Framework_4_MOF_4

[11] https://www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf

Protecting Operations

Notice how ITIL doesn't focus on individual systems or processes but rather on meeting business expectations at a pre-agreed level. IT operations teams have known for years that downtime is inevitable, and all they can do is limit its length and frequency. This is the whole purpose of SLAs—to ensure downtime is kept to an acceptable minimum. This is vital, and it's in stark contrast to how the cybersecurity industry portrays its function.

ITIL emphasizes the importance of getting the basics right and having the systems and processes to achieve the most important objective: minimizing downtime.

Bringing this into the cybersecurity domain, we can assume that some level of 'failure' is inevitable. Almost all organizations will be breached at some point, so the important consideration is how to minimize their frequency, impact, and duration. Scott Alldridge, President at the IT Process Institute (ITPI) and MSSP IP Services, explains:

> *Use a scorched earth approach. Assume you've already been breached and need to recover. What recovery point are you comfortable with, and how long can it take? Once you have your answers, reverse engineer security controls from there just like an IT department would.*

The Importance of Change Management

To ensure business expectations are met, one of the most critical components of ITIL is change management, which is the core function of service transition. For many years, IT departments have understood the importance of change management to maintain SLAs at an acceptable level.

In *The Visible Ops Handbook*, the authors explain (emphasis ours):

> *High-performing IT organizations **eliminate change as a causal factor for an outage as early as possible in the repair cycle.** They identify the assets directly involved in the service outage and examine all changes made on those assets in the previous 72 hours. This information is [compared to] all authorized and scheduled changes. [...] When issues are escalated to problem managers, they have all relevant and causal evidence at hand and [...] can successfully diagnose issues without logging into any infrastructure over 50% of the time!*

This approach is directly applicable to cybersecurity. By setting objectives (service strategy), a baseline for acceptable service levels and activities (service design), and managing changes from that baseline (service transition), cybersecurity teams can achieve the same level of operational success (service operation) as IT departments. Think about it. When was the last time your organization's IT systems went offline for a non-security reason—and how long did it last?

The Importance of Change Management

Cybersecurity Fundamentals: Less is More

How can we apply the ITIL mindset to cybersecurity? The first thing we can do is eliminate complexity and focus on a small number of basic principles. It's telling that just a handful of software vendors dominate the ITSM market.

By contrast, the cybersecurity market has hundreds or thousands of software vendors competing for budget, all with different solutions to different perceived problems. Simply, cybersecurity teams face a huge challenge just to understand their options—let alone to make effective decisions.

In The Paradox of Choice, American psychologist Barry Schwartz argues that eliminating consumer choices can greatly reduce anxiety for shoppers. Bring that into the cybersecurity world, and you can add an extra dimension. Limiting choice for cybersecurity leaders doesn't just minimize anxiety—it also improves results, as measured by the maintenance of acceptable service levels.

The Compliance Problem

Of course, cybersecurity teams face a complicating factor. Unlike traditional IT departments, they are subject to a complicated web of cybersecurity frameworks and regulatory requirements that aim to ensure organizations implement appropriate security controls. These requirements all have slightly different recommendations and priorities, adding to the confusion. Tony Sager, SVP and Chief Evangelist at The Center for Internet Security (CIS), explains:

> *Compliance requirements are what I call cosmic frameworks. They proclaim 'thou shalt achieve this,' but aren't prescriptive about how to do that. It creates an industry of tea leaf readers trying to interpret requirements, which is great for job security but very poor for business outcomes.*

To put this another way, most frameworks take a descriptive approach—they tell organizations what to achieve, but not how to achieve it. Tony explains that this approach creates a 'special snowflake' approach that forces each organization to find its own solution to each requirement. This alone creates a huge amount of work for cybersecurity teams, reducing the resources available to protect against threats.

However, this approach is fundamentally flawed. While there are undeniable differences between organizations, most are more similar than they are different. Worse, the vague nature of requirements creates a 'Wild West' approach to cybersecurity, where thousands of vendors spring up to fill organizations' perceived security and compliance needs—which are often contrary to the simple objective of minimizing the frequency, severity, and duration of security breaches.

Start at the Beginning

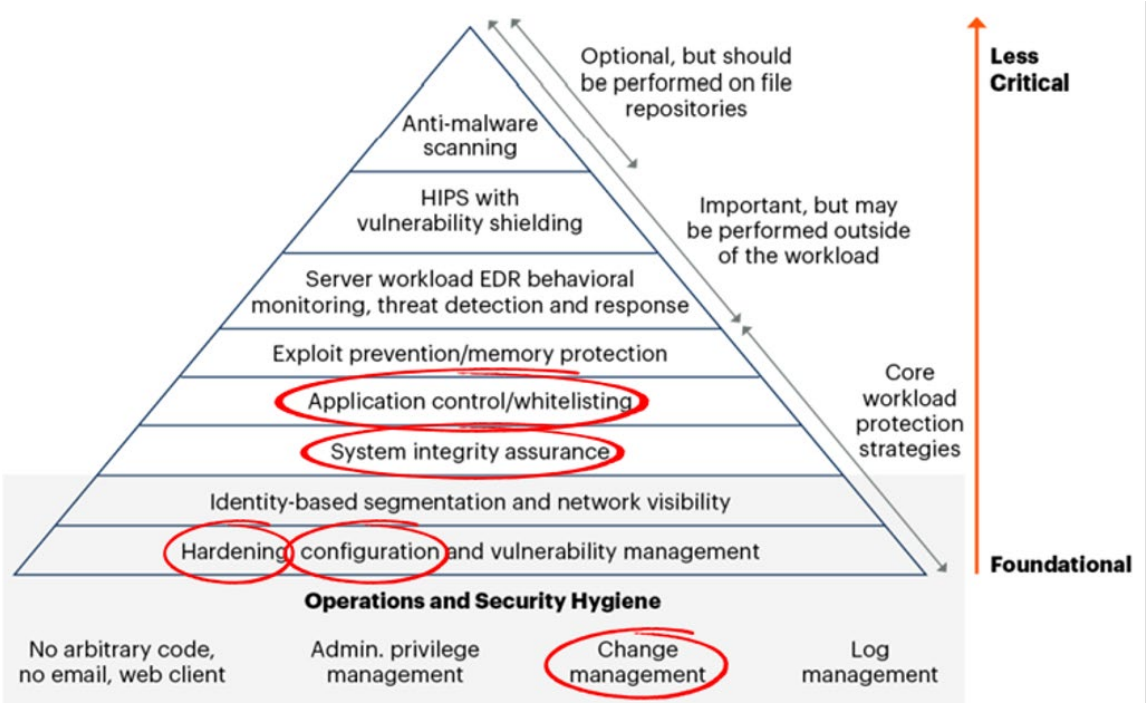
While it's rarely discussed, key players in the cybersecurity industry fully understand the importance of solid fundamentaly—it also improves results, as measured by the maintenance of acceptable service levels.

Notice how some of the industry's most widely discussed solutions are considered less critical and even ***optional***. These include:

- » Anti-malware
- » EDR
- » HIPS
- » TDR
- » Vulnerability shielding
- » Behaviour monitoring

These solutions are so widely marketed that you'd think they are ***critical*** to securing sensitive assets—but this Gartner report indicates quite the contrary.

Risk-Based Hierarchy of Workload Protection Controls



Meanwhile, more 'boring' controls like change management, system integrity assurance, application controls, segmentation, and configuration management are considered ***foundational*** and should be solidified before even considering controls further up the pyramid.

Going a stage deeper, are change management, system integrity assurance, application controls, hardening, and configuration management ***really even security controls?*** Or are they IT considerations? Either way, Gartner acknowledges them as some of the most critical requirements for a secure cloud environment.

Despite this, these controls are rarely discussed or publicized by vendors or analysts. As a result, they are rarely a cornerstone of an organizations' cybersecurity strategy. To find a genuine discussion (and recommendation) for such foundational cybersecurity controls, we have to turn to one of the industry's only ***prescriptive*** (i.e., tells you what to do, not simply what outcomes you need to achieve) frameworks: The CIS Controls.

Prescriptive Controls in Action

In 2001, the NSA released its security guides into the public domain, prompted by several high-profile breaches of its commercial partners. The boundaries between government agencies and their partners were disappearing, and there was a pressing need to help those partners ensure the security and integrity of government data.

There was a problem, though. The NSA guides were extremely thorough and provided far more guidance than a partner organization could implement in a short period. Further guidance was available from organizations like NIST, but this suffered from the same challenge—too many controls, too little time and money.

This resulted in a conversation at the NSA—led by lifelong NSA security expert Tony Sager—about producing a small, prioritized list of essential security controls. After many additions and several changes of ownership, this list became the CIS Controls, a list of just 18 best practice controls (referred to as Control Families).[12]

Unlike typical ***descriptive*** frameworks, the CIS Controls take a prescriptive approach, telling organizations exactly what to do to protect against pervasive cyber threats. To give an idea of their effectiveness, several independent studies of version 6.1 of the CIS Controls found that just the first five controls protected against 85% of all cyber attacks.[13]

Today, the first five controls are:

1. **Inventory and Control of Enterprise Assets**
2. **Inventory and Control of Software Assets**
3. **Data Protection**
4. **Secure Configuration of Enterprise Assets and Software**
5. **Account Management**

Do you see a correlation here to the ITIL controls discussed earlier? At a basic level, they require an organization to establish a continually updated baseline for hardware, software, data, user accounts, and asset configuration—and then track and remediate changes from that baseline.

Contributing to that baseline, CIS also maintains the CIS Benchmarks, a set of 140+ configuration guides to help organizations establish hardened systems to protect against evolving cyber threats. In line with ITIL's service design principle, the Benchmarks provide a baseline for the asset configuration. If the baseline remains current, it's easy to identify activity that isn't acceptable—i.e., unauthorized changes that negatively affect configuration—and block it at the source.

of all security incidents can be auto-detected with three detective controls…**configuration**, **change** and **release management**.

- IT Process Institute

[12] https://www.cisecurity.org/controls/cis-controls-list/

[13] https://static1.squarespace.com/static/555f9696e4b0767a7f0769b3/t/5c885173f4e1fcb114e1e2dd/1552437623967/The_First_Five_Guide_v1.1.pdf

Why Establish a Trusted Baseline?

> *When you're in an earthquake on a unicycle, juggling chainsaws, the only way to survive is to tack down everything you can tack down, so you can deal with what you can't.*
>
> **— Stephen Chakwin**

One of the strangest things about cybersecurity compared to other disciplines is the focus on finding bad things and preventing them. Think about how you would manage physical security for a building, e.g., a government office. How would you stop the wrong people from getting in?

Most likely, you wouldn't try to track ***every single person*** who isn't supposed to be in the building. That would quickly exhaust your resources and achieve essentially nothing. Instead, you'd build and maintain a list (baseline) of everybody who ***should*** be there and use a control system (probably ID cards and security guards) to ensure ***only*** those people are allowed in.

Of course, this system isn't perfect. Sometimes, someone who was supposed to have access isn't allowed in. This is easy to manage. The blocked individual simply tells the guard why they should be allowed in, and it's quickly verified (or not). This process is called 'managing by exception.'

Alternatively, some people will try to force their way in. Again, this is easy to manage by exception. The security guard will see the problem and apprehend them.

This approach runs contrary to most public discussions of cybersecurity principles.

Most cybersecurity controls use blacklists to try to identify all possible 'bad things' and prevent them. Instead of maintaining a small database of things that are allowed, cybersecurity teams maintain a monstrous database of things that ***aren't*** allowed and constantly monitor for them.

This approach is reactive, slow, and misses threats simply because they haven't been seen before.

Imagine how life would be for cybersecurity teams if we followed in the footsteps of traditional IT operations and service management. Consider this ITIL-inspired, basic approach to cybersecurity:

- **Service strategy:** Determine objectives for the security function
- **Service design:** Set a trusted, authoritative baseline of what you have (software, hardware, services, etc.) and what is allowed to ***be*** and what ***happen*** in your environment.
- **Service transition:** Enforce the baseline by monitoring changes in the environment and blocking anything that isn't explicitly allowed.
- **Service operation:** Carry out normal security operations to identify any threats or issues to make it past baseline enforcement.
- **Continual service improvement:** Learn from mistakes and make changes to the baseline.

As we'll see shortly, this approach is very achievable—and with far better results than most cybersecurity teams have come to expect.

Why is Change Important in Cybersecurity?

Once you have a trusted, authoritative baseline, you have a place to start from.

However, there's an obvious argument against the system described above. Even if your baseline is set to a mythical 'perfectly secure state,' one change could create a huge weakness.

Change is the nemesis of IT and cybersecurity professionals who need to maintain a secure and available environment. Unauthorized, unexpected, and unwanted changes to critical files, systems, and devices can quickly open a gaping hole in an organization's cybersecurity posture. At that point, it doesn't matter how good the rest of its controls are—a breach may be imminent.

What is a Change?

Everything that happens in an IT environment (good or bad) starts with a change: a file, configuration setting, or device is altered, deleted, added to, or even just read by a user or service.

Every bad thing in an organization's environment begins with change… but so does every good thing. The challenge lies in determining the difference between good and bad. This is also where our baseline comes into play. Anything not included in the baseline can be assumed bad until proven otherwise. For each change, an organization can follow a simple process:

1. Determine precisely what changed in the environment.

2. Check whether the change is authorized under the baseline.

3. Allow, block, or roll back the change as appropriate.

> *"You need to know what you have and what changes are acceptable. Then you have to stop everything else and manage by exception where necessary. It's not necessarily easy because there's lots of change. If you have the machinery to control this, you have the basis of integrity."*
>
> **— Tony Sager,**
> SVP and Chief Evangelist at The Center for Internet Security (CIS)

As of March 2020, the total number of new malware detections worldwide amounted to **677.66 million programs**, up from 661 million new malware detections at the end of January 2020. These malicious programs intend to add, modify or delete files, which can be mitigated through a closed-loop change control process.

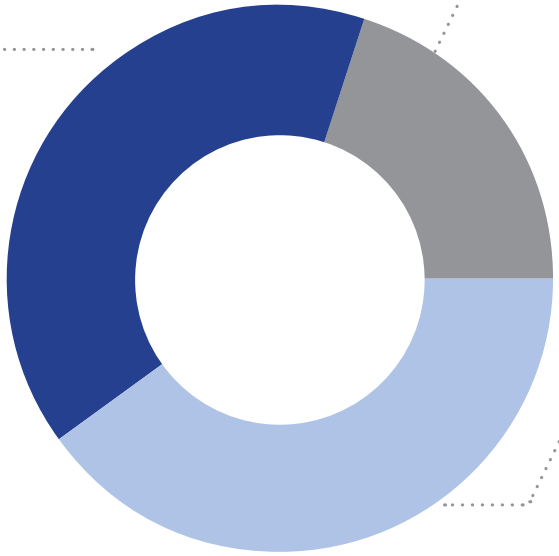
Why is Change So Important?

As we've seen, all bad things in an IT environment begin with change. This fact is clarified by IDC research, which found that a huge proportion of IT outages are caused by human error, including failure to conform to change management processes. In other words, failure to properly manage change in an IT environment is among the largest causes of unplanned downtime.

Operations Errors
40%

People and Process

- Hiring, Training, Procedures
- IT Process Maturity
- Automation & Ops Arch
- Change & Problem Mgmt.
- Integration and ProdIT-DRM Modernization Validation Testing



Environmental Factors, HW, OS, Power, Disasters
20%

Externals

- Redundancy
- Service Contracts
- Proactive Monitoring
- Business Support

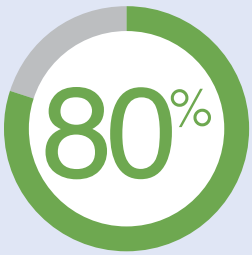
Application Failure
40%

People and Process

- App. Architecture/Design
- SDLC Enhancements
- Change & Problem Mgmt.
- Configuration Management
- Performance/Capacity Planning

Model is based on Gartner IDC Study on Causes of Network Downtime

Donna Scott, VP and Research Director at Gartner, goes a step further by stating that:



> 80% of unplanned downtime is caused by people and process issues, including poor change management practices, while the remainder is caused by technology failures and disasters.

Based on their experience working with hundreds of IT organizations, the authors of The Visible Ops Handbook further note that even once an incident has occurred, 80% of Mean Time To Recovery (MTTR) is wasted on non-productive activities. Most notably, determining which change is responsible for the outage.[14]

[14] https://itpi.org/the-visible-ops-book-series/visible-ops-handbook-review/

Managing Change as a Cybersecurity Function

A study commissioned by the U.S. Department of Defense (DoD) determined that:

> *Information security hinges on the effectiveness of the change management process. As a result, we need to implement a detective control to verify compliance [with an authoritative baseline] and take decisive action when the process is not followed.*

Source: File integrity monitoring tools: Issues, challenges, and solutions, Applied Research Center, Florida International University, 2020[15]

Notice the wording. Change management isn't just important—it's the lynchpin of the entire information security function. With all this in mind, why hasn't there been an attempt by cybersecurity vendors to address change management?

As it turns out, there has: File Integrity Monitoring (FIM) tools.

> *All security start with a change or a need for change. For this reason, change control becomes the ultimate security backstop regardless if it's on-prem, VM's or in the cloud.*

[15] https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5825

Why FIM Hasn't Solved Cybersecurity Problems

If change is so important, how do you monitor change in an IT environment?

Simple: use a monitoring tool that tells you every time something changes. This is what FIM tools were initially designed to do—detect changes in all files across an IT environment and alert the cybersecurity team. This approach is approved by the DoD study mentioned above.

Note the use of integrity. If a file has integrity, it is in precisely the right state and only affected by permitted changes. The state of a file is determined using a cryptographic checksum—known as a file hash—and other checks such as file size, version, modified by, creation date, modified date, cache operations, and configuration values.

The study goes on to note that a FIM tool "*[...] compares and verifies the current state and baseline of files [...] to detect unauthorized file operations in a system.*"

If FIM tools did what they were supposed to, they would help cybersecurity teams identify and prevent most attacks—at least those that rely on file changes or access. But, as most security professionals already know, FIM tools don't do what they are meant to do. Here's why:

> *Ensuring integrity of sensitive files in file systems is imperative to computer systems. The vast majority of attacks work through unapproved or unauthorized access to sensitive files to take secret data like secret keys, passwords, credit card numbers, and so on. After that, attackers generally conceal their traces by subverting critical files like system logs.*
>
> Source: File integrity monitoring tools: Issues, challenges, and solutions[15], Applied Research Center, Florida International University, 2020

Problem #1: Noise

A typical FIM tool simply monitors files for change and produces alerts—lots of alerts. They produce so many alerts they have become 'shelfware' for most cybersecurity teams. They are theoretically valuable but useless in the real world because they produce too many alerts to manage with no context or verification.

Noise is a ubiquitous issue across many cybersecurity tools. Security Operations Centers (SOC) and Incident Response (IR) teams are already buried under more alerts than they can manage, so they simply shut off or ignore alerts from their FIM tool. They keep the tool for compliance purposes, of course—they just don't use it.

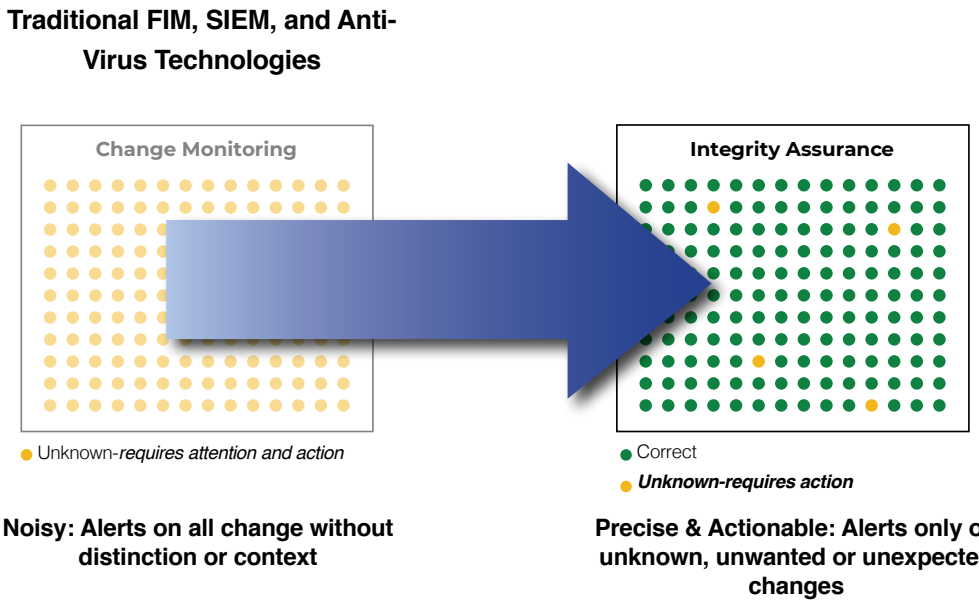
[15] https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5825

Problem #2: FIM Isn't FIM

At the heart of this problem lies a simple fact:

FIM tools don't provide FIM (File Integrity Monitoring) at all. They provide basic File Monitoring or in many cases just the simple action of detecting change.

The following graphic shows the difference between File Monitoring and System Integrity Assurance.



On the left, we see what typical 'FIM' tools provide: a massive list of changes without any context or distinction. This list is too large to triage, so cybersecurity teams ignore these change alerts.

On the right, we see what a FIM tool should provide: a small list of unverified changes to be signed off, prevented, or rolled back. This list is easy for cybersecurity teams to process and helps to maintain the integrity of files or directories. To use our ITIL-inspired objectives, it also helps to minimize the frequency, severity, and duration of incidents and breaches.

Imagine the difference between File Monitoring and FIM after a big update, e.g., Patch Tuesday.

There could be hundreds of thousands of changes in the IT environment, and a File Monitoring tool would create an alert for every single one. There could be a hundred unauthorized, dangerous changes in that list of alerts, but nobody would know because they don't have time to check. At best, the tool might integrate with some blacklist resources to identify changes known to be malicious. Still, though, the list of unverified changes is far too large to manage.

On the other hand, a genuine FIM tool (i.e. a System Integrity Assurance platform) can identify every change that is allowed, including those made by vendor-verified patches, and exclude those from its alerts but still securely stored for audit evidence. By highlighting only changes that aren't explicitly allowed, FIM tools could enable cybersecurity teams to manage by exception—and FIM then becomes a cornerstone to what its initial intentions and objectives were designed for.

Problem #3: Too Resource-Intensive

Most FIM tools identify change by completing daily polling scans of all files in an IT environment. This process is hugely resource-intensive, so it usually happens overnight. While it would be more valuable to scan the environment continuously, this is simply impossible, as it would interfere with other IT operations.

Bringing Integrity to Your Environment (Not Just Files)

Integrity is the accuracy and completeness of data throughout its entire life cycle. That means no matter what service, device, or user accesses, stores, processes, transmits, or receives data, it remains accurate and complete. For this to be possible, four things are needed:

1. **An authoritative baseline of what data should look like.**
2. **A way to identify and protect data from unauthorized change.**
3. **A way to roll back unauthorized changes not blocked at the source.**
4. **A way to verify that controls 1 – 3 are in place and working correctly.**

Notice we're talking about ***data***, not just files. To have integrity, you need to protect all of the data in your environment—including data held in configuration files, network devices, endpoints, directory services, cloud instances, and more. We'll cover this in more detail in the next section.

Other Tools that provide 'FIM'

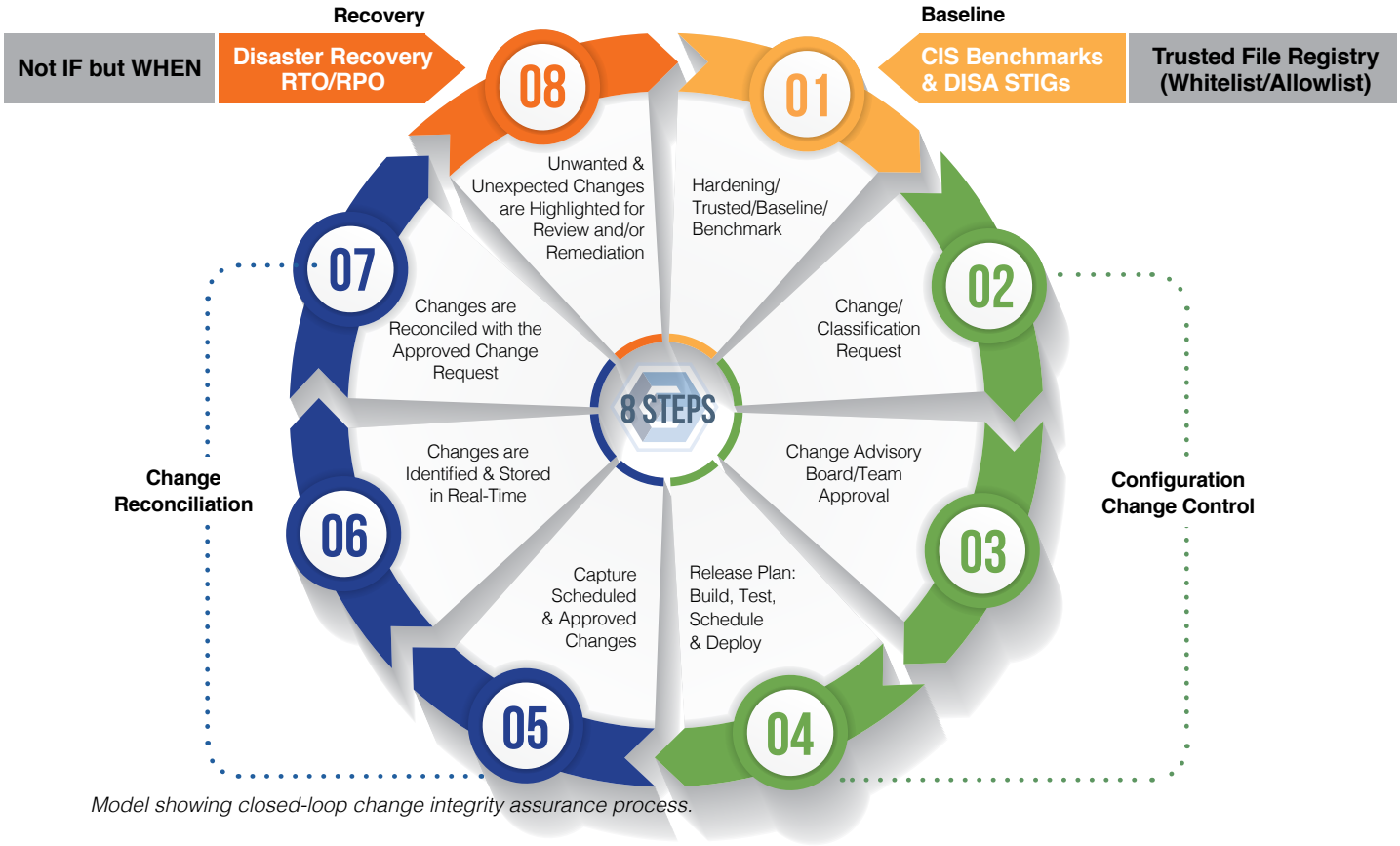
Many cybersecurity solutions like AV and SIEM tools claim to provide FIM. However, these tools suffer from the same problems—they provide change alerts without context or verification. Once again, this is just FM or Simple Change Monitoring posing as FIM.

> *Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct.*
>
> **— Mike Chapple,**
> Professor of IT, Analytics & Operations, University of Notre Dame

Working From a Trusted Baseline

System integrity assurance works under the same principle as physical security. It establishes a known, trusted, and authoritative baseline of what is allowed and then prevents, limits, or rolls back everything else. Whenever an unknown change occurs, it's managed by exception so that acceptable changes are added to the baseline while unacceptable changes are prevented.

Closed-Loop Integrity Assurance can be demonstrated to work as follows in the real world.



Model showing closed-loop change integrity assurance process.

This is a closed loop process for managing changes from a trusted baseline. Similar to the change management procedures laid out by ITIL, the loop covers all stages needed to ensure only acceptable changes are allowed to proceed, while others are prevented or rolled back.

There's an obvious elephant in the room: **This looks way too time-consuming.** What cybersecurity (or IT) team has time to run through this entire process for every single change?

So long as there is a trusted and authoritative baseline in place that includes everything that should ***be*** and ***happen*** in the environment, the loop only needs to occur for unknown changes that need to be verified. I.e., changes that aren't known for sure to be good or bad.

Further, the majority of this loop can be automated. With the right technology—one that continually updates the baseline to reflect changes known to be good or bad—human intervention is only needed for a small percentage of changes. In the next section, we'll see FIM in action, including how it can suppress traditional 'change noise' by up to 95%. First, there's another elephant in the room.

Why is Nobody Talking About Integrity?

Beyond 'lip service,' almost nobody in cybersecurity talks about integrity, least of all vendors. Some compliance frameworks include integrity as a requirement but include no guidance on how to achieve it—and most of the time, genuine integrity isn't required to pass a compliance audit.

The obvious reason is that **integrity is boring**. It's more fun to focus on the latest shiny tools than to steadfastly stick to the fundamentals. However, this theory puts the blame on the shoulders of cybersecurity teams and their leaders—when in fact, it should be somewhere else.

Tony Sager, SVP and Chief Evangelist at The Center for Internet Security (CIS), explains it like this:

> *Cybersecurity has been treated like wizardry. If you treat it like wizardry, the only defense is more wizardry. You need flashy tools and insight into what some hacker is doing in another country. Honestly, most of this stuff is overblown in terms of its real value. Wizardry is great for job security but bad for corporate success. You can't have a program based on wizardry. You need to have discipline and management and repeatability and data and science behind it.*

Dr. Ian Levy, chief technical director of GCHQ's National Cyber Security Centre, took a more direct approach to the problem during a 2019 talk:

> *We are allowing massively incentivized companies to define the public perception of the problem. If you call it an advanced persistent threat, you end up with a narrative that basically says, 'you lot are too stupid to understand this, and only I can possibly help you. Buy my magic amulet, and you'll be fine.' It's medieval witchcraft. It's genuinely medieval witchcraft.*

The System Integrity Assurance Platform(s)

A system integrity assurance platform enforces the Integrity Assurance Loop explained in the previous section. It enforces a trusted baseline across an entire IT environment to allow expected, legitimate changes to go ahead, block or roll back changes known to be dangerous, and alert on unexpected changes that aren't known to be good or bad. A system integrity assurance platform is very different than a simple change monitoring/detection tool. A system integrity assurance platform focuses on encompassing the entire workflow while interfacing with a variety of external tools, in order to achieve compliance.

To achieve this, system integrity assurance platforms must rely on three critical components:

1. **Maintain and secure a complete inventory and register of all critical files** throughout the network. This includes those held by hardware and software assets, along with their correct states, configurations, and settings.
2. **Access to whitelist/allowlist database of known and trusted file hashes** containing metadata, and configuration settings to validate and verify the integrity and authenticity of data, no matter where it is.

Remember our physical security analogy? The best way to ensure bad things don't happen in an IT environment is to *only* allow good assets and changes.

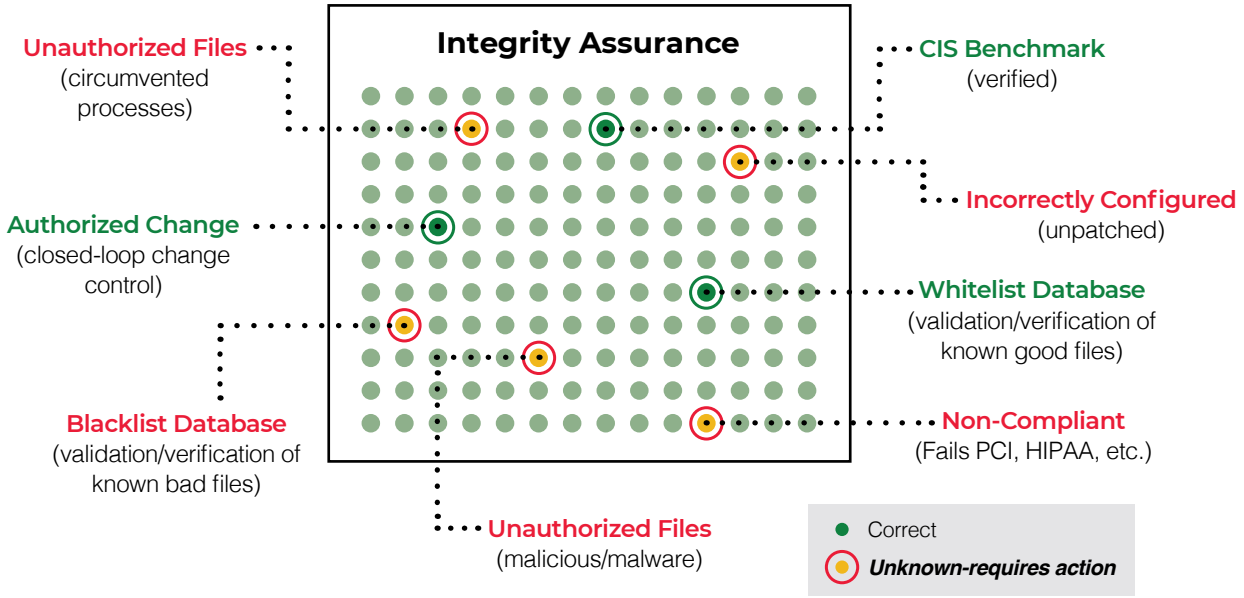
However, there is still a benefit to the traditional approach of identifying and categorizing malicious files and activity: it reduces noise. If you have a current list of files and activities known to be malicious, there's no need for a human to manually investigate them when they turn up in an IT environment. This is why integrity assurance platforms employ a fifth component:

3. **A blacklist/denied list** of known bad file hashes from external intelligence from threat feeds, file reputation services, and malware data repositories. Ideally, an integrity assurance platform would be able to alert if any blacklisted/denied list files were ever resident on any device or system during it entire operating life-cycle.

What's in a whitelist/allowlist?

A whitelist/allowlist must include all known and trusted file hashes to validate and verify the authenticity and integrity of individual files, configuration settings, etc. This requires a massive database constantly updated with the latest OS updates, software patches, etc., in all languages, customized by country. This amounts to a list of billions of hashes, and the list must grow in real-time to keep change noise to an absolute minimum.

By including these three components, system integrity assurance platforms can further enforce integrity across the IT environment while suppressing traditional change noise by 95%. Instead of triaging a torrent of unknown changes (which no one can do), cybersecurity teams only triage a small number of potentially harmful changes. Once these changes are categorized, the baseline is automatically updated so that the platform can handle future changes of the same type without human intervention.



This brings us to the ultimate question:

What happens if you know every time something changes, and you stop anything that isn't authorized… and you expand this capability across all asset classes?

- Ransomware and other malware can't run in the environment.
- Attackers can't traverse the network or exfiltrate data.
- Nobody can add, modify or delete files or configurations to make them non-compliant or introduce new risks or vulnerabilities.
- Users can't accidentally run malicious attachments.
- Nobody (even privileged administrators) can alter critical system files.
- Mitigates software supply chain security issues and risks.

This approach doesn't solve cybersecurity entirely. The field is too large and complex for that to be possible. But it does take away a massive proportion of the risk and threats that can arise in an IT environment with minimal human involvement.

It's Not Just About Files (or Monitoring)

As we have already alluded, FIM is crucial, but it's not enough to ensure integrity across an IT environment. File changes are important, but what's vital is changes to data—wherever it exists. This covers a wide range of hardware and software assets, including:

- Files
- Configuration
- Databases
- Hypervisors
- Network devices (e.g., firewalls, switches)
- Metadata (e.g., of databases)
- Directory services
- Endpoints
- Cloud instances and containers

At the same time, integrity is about far more than monitoring change. A system integrity assurance platform must include ten critical capabilities to enforce integrity across an IT environment:

CIS or DISA STIG benchmark support and integration.

Real-Time change monitoring and detection to identify all changes within the environment.

Collection and storage of forensic evidence and detail for every change, including the source IP, user, time, and process.

Reconciliation and curation between observed changes against authorized/approved changes.

Categorization (i.e. whitelist/allowlist and black list/deny list) of changes as good, bad, or unknown.

Alerting for unknown changes that require human intervention.

Prevention of disallowed changes to sensitive assets.*

Roll back and remediation (A.K.A. 'self-healing' or resiliency) of disallowed changes to other asset groups.*

Baseline updates to include new file hashes and configurations categorized as good.

Embedded ticketing functionality to enable workflow automation and control or integration with traditional ITSM tools.

What's in a trusted, authoritative baseline?

A trusted baseline includes all of the assets, file hashes, configuration settings, etc., allowed to exist in an environment. In addition to information determined by the organization, an integrity assurance platform leverages best practices from authoritative sources like CIS Benchmarks and DISA STIGs to establish a known and trusted baseline that can be restored at any point in time.

*Some assets (e.g., critical system files) should never be changed, so these changes are blocked. Other changes are categorized as bad after the event and immediately rolled back to a trusted state.

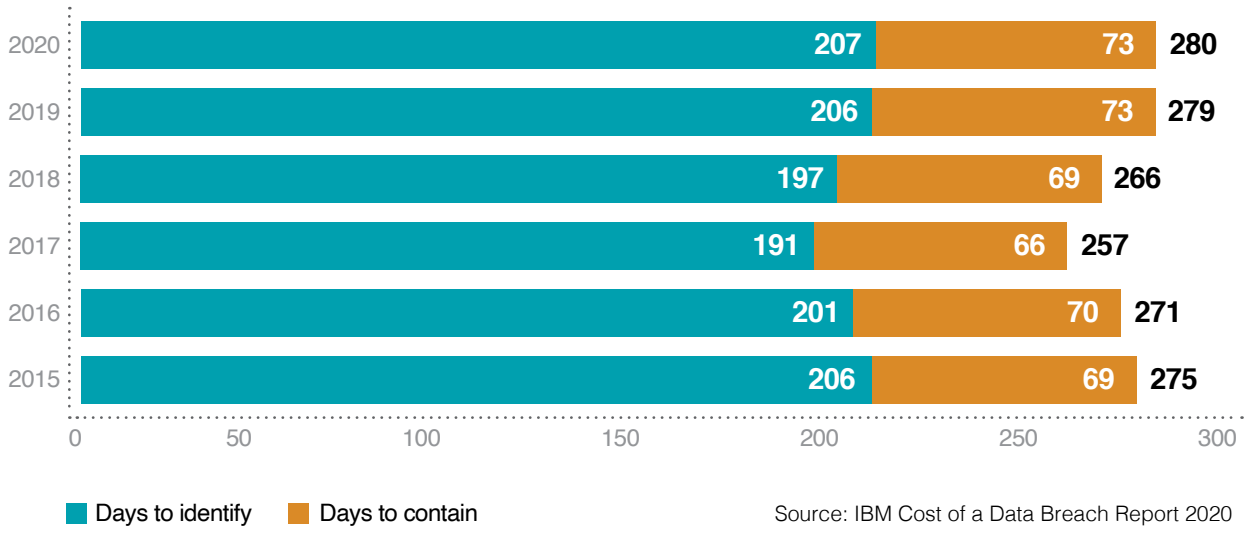
A system integrity assurance platform completes these actions automatically and in real-time. A human only gets involved with unknown and unexpected changes to decide if they are acceptable. Even then, the platform should note the decision to deal with similar changes automatically in the future.

This provides several key benefits:

- Blocks most threats at their source.
- Instantly 'heals' files and settings to their trusted state.
- Provides deep insight into the state of any asset or system.
- Decreases incident response time by providing thorough forensic evidence.
- Reduces remediation time and costs.
- Drastically improves compliance audit (preparation and inspection).
- Decreases MTTI and MTTC to just seconds…rather than months.

A system integrity assurance platform drastically improves cybersecurity posture and outcomes without the need for flashy gimmicks, advanced CTI, or Artificial Intelligence. It might be boring, but it works.

> *Based on our extensive testing across the DoD, Intelligence Community, and rest of government, it was clear to me that secure configuration management is a foundational, must-do element of any successful security management program.*
>
> **— Tony Sager,**
> Senior VP and Chief Evangelist at the Center for Internet Security (CIS)



Source: IBM Cost of a Data Breach Report 2020

Why Verify Integrity in Real-Time?

There's little point in reaching a trusted baseline if you can't maintain it.

A major failing of traditional FIM tools is their lack of real-time monitoring. Most FIM tools run daily polling scans that drain system resources and fail to identify any harmful changes in between. This renders the organization unable to respond to attacks (and even mistakes) for as much as 24 hours, giving attackers ample time to cause damage, traverse the network, or steal sensitive data.

Even then, a typical FIM tool only provides monitoring, leaving the organization to identify malicious changes and complete remediation efforts.

Real-Time Verification Prevent Breaches

Only by monitoring change in real-time can an organization respond instantly to unexpected and unwanted changes. This is the only way to proactively prevent cyberattacks at their source without restricting operations to reactive threat feeds.

There's nothing wrong with ***using*** threat feeds, of course—but they should be a supplement to integrity assurance, not a replacement.

A major benefit of integrity assurance platforms is the ability to 'self-heal' files and settings to a trusted state. For example, if a server configuration setting is changed in a way that makes it non-compliant with the appropriate CIS Benchmark or DISA STIG, the integrity assurance platform can instantly reverse the change before it causes harm.

For sensitive files and assets, the platform takes this a stage further by enabling cybersecurity teams to block all changes at the source. Now, even a privileged administrator will be unable to make changes unless the block is lifted.

All of this is only possible with an integrity assurance platform.

Improved Performance

We've established that the polling scans conducted by typical FIM tools are resource-intensive. Doesn't that mean real-time monitoring should be even more resource-intensive… *all the time?*

No. System integrity assurance platforms don't scan the environment constantly. They scan it once to establish a baseline, then receive change data from agents and modules across the environment, often in real-time. If an asset or file doesn't match the baseline, the tool knows a change has occurred. This process is highly efficient and barely registers on the resource monitor.

Note: Agents and modules harvest data at the kernel level with higher privileges than the pure user-mode only solutions employed by other FIM tools. This enables system integrity assurance platforms to gather deeper forensic evidence, adding more value to change management and incident response.

Mastering Compliance (Without Wasting Resources)

Perhaps the biggest challenge organizations face is maintaining compliance with regulatory and partner requirements. They manage it briefly for their annual audits, but maintaining compliance year-round seems out of the question. This is another area where cybersecurity can learn from IT.

In *The Visible Ops Handbook*, the authors note that high-performing IT organizations have a trusting relationship between operations and auditors. Controls and policies are effective, well-enforced, verifiable, and regularly reported on. As a result, they spend very little time on compliance activities and audit preparation—and they also have fewer audit findings and repeat findings.

When you have outstanding systems and processes—including automatic audit trail capture—the proof element of compliance becomes easy to manage.

> *Compiling evidence for compliance isn't a good use of time. You only do it because the regulator says you have to. Most organizations have lots of regulators to satisfy, so it becomes a very repetitive and painful process. If you have good machinery and operations, it provides almost all the proof they need, and those resources are freed up for more useful activities.*
>
> **— Tony Sager,**
> Senior VP and Chief Evangelist at the Center for Internet Security (CIS)

System Integrity Assurance for Compliance

A system integrity assurance platform automates the process of achieving and maintaining compliance with frameworks like PCI-DSS, HIPAA, NIST 800-171, CMMC, and many more. It does this by:

1. **Building the requirements of all applicable frameworks into the trusted baseline.**
2. **Continually monitoring all files and configurations against the baseline.**
3. **Raising an alert when it finds an issue or misconfiguration and providing clear evidence and guidance on how to resolve it.**

Armed with this information, it's easy for cybersecurity teams, asset owners, and IT operations teams to quickly identify and resolve any issues that bring the organization out of compliance.

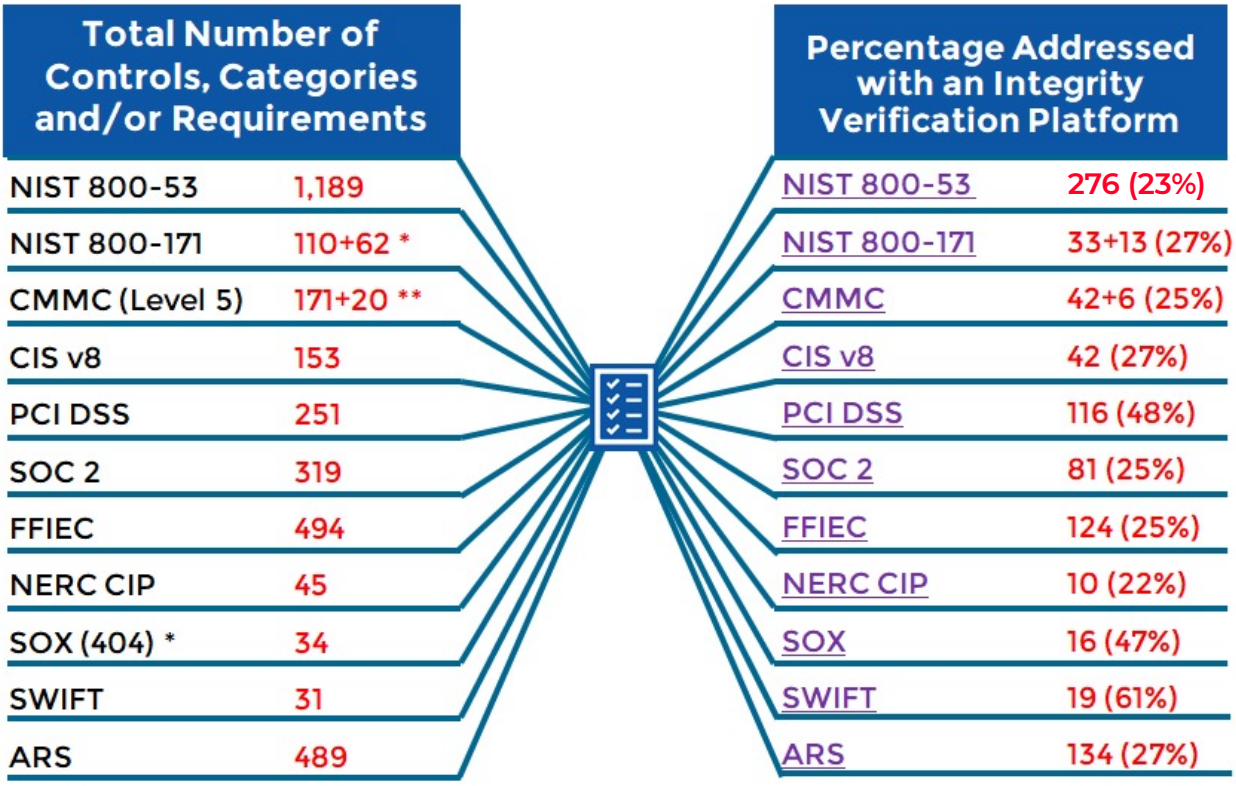
Critically, this mostly automated process provides the monitoring, enforcement, and audit trail needed to demonstrate compliance at any time—not just during an audit. This drastically reduces the amount of time and resources spent on compliance activities, freeing them up for more valuable, security-oriented functions.

Note: This is another area where roll back or 'self-healing' capabilities come to the fore. Most of the time, changes that lead to non-compliance are unintentional, and the files or configurations involved shouldn't be changed. An integrity assurance platform can automatically roll back these changes, ensuring ongoing compliance and reducing the compliance workload.

How Compliance Frameworks Map to Integrity Assurance

Integrity assurance can help any organization reach and maintain compliance with any framework. All that's required is for the cybersecurity team to update its trusted baseline to include all relevant compliance requirements and then action any alerts the system raises.

To give an idea of how valuable integrity assurance can be to a compliance program, the image below shows how it maps to eleven common frameworks.



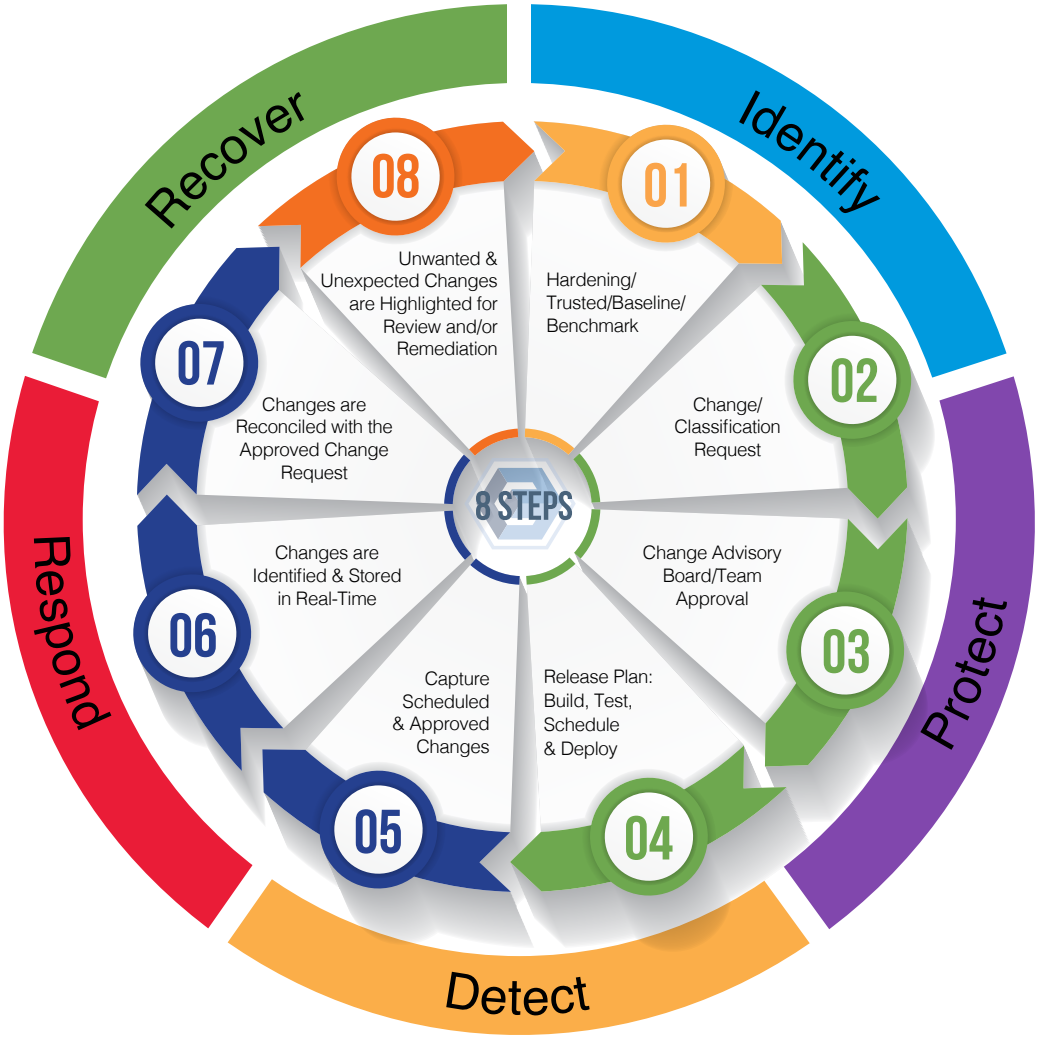
Integrity Assurance and PCI-DSS

PCI-DSS includes two sections that require a change detection capability: 10.5.5 and 11.5. An integrity assurance tool comfortably satisfies these requirements—but it goes much further. An integrity assurance tool covers 116 (48%) of the framework's controls, drastically reducing the amount of resources needed to reach and maintain compliance.

How Does System Integrity Assurance Align With NIST?

The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public.

One of those best practices frameworks is the Cybersecurity Framework (CSF) which helps organizations understand and address risks with a common approach and language to improving critical infrastructure cybersecurity. The Framework Core is a set of cybersecurity activities and principals aligned with a desired outcome common to all critical infrastructures and verticals industries. The Framework Core consists of five functional areas that considers a lifecycle approach to an organization's management of cybersecurity risk—Identify, Protect, Detect, Respond, Recover.



As you can see, NIST's five core functional areas align directly with that of the eight steps of a closed-loop integrity assurance model. This alignment provides for a consistent and uniform strategy when implementing an integrity strategy that incorporates not just one or two of the NIST functional areas but all five.

Zero Trust IS System Integrity Assurance

Zero Trust is a strategic initiative that helps identify and prevent successful data breaches by eliminating the concept of trust within an organization's network architecture and replacing it with integrity assurance. This is further supported by SANS CIA which includes three key security principals that every system should adopt as a standard and best practices—Confidentiality, Integrity and Availability.

There are three stages of a Zero Trust security model—Assessment, Control, and Recovery operations. The premise for a Zero Trust solution requires an approach to never trust but to always verify. This means that every user, device, application, workload and data flow should be treated as untrusted. Zero Trust is fundamentally a shift in how we approach security. To date, we've tried to identify malicious activity through a methodology of searching for the bad as opposed to managing form a known good and verified state of operation. When changes to a system happen, they ALL must be considered untrustworthy until a workflow process validates and verifies its integrity of those changes by determining if they were approved and authorized by an authoritative person or board. Only until this happens will the concept of Zero Trust become a reality.

Conclusion

It All Comes Down to This

In exercise science, there's a common expression:

> *Complicate to profit, simplify for results.*

The implication being that if you want to lose weight or get fitter, you don't need a Navy SEAL inspired workout or an expensive exercise machine. Instead, you should focus on the basics: eating better and getting some exercise. Most people intuitively know how to do these things—but there's no money in teaching people how to do the basics.

Parallels to the cybersecurity industry abound.

With literally thousands of vendors selling a cacophony of products, services, solutions, and advice, it's hard for cybersecurity teams to know where to focus their efforts and resources.

This white paper has made a case for focusing not on flashy toys, but on getting the basics right. It's not the most exciting approach to cybersecurity, but it's far more effective than chasing the latest trends and threats.

System integrity assurance is a path to create and maintain an IT environment that is resilient to dangerous change—both accidental and malicious. As mentioned multiple times throughout this paper, the end goal is the same as it is for IT operations:

To maintain a secure, available IT environment that supports business objectives.

If you have questions about system integrity assurance—or anything else related to this white paper—you can contact us at info@cimcor.com

The System Integrity Assurance Platform Selection Checklist

System Components:

- Asset discovery capabilities to identify, inventory, and collect information about all physical assets connected to the network. Includes routers, switches, servers, hosts, and firewalls.
- A comprehensive register and storage of all critical files in the environment, including those held in hardware and software assets, cloud instances, containers, etc.
- Built-in ticketing system, or at least two-way integration with an existing ticketing system.
- Compliance assessment, reporting, and remediation guidance.
- Integration with tools (e.g., SIEMs) to provide the enhanced analysis, correlation, and forensic data needed to mitigate attacks and detect anomalies.
- Ability to query both whitelist and blacklist databases to validate and verify file trust and authenticity.
- Comprehensive dashboards and reporting for all security and compliance needs.
- A full change management workflow that covers identification, investigation, triage, assigning tasks to engineers, final remediation, and confirmation.

Note: An unalterable audit trail avoids the danger of an administrator disabling the solution or monitoring of specific files/configurations.

Security Requirements:

- Encrypted communications between system components.
- Encrypted and compressed storage of file hashes and settings.
- Encrypted audit logs that are unalterable, even by system administrators.
- Monitoring of actions taken by solution administrators and users.

Questions to ask:

- Is the solution capable of true real-time change detection?
- Does it provide all the functions needed for integrity assurance (or is just file monitoring)?
- Is it easy to install, configure, and use?
- Can it be set up to meet your needs? (e.g., agent or agentless, on-premise or virtualized)
- Does it collect critical change information such as the user, process, and originating IP?
- Can it show precisely how a file changed with a side-by-side comparison to the original file?
- Does it integrate with other security solutions such as SIEMs?
- What inherent security does the solution have?
- Does it require costly training or professional services to implement and maintain?
- Is it scalable to meet your integrity assurance needs?

Bring Integrity to Your Environment with CimTrak

CimTrak is the industry's only genuine system integrity assurance platform. It combines all the capabilities required for "real" FIM, plus everything else discussed in this paper.

That includes:

- **CIS of DISA STIG benchmark** support and integration.
- **Real-time change monitoring and detection** across the entire IT environment.
- **Collection of forensic details** and evidence for every change.
- **Reconciliation and curation** between observed changes against authorized and approved changes.
- **Alerting** for unknown changes that require human intervention.
- **Comprehensive whitelist/allowlist and blacklist/deny list** to categorize changes and reduce noise by 95%.
- **Prevention, roll back, and remediation** of disallowed changes.
- **Automatic baseline updates** to include accepted changes to hashes and configurations.
- **Embedded Ticketing** or support ITSM integrations to assign and track authorized work orders and remediation if necessary.
- **Seamless integration with leading SIEMs**, helpdesk, incident, and ticketing systems.
- **Full encryption** of all communications, data, and audit logs.
- **24/7/365 compliance** enforcement, benchmarks, and reporting.

CimTrak also uses the **Trusted File Registry™** to identify all changes caused by vendor-verified patches and updates. This enables the tool to automatically categorize hundreds of thousands of changes as good, ensuring analysts remain free to focus on changes that pose a real danger.

To see what CimTrak can do for your organization, arrange a free demo today.

CIMTRAK

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others

CIMCOR

PROTECTING THE U.S.
From Software Supply Chain Attacks

Why technology regulation is the best route to reducing supply chain risk across the public and private sectors

Contents

Executive Summary

Software supply chain attacks are among the top threats facing the U.S. today. A string of high-profile attacks against prominent targets—including federal agencies, critical infrastructure providers, and economically significant private sector organizations—has exposed the lack of effective supply chain risk management (SCRM) practices currently in place.

Despite several initiatives and publications by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), little progress has been made. The President's recent Executive Order 14028 recognizes the danger of supply chain attacks, but its requirements don't run deep enough to provide an effective defense.

Key Takeaways From This Report:

- While EO 14028 and new publications from NIST and CISA are a positive start, the U.S. is nonetheless highly vulnerable to supply chain attacks.
- Consequences of a successful supply chain attack include loss or theft of sensitive government data, serious disruption to public services and critical infrastructure, and potentially trade, intelligence, and military disadvantages.
- Due to their prevalence and current low levels of SCRM and associated cybersecurity controls, technology vendors pose a significant risk.
- Currently, the emphasis sits heavily on buyers to vet their technology suppliers for their ability to resist cyber attacks. This is not a fair or realistic responsibility, as there are too many suppliers to vet and no agreed framework for the vetting process.
- There are currently no legal SCRM requirements or consequences for technology vendors.
- Regulators should consider a legal mandate for technology vendors to implement foundational cybersecurity controls. These controls should include:
  - Following an agreed SCRM framework
  - Focusing on baseline integrity
  - Establishing closed-loop change control
  - Adopting resiliency-focused security operations
- Requirements for technology vendors should be prescriptive, stating what a vendor must achieve ***and*** how to achieve it.

Introduction

In 2008, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI) to protect the U.S. against the economic and national security threat posed by cyberattacks. President Obama later ordered a review of federal efforts to protect U.S. information and critical infrastructure and the development of a plan to secure America's digital future. In 2009, President Obama accepted the resulting recommendations, publishing a list of 12 initiatives—including one to "Develop a multi-pronged approach for global supply chain risk management."

Several further attempts have been made to embed supply chain risk management (SCRM) in legislative and best practice cybersecurity frameworks. Notably, the National Institute of Standards and Technology (NIST) began work on

its first SCRM framework shortly after the CNCI document was released. This led to the publication of NIST SP 800-161 in 2015. SCRM was later added to the Cybersecurity Framework (CSF) in 2017 in recognition of the risk of supply chain attacks on critical infrastructure. In 2021, NIST released a further publication on SCRM best practices.

Further guidance and recommendations have been published on several occasions by the Cybersecurity and Infrastructure Security Agency (CISA) to help federal agencies understand and protect against supply chain threats. As of December 2021, NIST is in the process of updating SP 800-161, partially in response to the President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.

Things Aren't Improving

Despite attempts to regulate improvements to SCRM, the nation's resilience to supply chain threats remains poor. This has been highlighted by several recent and high-profile attacks, which have led to the compromise of an unknown (but very high) number of sensitive and confidential records from government agencies, critical infrastructure providers, and private sector organizations.

This should not be a surprise. In 2020, the General Accountability Office (GAO) reviewed 23 federal agencies' SCRM practices to determine the extent to which they had implemented foundational SCRM practices. The GAO published its findings in December 2020, finding that none of the agencies had fully implemented all of the SCRM practices, and more than half had not implemented any of the practices.

The report concluded that: "As a result of these weaknesses, these agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain causing disruption to mission operations, harm to individuals, or theft of intellectual property."

> *"Executive Order 14028 only goes so far due to its requirements focus on government agencies, not private industry. The same goes for NIST publications. This misplaced reliance on "trickle-down" cybersecurity requirements is underscored by the low-adoption rate of NIST SP 800-171 for defense contractors. It highlights the significant challenges of rolling out cybersecurity requirements to private industry through purchasing-specific regulations that are limited in scope, as compared to a Federal law that can have more uniform applicability that spans industry verticals. Requirements for SCRM have to be understood and adopted by every stakeholder within the supply chain for SCRM to work."*
>
> **— Tom Cornelius**
> **Senior Partner**
> **ComplianceForge**

What Damage Could Supply Chain Attacks Cause?

Further successful supply chain attacks against U.S. targets pose a significant threat. The country has political and economic adversaries that have a vested interest in disrupting U.S. infrastructure and stealing state and industry secrets. There is no doubt these adversaries are already searching for further targets for supply chain attacks and may well already have a foothold inside key supply chain targets, waiting for an opportunity to infiltrate high-value targets.

Some of the top risks associated with supply chain attacks include:

- Serious disruption to federal agencies, public services, or critical infrastructure.
- Loss, theft, or tampering of classified government data by criminals or nation states.
- Theft of personally identifiable information relating to U.S. citizens.
- Theft of data or digital assets that could allow rival nations to gain an advantage over the U.S. in trade, intelligence, or military action.

These consequences aren't limited to supply chain attacks targeting branches of the U.S. government or critical infrastructure providers. Advanced threat groups have frequently displayed a willingness to infiltrate other targets of interest in the private sector, including universities, pharmaceutical providers, hospitals, technology companies, and more. Common motives include espionage, sabotage, and—in the case of criminal groups—pure profit.

What are Software Supply Chain Attacks?

In a supply chain attack, a bad actor infiltrates a technology vendor's network and abuses its trusted relationship with its customers to gain access to one or more target networks.

An organization's technology supply chain can include hundreds of retailers, distributors, suppliers, and developers that play some role in creating, distributing, selling, and maintaining hardware, software, and IT services. The rationale for a supply chain attack is simple. Breaching one or more desired targets—for example, government departments or critical infrastructure providers—is harder than infiltrating a single weak link in the supply chain.

The successful compromise of a single technology vendor can enable a bad actor to compromise dozens of high-value targets, each of which would have been challenging to infiltrate directly.

Software Supply Chain Attack Vectors

The most common form of supply chain attack involves infiltrating an IT vendor's network and inserting malicious code into a legitimate software product before it is sent to the customer. Due to the trusted nature of its source, this compromised software is assumed by the customer to be legitimate and installed. This results in the customer's network being compromised.

There are four common ways that software supply chain attacks can occur:

Developer is a bad actor. This is the most obvious and hard-to-combat scenario. If a bad actor has direct access to the development process and environment, they will have many opportunities to inject malicious code. This situation could conceivably arise through blackmail or bribery, but more likely an advanced threat group would plant the bad actor by positioning them as a legitimate, highly-qualified applicant who makes their way through the hiring process.

Compromise of open source code. Many developers use open source code libraries—sections of pre-written code—as 'building blocks' to add common functionality into their own code. Unfortunately, it has become common practice for bad actors to inject malicious code into popular open source projects and distribute them via fake websites. Since open source code is routinely built into commercial software, this can lead to serious vulnerabilities in popular software products. Worse, customers typically don't know products contain open source code, so they are unable to act if it later arises that the code includes vulnerabilities.

Hijack of software updates. Software updates are essential to fix bugs, add new features, and resolve security weaknesses. Customers typically download software updates from a central server owned by the software vendor. By hijacking this infrastructure, bad actors can inject malicious code into legitimate software updates, which are trusted implicitly and installed by customers.

Undermining codesigning. Software vendors use codesigning to verify the source, authenticity, and integrity of software downloads and updates. Bad actors can subvert codesigning by self-signing certificates, abusing signing systems, or exploiting account access controls. This enables them to disguise malicious software as legitimate software or updates, often including expected legitimate functionality to avoid arousing suspicion.
implicitly and installed by customers.

The Consequences of a Software Supply Chain Attack

Bad actors can use a compromised technology vendor's privileged relationship with customers to access one or more target networks. Once inside, the actor can expand its presence and capabilities by moving through the network and installing additional malicious software. This can enable the actor to regain persistent access to the network even if the victim detects and closes the original entry point.

The ultimate consequences of a supply chain attack depend on the bad actor's motive, resources, and skill. Common motives include extortion, data theft, espionage, and sabotage. For private organizations, the cost of investigating, resolving, and recovering from supply chain attacks can be crippling.

However, the real consequences of supply chain attacks can be far more dangerous. High profile examples of these dangers include:

Lockheed Martin—in 2011, three U.S. military contractors (including Lockheed) were infiltrated using multi-factor authentication codes stolen from network security vendor RSA. Officially nothing was compromised, but these types of attacks pose a clear threat to national security.

U.S. Government et al.—in 2020, a supply chain attack by an alleged Russian state-sponsored group compromised at least 12 U.S. Federal Agencies, NATO, European Parliament, UK Government, and several global technology companies. The attack exploited software and credentials from Microsoft, VMware, and SolarWinds. It led to the theft of so much data that, if printed out, it might total the size of "several Washington Monuments." Commentators suggested the stolen data could increase the attacker's influence for years and could even inform hard attacks against targets like the CIA or NSA.

There are also fears that supply chain attacks could be employed against critical infrastructure providers. While not a supply chain attack, the Colonial Pipeline hack demonstrated the impact a cyber attack can have on critical infrastructure, prompting President Biden to sign Executive Order 14028.

How Did We Get Here?

Today's technology vendors and buyers are unprepared to cope with supply chain attacks. Even global giants Microsoft and VMware were unable to prevent infiltration of their infrastructure in last year's attack. This left customers vulnerable to attack by sophisticated actors working with privileged access.

Meanwhile, even high-end buyers like federal agencies are unprepared to tell whether a supplier can withstand cyber attacks. Fully vetting a product before procurement takes months, and an agency or organization can easily use dozens or even hundreds of technology products. A lack of time, resources, and standardized vetting processes means that, in practice, even organizations with highly sensitive functions and responsibilities are unprepared to assess their supply chain risk.

So, why is the standard of supply chain risk management so low in the technology industry? Principally, it comes down to a series of technical, legal, and economic challenges.

The attack on SolarWinds was an inflection point. For years there have been theories about sophisticated groups that could bring resources to bear over months or years to compromise a target. Now we know these groups exist, and they aren't just targeting government agencies.

"It's not that we couldn't have done better. We could have. But we didn't have any major weaknesses. Our security hygiene and visibility were good. Our tooling and vulnerability detections were good. But in the face of a patient, dedicated, skilled adversary, they weren't good enough."

— Tim Brown
VP Security Architecture and CISO
SolarWinds

Technical Cybersecurity Challenges

Outdated security strategies. The traditional, perimeter-centric approach to cybersecurity is outdated and not sufficient to protect against today's supply chain attacks. With distributed network architecture and an increasingly remote workforce, it is no longer reasonable to rely exclusively on barrier technologies like firewalls and Intrusion Detection/Prevention Solutions (IDS/IPS).

Over-reliance on Artificial Intelligence (AI). AI and machine learning (ML) are effective for identifying attacks that have been seen before. However, new software, exploits, and attack behaviors are invisible to technologies that rely on AI/ML. Attacks against high-profile U.S. organizations and their supply chains will likely include new elements, rendering AI/ML solutions ineffective.

Assuming organizations can prevent breaches. This is no longer true. No matter how mature an organization's security is, it will sometimes be breached. It must be able to detect, remove, and recover from these breaches quickly and efficiently with minimal exposure of sensitive assets or data.

Treating supply chain attacks as purely a development problem. Many supply chain attacks insert malicious code during the development process. However, the solution is not purely to secure development environments. Modern supply chain attacks are multi-stage operations that require an initial entry point, movement through the network, privilege escalation, and often injection of further malicious software. Preventing these attacks requires a ground-up cybersecurity approach that enables vendors to detect, address, and recover from intrusions before a bad actor can enact its mission.

Legal and Economic Challenges

Lack of legal consequences for vendors. An organization or federal agency can be investigated and fined for losing restricted information. However, there is usually no legal consequence for a technology vendor for failing to properly secure its infrastructure. It's down to buyers to select vendors they believe will take adequate security measures—however, as noted above, it's not realistic to expect buyers to complete the necessary due diligence for every technology vendor in their supply chain.

There is no legal standard for SCRM. Currently, technology vendors have no legal obligation to meet certain security standards to protect customers from supply chain attacks. Most vendors do have regulatory compliance requirements that influence cybersecurity investments and decisions. However, these are not sufficient to protect critical U.S. targets from the danger of supply chain attacks.

> *"When you buy a piece of software, it's compiled. We can't look at the source code to search for vulnerabilities, and even if we could, we don't have the resources to do that for every product we use. Federal agencies do their best with outdated approved software lists and intra-agency communication to avoid duplication of effort, but it's a slow and cumbersome process, and there are no guarantees."*
>
> **— Gerald Caron, CIO**
> **Assistant Inspector General for Information Technology, Department of Health & Human Services, Office of the Inspector General**

These legal issues create a further economic barrier. Even if a vendor wanted to take the initiative to improve SCRM, they are economically blocked. The cost of substantially improving SCRM capabilities will be significant, and—unless all vendors are legally obliged—would place a vendor at a competitive disadvantage in the marketplace. Even if a vendor was willing to absorb this, there's a final problem:

There is no agreed standard for SCRM improvements. This makes it hard for vendors to justify the expense of improving SCRM and equally tough for buyers to evaluate vendors' SCRM maturity. Most vendors will not invest significantly in SCRM until they know what legal obligations lie ahead.

Current Legal and Compliance Initiatives

There have been several attempts in the past by organizations like NIST to set SCRM requirements for technology vendors that sell to federal agencies. Up to now, these attempts have lacked the 'bite' needed to compel significant changes to the security posture and practices of technology vendors.

In 2021, two significant initiatives began the process of mandating a higher standard of SCRM:

Executive Order 14028. President Biden's EO is wide-ranging and sets new requirements for federal agencies and technology vendors that sell to them. The new regulations require:

- Federal agencies to move away from legacy infrastructure, adopt a Zero Trust cybersecurity strategy, and implement multi-factor authentication (MFA).
- Technology vendors who sell to the federal government to do more to secure their development environments, improve detection of vulnerabilities in their products, and publish a Software Bill of Materials (SBoM) that lists all open source software included in a product.

The EO also establishes the Cyber Safety Review Board, which will investigate major cybersecurity incidents and report on changes to best practices, regulations, or organizations' practices. Initially, the board will have no subpoena power, so cooperation by private organizations will be voluntary.

> *"An executive order can't tell private companies how to operate, it can only tell agencies who they can buy from. From early 2022, agencies will only be able to buy from technology vendors that meet certain standards, which is a positive start. In the meantime, NIST has launched the National Initiative for Improving Cybersecurity in the Supply Chain, which focuses on working with the private sector to establish SCRM best practices for technology providers."*
>
> **— Jon Boyens**
> **Deputy Chief of the Computer Security Division**
> **NIST**

NIST SP 800-161. NIST is currently revamping its cybersecurity SCRM publication, which provides guidance for enterprises on "how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risk in the supply chain."

Additions to the publication guide federal agencies on assessing supply chain risk and where to find best practices to support the implementation of the controls set out by EO 14028.

Limitations of Current Initiatives

While valuable, EO 14028 and the updated NIST SP 800-161 are insufficient to protect the U.S. from the dangers posed by sophisticated supply chain attacks against government agencies, critical infrastructure, and the private sector. This is for two principal reasons:

1. There is still no imperative for technology vendors to improve SCRM unless they sell to the federal government.
2. The legal requirements mandated by EO 14028 are not sufficient to protect the U.S. from the consequences of sophisticated supply chain threats.

The requirements prompt technology vendors to adhere to a minimum security standard if they sell to the federal government. This fails to protect the wider U.S. economy and is insufficient to protect federal agencies and critical infrastructure from supply chain threats like those we have already seen.

Further, both EO 14028 and NIST SP 800-161 continue to place the burden of ensuring a supplier meets a certain standard of SCRM on the buyer. This approach has been proven to be ineffective.

A 2019 analysis of defense contractors found that zero percent complied with all controls from NIST SP 800-171, and the average contractor was compliant with just 39 percent of controls. At that point, NIST SP 800-171 compliance had been a requirement for defense contractors for two years. This failure was the motive for implementing the Cybersecurity Maturity Model Certification (CMMC), requiring contractors to be audited for compliance before bidding on DoD contracts.

Without similar enforcement action, the standard of SCRM within U.S. supply chains is unlikely to meet the standards laid out by EO 14028 and NIST SP 800-171.

Addressing Supply Chain Risk in the U.S.

To adequately protect the U.S. economy, citizens, and critical infrastructure from supply chain attacks, regulators should consider a legal mandate that requires technology vendors to implement:

1. A higher standard of cybersecurity in the development environment and across the business.
2. A robust risk assessment of their own supply chains to protect against similar threats.

These requirements should go beyond those laid out in EO 14028 and NIST SP 800-161. The following section outlines proposed requirements to ensure technology vendors that play a crucial role in U.S. federal and critical infrastructure supply chains are resilient against modern supply chain attacks.

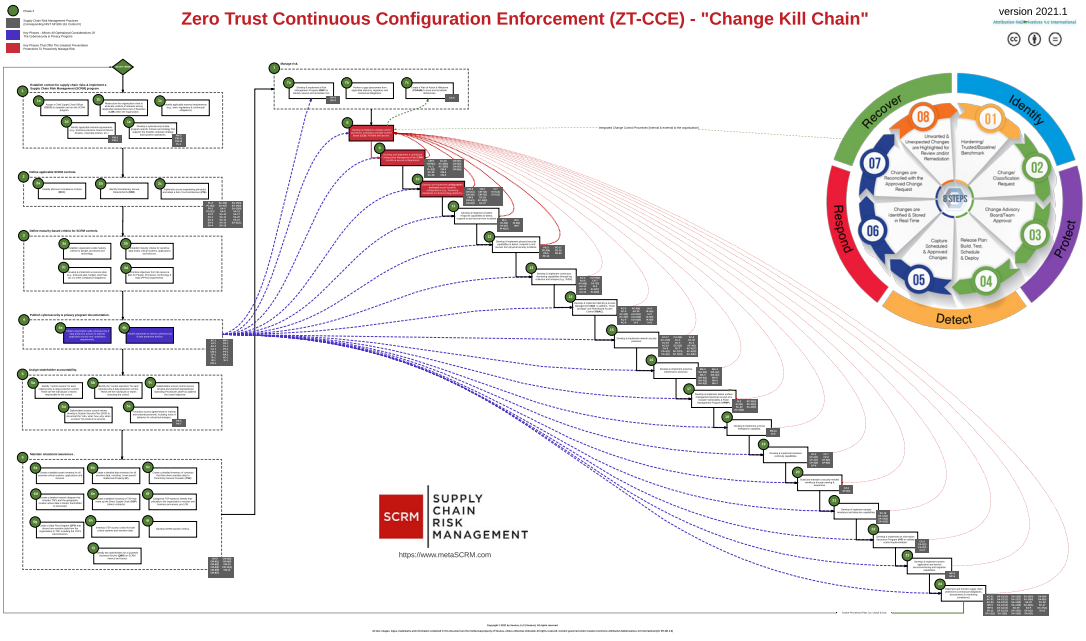
Proposed Requirements for Technology Vendors

Requirement #1: Follow an agreed framework for SCRM

One of the challenges facing technology buyers is the lack of an agreed framework for implementing SCRM. Technology vendors can implement their version of an SCRM practice, but it's difficult for buyers to determine its validity or effectiveness without a best practice to compare it to.

The specific requirements of such a framework are beyond the scope of this document and should be agreed by a combined effort of public and private entities as with other industry best practices. The framework should align with accepted industry standards such as NIST Cybersecurity Framework (CSF).

An example of such a framework is the Zero Trust Continuous Configuration Enforcement (ZT-CCE) model developed by ComplianceForge, Cimcor, Defcert, and BDO which sets out a phased model to prioritize SCRM activities. Click on the image to see the full version.

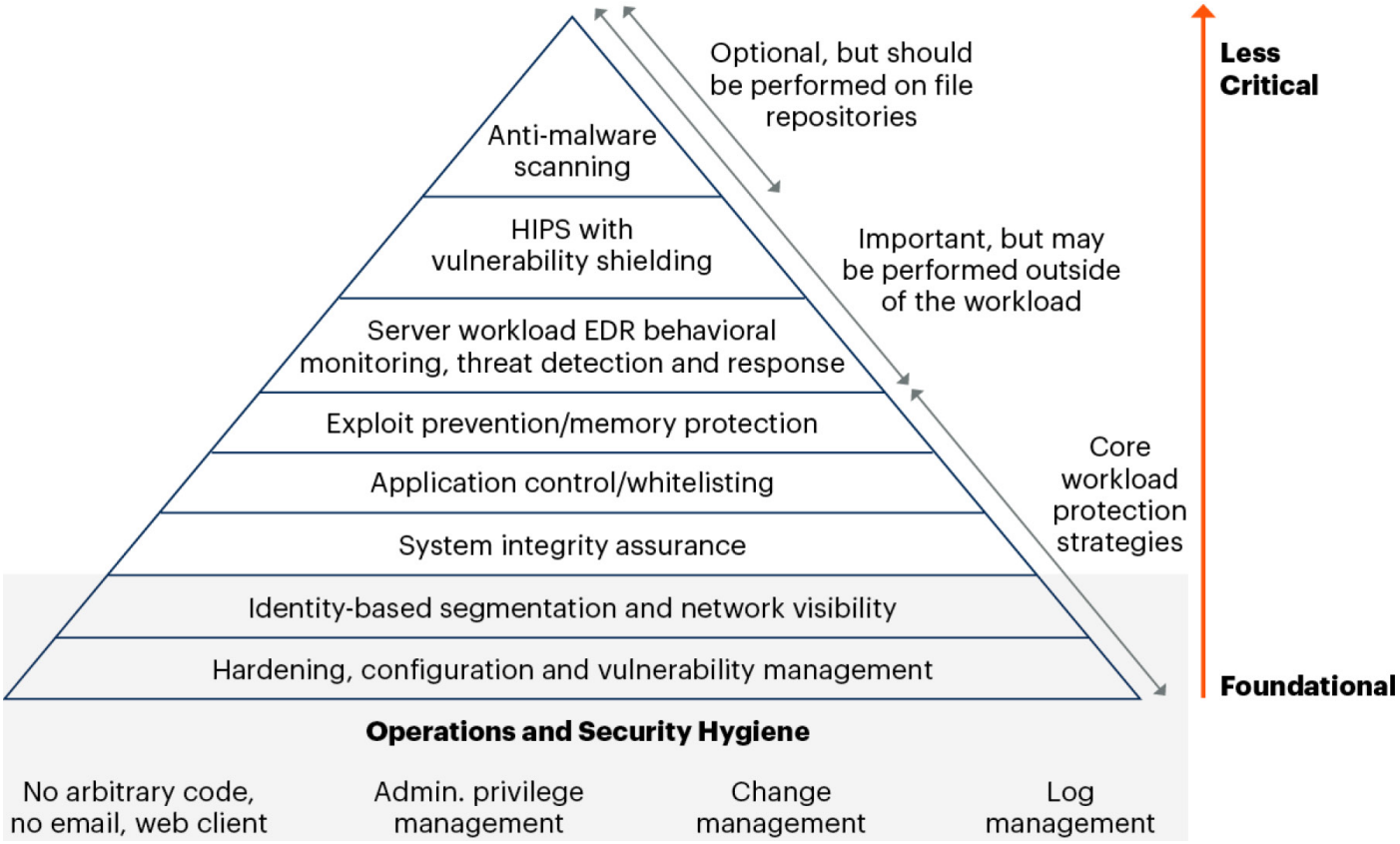


Requirement #2: Focus on Baseline Integrity

Most cybersecurity programs place too much emphasis on complex tools while neglecting the basics. Coupled with an outdated focus on perimeter defense, this leaves organizations continually reacting to incoming threats, and never able to establish control over their environments. Guidance issued by organizations like NIST and Gartner consistently highlights the importance of fundamental cybersecurity capabilities like configuration management, change management, and vulnerability management.

The diagram below has been issued repeatedly by Gartner and has been largely unchanged since 2018.

Risk-Based Hierarchy of Workload Protection Controls



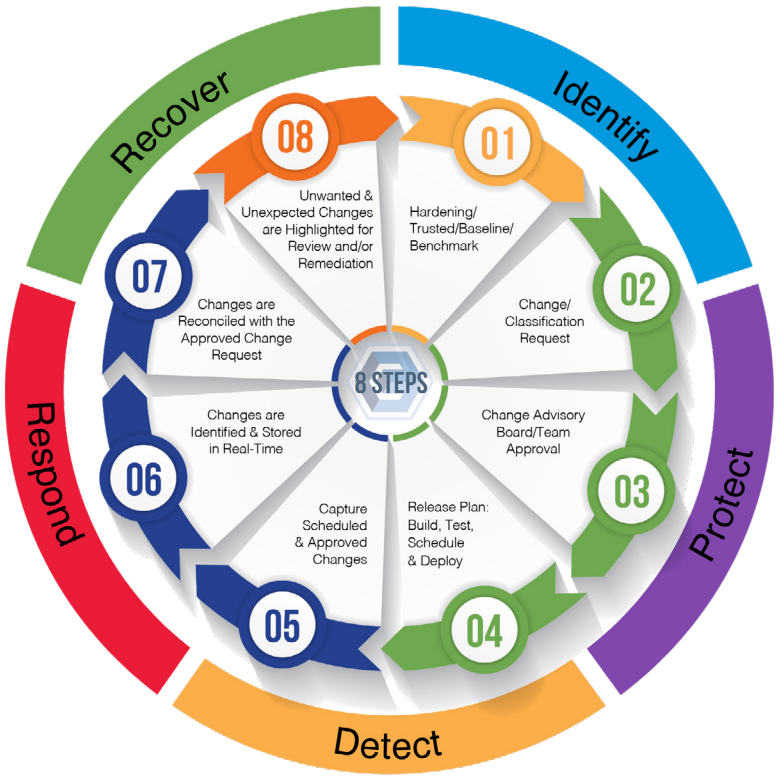
Source: Gartner 716192_C

The basic controls mentioned above are the foundation for effective cybersecurity and should be solidified before progressing to more complex controls. Having a solid basis in these disciplines makes an organization far more resilient to cyber attacks, as it is much more difficult for a bad actor to establish and grow a foothold inside a network that is securely configured and free from vulnerabilities.

Requirement #3: Establish Closed-Loop Change Control

Everything that happens in a network begins with a change. The ability to distinguish between good and bad changes determines an organization's ability to detect, prevent, and respond to attacks.

Closed-loop change control works from an established, trusted baseline of what is allowed within a network and then aims to prevent, limit, or reverse everything else. Whenever an unknown, unexpected change occurs, the organization manages it by exception, either adding it to the list of acceptable changes or preventing it altogether. The Integrity Assurance Loop demonstrates how this works:



With the right combination of technology and a trusted, authoritative baseline, this loop need only occur for unknown changes. I.e., changes that aren't yet known to be good or bad. Further, most of the loop can be automated, so human intervention is only required for a small percentage of changes.

This closed-loop process is fundamental to cybersecurity and IT operations. It is codified into best practice frameworks like NIST CSF and the IT Infrastructure Library (ITIL). Despite this, very few organizations have mature change control processes, leaving them highly vulnerable to cyber attacks.

Requirement #4: Adopt Resiliency-Focused Security Operations

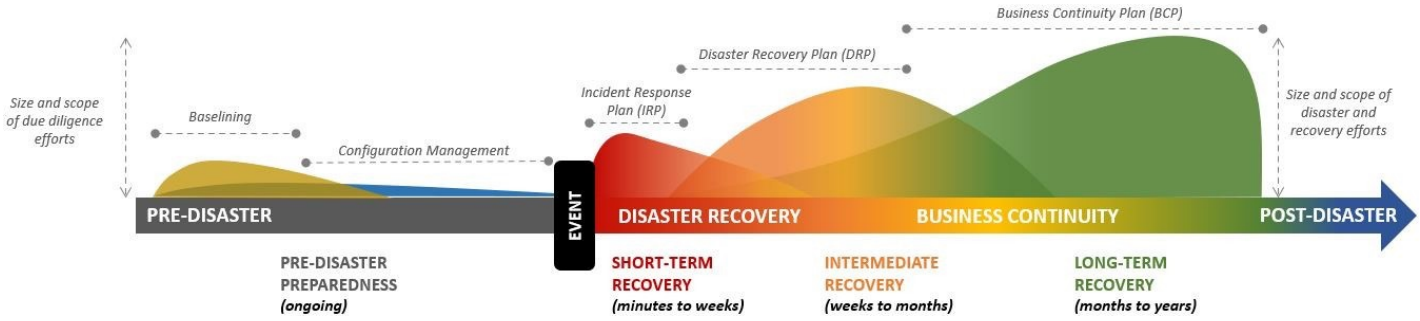
Today, most organizations model security operations using a perimeter defense and recovery model. Simply, they aim to fortify their perimeter with security technologies and then invest heavily in recovery when a breach occurs. As EO 14028 explains, this model is outdated for two reasons:

1. Network traffic and assets are increasingly positioned outside the corporate firewall, making perimeter defense impractical and ineffective.
2. Reactive-focused security operations are expensive and too slow to prevent the loss of sensitive data or disruption to critical assets or infrastructure.

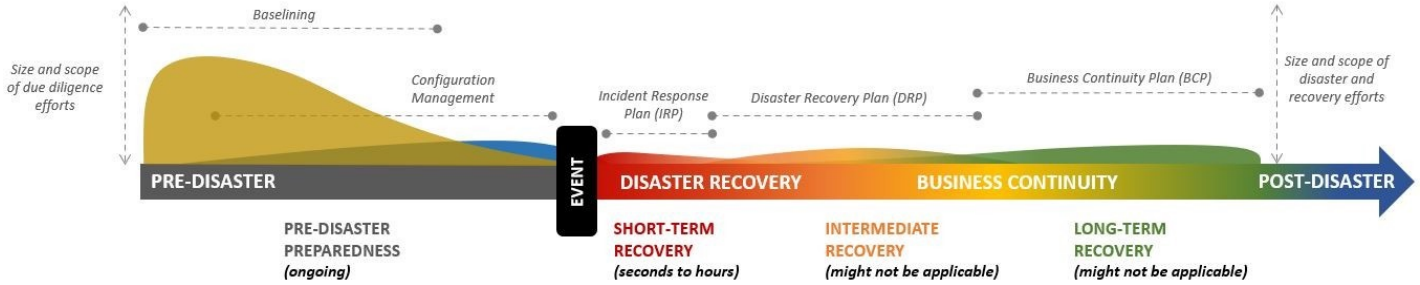
Instead, technology vendors (or any organization that needs robust cybersecurity) should implement resilient security operations that focus on prevention and automated recovery. Under this model, vendors would invest resources upfront in establishing a trusted baseline for their environments and enforcing security configuration of assets in line with a best practice such as DISA STIGs. Through this and the capability to automatically return to their trusted baseline, vendors would drastically reduce the time and cost of recovering from a network intrusion when (not if) it occurs.

The diagram below shows the difference between reactive- and resiliency-focused security operations.

REACTIVE-FOCUSED SECURITY OPERATIONS



RESILIENCY-FOCUSED SECURITY OPERATIONS



While resiliency-focused operations require a greater upfront investment of time and resources, they enable substantially improved response outcomes in the event of a breach. Recovery efforts are typically measured in minutes and hours rather than months and years, as with reactive-focused operations. This enables the organization to minimize the cost of response activities and the breach's negative impact, including on third parties and customers.

Requirements Should Be Prescriptive

A strong foundation in the above controls would help technology vendors protect against the dangers of supply chain attacks. However, regulations should go beyond telling vendors ***what*** to do by also telling them ***how*** to do it—i.e., they should be ***prescriptive*** rather than ***descriptive.***

Most cybersecurity frameworks tell organizations what to achieve but don't provide guidance on how to achieve it. This creates what Tony Sager, SVP and Chief Evangelist at the Center for Internet Security (CIS), calls a "special snowflake" approach that forces each organization to find its own solution.

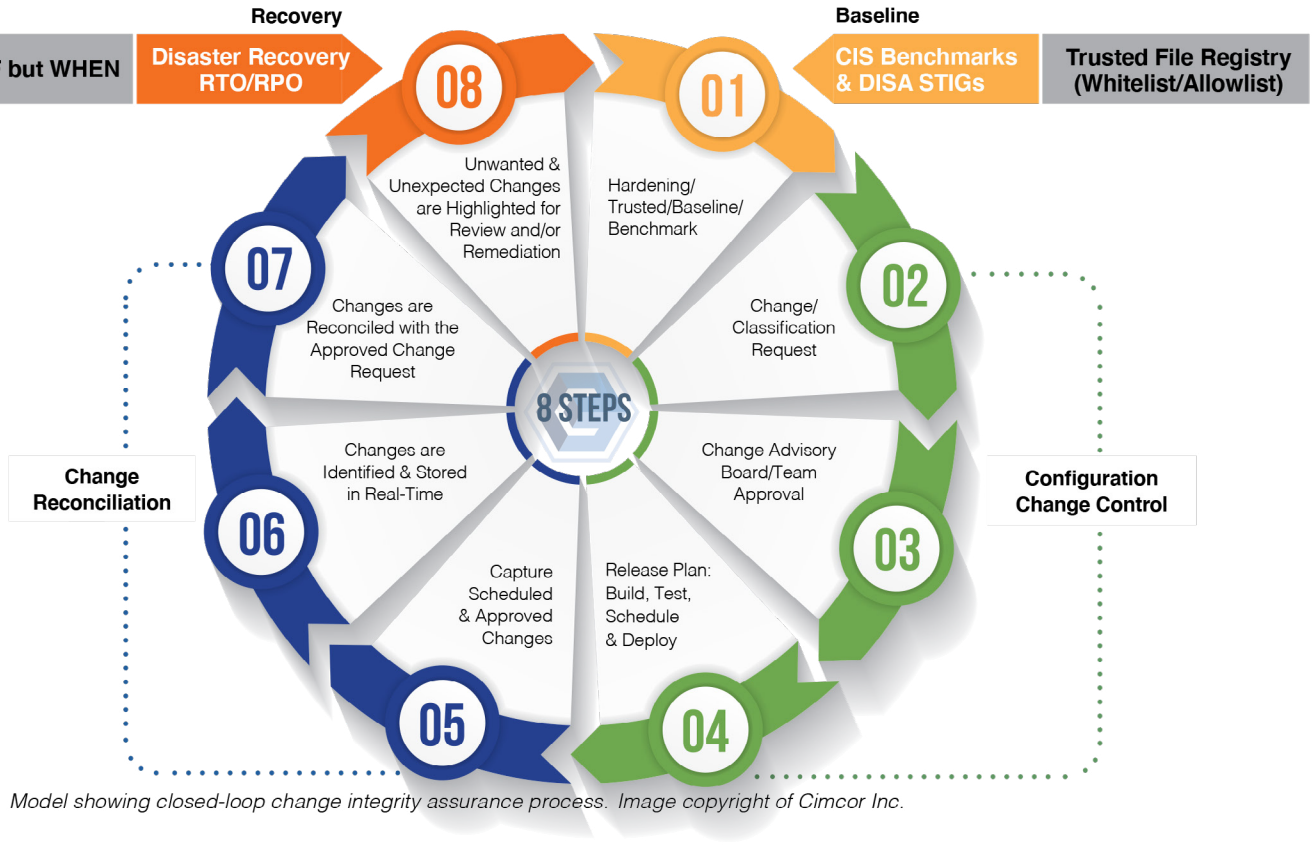
To protect the U.S. from supply chain attacks, requirements for technology vendors must be prescriptive, laying out a single best practice route to effective SCRM.

> *"Compliance requirements are what I call cosmic frameworks. They proclaim 'thou shalt achieve this,' but aren't prescriptive about how to do that. It creates an industry of tea leaf readers trying to interpret requirements, which is great for job security but very poor for business outcomes."*
>
> **— Tony Sagar**
> **SVP and Chief Evangelist**
> **The Center for Internet Security (CIS)**

Bringing Integrity into your Software Supply Chain Vulnerabilities with CimTrak

Integrity is the most overlooked component of DevOps (and security). Specific to software supply chain attacks, integrity is one of the leading indicators that there is a potential vulnerability. Given any of the four the most common supply chain attack vectors described earlier in this document, bad actors know that the vulnerability will eventually be discovered and patched. However, what is unknown without an integrity solution is the activities the bad actor may have executed during that window. Simply put…bad actors will leverage the initial vulnerability from the software supply chain compromise by making changes (add/modify/delete files and/or directories to compromise systems and devices for either financial, destructive, or continuous access/use).

CimTrak has the unique ability to detect in real-time changes caused by a DevOps vulnerability that might not have been linked or associated to a supply chain attack. This is accomplished by facilitating a closed-loop process for configuration management and change control which helps customers identify and contain breaches (MTTI & MTTC) in seconds as opposed to the current industry average of 207 and 73 respectively.



Model showing closed-loop change integrity assurance process. Image copyright of Cimcor Inc.

CimTrak is the industry's only genuine system integrity assurance platform that provides complete in-product functionality of all 8 steps. It provides all the required integrity capabilities that support and align with development, operations and security (DevSecOps).

This includes:

- CIS of DISA STIG benchmark support and integration.
- Real-time change monitoring and detection across the entire IT environment.
- Collection of forensic details and evidence for every change.
- Reconciliation and curation between observed changes against authorized and approved changes.
- Alerting for unknown changes that require human intervention.
- Comprehensive whitelist/allowlist and blacklist/deny list to categorize changes and reduce noise by 95%.
- Prevention, roll back, and remediation of disallowed changes.
- Automatic baseline updates to include accepted changes to hashes and configurations.
- Embedded Ticketing or support ITSM integrations to assign and track authorized work orders and remediation if necessary.
- Seamless integration with leading SIEMs, helpdesk, incident, and ticketing systems.
- Full encryption of all communications, data, and audit logs.
- 24/7/365 compliance enforcement, benchmarks, and reporting.

CimTrak also uses the Trusted File Registry™ to identify all changes caused by vendor-verified patches and updates. This enables CimTrak to automatically categorize hundreds of thousands of changes as good, ensuring analysts remain free to focus on changes that pose a real danger.

To see what CimTrak can do for your organization, arrange a free demo today.

Summary and Further Reading

Federal agencies, critical infrastructure providers, and other high-value organizations in the U.S. need to take more thorough precautions to vet their suppliers and minimize supply chain risk. However, the onus should not purely be on buyers.

Technology vendors are frequently the weak link that allows criminal and state-sponsored hacking groups to access sensitive data and systems, conduct espionage, and disrupt operations. To adequately protect against the dangers of supply chain attacks, technology vendors must have a legal obligation to uphold a minimum standard of SCRM.

Further Reading

Executive Order 14028, Improving the Nation's Cybersecurity

- EO 14028
- Timeline for EO 14028

National Institute for Standards and Technology (NIST) publications on SCRM

- Cyber SCRM Fact Sheet
- SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, Revision 1 (October 2021)

Cybersecurity and Infrastructure Security Agency (CISA) publications on SCRM

- Defending Against Software Supply Chain Attacks (April 2021)

Further Government Regulations and Initiatives

- Comprehensive National Cybersecurity Initiative
- Federal Acquisition Security Council Rule

Other

- Zero Trust Continuous Configuration Enforcement (ZT-CCE)

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

File additions, deletions, and modifications
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

CIMCOR

The Missing Components of Zero Trust

Why organizations must go beyond identity and access to realize the full Zero Trust value proposition

CONTENTS

WITH SPECIAL THANKS TO

Nicolas Chaillan, former Chief Software Officer, U.S. Air Force and Space Force, and CTO, Prevent Breach
Stefan Lesaru, IDSA Zero Trust Technical Working Group Lead, Big Data and Security Director, Atos
Kathleen Moriarty, Chief Technology Officer, Center for Internet Security

EXECUTIVE SUMMARY

Zero Trust promises to help organizations reduce cyber risk, in both on-prem and cloud-centric environments where perimeter defense tools are no longer effective. However, vague definitions, sparse practical guidance, and widespread misuse of the term by marketers have left many organizations with serious misconceptions about what Zero Trust really is.
This report will help define Zero Trust, examine significant gaps in existing guidance, and detail the most important concepts and capabilities required for an effective Zero Trust Architecture.

Key Takeaways From This Report:

- Zero Trust replaces outdated perimeter security with a strategy and architecture that pervades every aspect of an IT environment. It aims to replace assumed trust of users, devices, and services with verified proof that each subject is legitimate, authorized, and secure.
- Zero Trust works from the assumption that a network is already breached and aims to limit an intruder's ability to access resources, traverse the network, and act on malicious objectives.
- While President Biden's Executive Order and NIST guidance are an excellent introduction, they provide limited guidance on how to implement a Zero Trust Architecture and only briefly mention some of the critical capabilities required to realize the full value proposition.
- Under a Zero Trust Architecture, three types of proof are demanded when a resource is requested—user/service identity, device/architecture identity, and device/architecture health. Access to resources is never "inherited" from a previous authorization—the full process is repeated every time a resource is requested.
- Least privilege is a foundational principle. Once authorized, a user or service is granted the minimum access required to fulfill its function, and only for the shortest necessary duration.
- A Zero Trust Architecture enforces dynamic cybersecurity policies across four layers: Identity, Device/Workload, Access, and Transaction.
- Most discussions of Zero Trust focus on authentication and authorization. However, this is only one component. Other critical capabilities include system integrity, system hardening, configuration management, vulnerability management, and network monitoring. These capabilities are briefly mentioned in official guidance, but aren't described in detail and are frequently forgotten.
- Only by implementing a comprehensive Zero Trust Architecture can organizations realize the full value proposition. This includes reduced attacker dwell time, protection against unknown cyber threats, significantly reduced incident response effort and costs, and greater scalability.

INTRODUCTION

The traditional approach to cybersecurity is fundamentally wrong. While perimeter defense tools and Trusted Internet Gateways have done a reasonable job of protecting organizations from cyberattacks via the Internet, they fail in two critical ways:

1. **They cannot detect or prevent attacks that originate inside the corporate perimeter.** An attacker that successfully accesses a corporate network can often reside there indefinitely, traversing the network and expanding privileges before acting on their objectives.

2. **They are ineffective for protecting users and assets outside the corporate perimeter.** Today's distributed network architectures and work policies mean most organizations are faced with protecting a host of remote users, cloud services, edge devices, and more. For this purpose, traditional perimeter defense tools are ineffective.

Zero Trust is an alternative cybersecurity strategy that has evolved over the past decade. Rather than attempting to fortify the perimeter of a corporate network and then trusting that everything inside is legitimate, Zero Trust aims to eliminate the need for trust by continuously verifying the identity and integrity of all users, devices, applications, and infrastructure—regardless of their location.

A PRESIDENTIAL CALL TO ARMS

In May 2021, President Biden issued Executive Order (EO) 14028 on Improving the Nation's Cybersecurity in response to a spate of high-profile attacks targeting major technology vendors and U.S. Federal agencies. The Order focused on expanding several cybersecurity capabilities for government agencies—most notably, mandating a shift towards Zero Trust principles.

EO 14028 describes Zero Trust like this:

"The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment."

While the Order is only binding for U.S. government agencies, it has raised awareness of Zero Trust principles across a broader audience. However, a lack of prescriptive guidance within the Order and broad misuse of the term throughout the cybersecurity industry have left many organizations with a skewed understanding of Zero Trust and how to implement it.

WHAT IS ZERO TRUST?

The traditional approach of fortifying the network perimeter and implicitly trusting anything inside is dangerous. Even with outstanding security policies and controls, there is no way to prevent 100% of attackers from gaining access—and once inside, assumed trust allows attackers to move around the network and escalate privileges with relative ease. This leads to substantially worse outcomes—a dynamic threat environment.

ZERO TRUST DEFINITIONS

While Zero Trust hype has exploded in recent years, the concept isn't new. U.S. Federal agencies have been urged to adopt Zero Trust principles for over a decade by programs such as the Federal Information Security Modernization Act (FISMA), Federal Identity, Credential, and Access Management (FICAM), Trusted Internet Connections (TIC), and Continuous Diagnostics and Mitigation (CDM).

Despite this, Zero Trust is still poorly understood—partly because it's often vaguely defined. This is how some of the leading cybersecurity analysts and organizations define Zero Trust:

"[...] an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented."

— Forrester, The Definition of Modern Zero Trust

"[...] an approach where implicit trust is removed from all computing infrastructure. Instead, trust levels are explicitly and continuously calculated and adapted to allow just-in-time, just-enough access to enterprise resources."

— Gartner, New to Zero Trust? Start Here

"[…] Zero Trust promotes a micro-perimeter approach based on user access, data location, and an application hosting model."

— PwC

"[..] key element of the zero trust approach is microsegmenting networks, data, applications, workloads, and other resources into individual, manageable units to contain breaches and wrap security controls at the lowest level possible."

— Deloitte

> *"Traditionally, agencies (and enterprise networks in general) have focused on perimeter defense and authenticated subjects are given authorized access to a broad collection of resources once on the internal network. As a result, unauthorized lateral movement within the environment has been one of the biggest challenges for federal agencies."*
>
> **— NIST Special Publication on Zero Trust Architecture (NIST SP 800-207)**

Coming to any of these definitions cold would leave most audiences feeling uninformed about precisely what Zero Trust is—or what it might look like in practice. However, these definitions do cover some of the foundational components of Zero Trust, including:

- Zero Trust is a strategy, not a solution.
- Trust—and the privileges associated with it—is never assumed, but continuously verified.
- Users, devices, and workloads should always receive the least privileges needed to function—and only for the minimum necessary duration.
- Zero Trust principles should pervade all parts of an organization's IT infrastructure, including identity and access management, operations, endpoints, hosting environments, etc.

While these components are undoubtedly important, a true Zero Trust strategy is broader than the above definitions suggest. A good reference point for adopting and implementing Zero Trust can be found in NIST's 800-207 Zero Trust Architecture publication that outlines seven core tenets which is later described in this paper.

"[…} a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero Trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure."
— NIST SP 800-207, Zero Trust Architecture

ZERO TRUST PRINCIPLES

The term Zero Trust was coined by then-Forrester analyst, John Kindervag in 2009, who posited that trust was a vulnerability and security should follow a strategy of "Never trust, always verify."

Today, trust is assumed throughout a typical organization's infrastructure. Notably:

- After a single authentication, users, devices, services, and workloads are trusted to be legitimate and are granted access to a broad range of resources.
- The ubiquitous use of denylists in security tools inherently trusts that all activity is legitimate unless known to be malicious.

This is a problem. Breaches of the corporate perimeter are inevitable, and denylist-centric security tools can only detect a fraction of the threats faced by today's organizations. This is precisely why John Kindervag stated that trust is a vulnerability. When an organization implicitly trusts that a user, device, application, workload, or connection is legitimate unless proven otherwise, it opens itself up to a huge amount of risk—the approach will inevitably fail to detect a high percentage of malicious activity.

At its core, a Zero Trust strategy aims to improve on this approach by adhering to three principles:

1. Assume breach

Organizations should assume at all times that there is a malicious presence inside their environment and implement security controls to minimize the impact.

2. Verify, don't trust

Instead of assuming legitimacy, organizations should continuously verify all components within their IT infrastructure to

ensure they haven't been compromised. This includes:

- Reauthorizing users and devices every time they try to access a resource to prevent hijacked accounts, devices, and sessions from going unchecked.
- Continuously monitoring and enforcing the health and configuration of all enterprise assets—including devices, applications, services, endpoints, cloud instances, and more—to ensure they remain in a known and accepted state.
- Assuming by default that everything that is and happens within an IT environment is malicious—unless it has been expressly authorized.

Put simply, a Zero Trust strategy means moving to a 'deny-by-default' approach instead of the more trusting 'allow-by-default' approach used in most cybersecurity strategies.

3. Least privilege

Once verified, users, devices, and services should be granted the minimum possible access required to complete their function—and for the shortest possible period. This minimizes the potential impact of malicious activity.

THE 7 TENETS OF ZERO TRUST

As helpful as the above principles may be for understanding Zero Trust, they still provide little guidance on implementation. NIST SP 800-207 sheds more light on what Zero Trust looks like in practice by providing seven core tenets:

1. All data sources and computing services are considered resources. Users, devices, and services need access to these resources to complete their functions.

2. All communication is secured regardless of network location. Since organizations must assume they are breached, all digital communications must be secured to the same standard regardless of their origin.

> *"Allowlists are more secure and lower maintenance than denylists. Instead of assuming everything is legitimate unless proven otherwise, an allowlist blocks everything unless it meets an expected set of policies and measurements. This means threats are blocked even if they aren't known, and also, managing allowlists by exception requires far less human effort than constantly updating huge denylists of known threats."*
>
> **— Kathleen Moriarty, CTO Center for Internet Security**

3. Access to individual enterprise resources is granted on a per-session basis. Upon successful verification, users, devices, and services are granted the minimum necessary access—and only to a single resource. Accessing further resources requires additional verification.

4. Access to resources is determined by dynamic policy. Access policy considers the broadest possible range of factors, and policies are updated continuously to reflect new information. Factors can include:

- Client or service identity, credentials, and behaviors.
- Device health, configuration, software versions, network location, analytics, etc.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets. All devices connected to the organization's IT infrastructure should be continuously monitored to ensure they remain configured in a state that is known to be legitimate and secure.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. Access to resources is never 'inherited' from a previous step. Policies are enforced every time a user, device, or service requests access to a resource.

7. The enterprise collects as much information as possible on the current state of assets, network infrastructure, and communications and uses it to improve its security posture. Uses of this data include maintaining access policy, activity allowlists, etc.
Note: these tenets don't prescribe a specific solution-based approach to Zero Trust—this is intentional. There are many possible approaches to delivering a Zero Trust strategy. Each organization should develop a strategy and tool stack that matches its unique needs and existing infrastructure.

Why Implement Zero Trust?

The objectives of a Zero Trust strategy are simple:

- Minimize malicious access to resources
- Minimize attacker 'dwell time' within the environment
- Prevent unauthorized lateral movement throughout the environment
- Minimize attackers' ability to act on their objectives
- Minimize the impact of a malicious presence within the environment

DOES ZERO TRUST WORK?

Currently, few organizations have a mature Zero Trust strategy in place. However, some compelling early evidence demonstrates a correlation between Zero Trust implementation and a reduction in key metrics such as attacker dwell time and breach costs.

Kathleen Moriarty, CTO at the Center for Internet Security, highlights the relationship between Zero Trust tenets and the Lockheed Martin Cyber Kill Chain, noting:

"The evidence of the tenets of zero trust working is clear when you consider its deployment in concert with kill chain detection controls as evidenced by attacker dwell time patterns."
Source: Where Does Zero Trust Begin and Why is it Important?

> *"One of the biggest misconceptions is that Zero Trust is a tool or set of tools. It's not. Each organization must define its own concept based on an evaluation of the current network environment and any gaps that exist. They have to embrace the concept and culture and then move towards it. Zero Trust is a journey that may take several years to realize, and each organization's journey and final implementation will look different."*
>
> **— Stefan Lesaru**
> **IDSA Zero Trust Technical Working Group Lead**
> **Big Data and Security Director**
> **Atos**

Research by Mandiant highlights a significant reduction in attacker dwell time during the last decade, corresponding to the early adoption of Cyber Kill Chain and Zero Trust security principles.

The M-Trends 2021 report shows the global median dwell time has fallen from 229 days in 2013 to just 24 days in 2020. This trend is particularly noticeable in the U.S. regional figures, where dwell time figures began to reduce several years earlier than in other regions, and to a greater extent—reflecting the earlier adoption of Cyber Kill Chain and Zero Trust principles by U.S. organizations.

Similarly, the IBM 2021 Cost of a Data Breach report highlights a $1.76 million cost difference in breaches where mature Zero Trust was deployed compared to no Zero Trust. While there is no clear definition of what is considered mature, it can be assumed that the increased oversight and prevention of lateral movement and privilege escalation within Zero Trust environments is responsible for this reduction in breach impact.

WHAT IS TRUST AND WHY CAN'T WE ASSUME IT?

Trust in IT is the assumption that a user, device, application, or service (a.k.a. a "subject") is:

- Who or what it claims to be
- Allowed access to the resource it is requesting
- Configured and behaving in an expected way
- Free from compromise
- Allowed to take the actions it is currently taking

This is a significant list of assumptions. In a traditional network architecture, a subject is required to authenticate once—and then the above assumptions are held until the session is logged out. This is extremely dangerous, as it allows malicious actors to reside inside corporate networks for weeks or months while they gradually move laterally and expand their privileges.

Some of the dangers of assumed trust include:

- Even if a user is legitimate, their device may be compromised. This is particularly likely if the user is outside the corporate perimeter, is using their personal device (BYOD), or is a partner or customer that is not subject to the same security requirements as an internal user.
- A device may initially be secure but become compromised while connected to the network. If trust is assumed following a single authentication, there's no easy way to detect this.
- Perimeter defenses are beatable. Malicious actors can easily defeat a single authentication requirement—often using legitimate credentials. In traditional architectures, it's common for malicious actors to 'dwell' within networks for weeks or months before acting on their objectives.
- Today, many users connect from potentially hostile networks, including infected home networks and public WiFi. As a result, even legitimate users can pose a significant risk to the network.

Zero Trust reduces these risks by forcing subjects to prove their trustworthiness every time they attempt to access a resource. Under a Zero Trust Architecture, three types of proof are demanded every time a resource is requested:

1. **User identity** "who is this user, service, or application, and should it have access to this resource?"
2. **Device identity** "is the device or infrastructure this request originates from known and expected?"
3. **Device health** "is this device in the expected state and free from compromise?"

As described earlier, policies for establishing the legitimacy of these three proofs are dynamic and constantly updated. The result is an access and authorization architecture that looks like this:

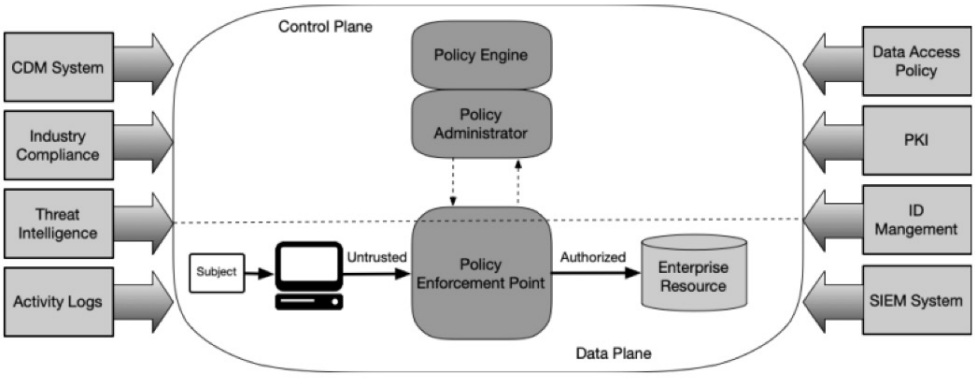


Figure 1: Abstract Zero Trust Logical Architecture

Source: Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators

Note that the policy engine is continuously fed with data from many sources, enabling it to assess user identity, device identity, and device health in real-time with a high degree of confidence.

Once proofs are accepted, the subject is allowed precisely the access needed to perform its function, for the minimum necessary period. If the subject needs access to further resources, the process repeats.

> *"If you don't enforce policies for user identity, device identity, and device health, it's not Zero Trust."*
>
> **— Nicolas Chaillan**
> **Former Chief Software Officer**
> **U.S. Air Force and Space Force**
> **CTO of Prevent Breach**

The term Zero Trust implies a total removal of trust from the environment. However, in practice, there is still a degree of trust—it's just not assumed automatically. A legitimate user who behaves normally and can prove their identity and device state is temporarily trusted to access a resource. If the user is compromised—either by an undetectable threat or a real-world situation—this could still backfire.

However, by substantially reducing the level of trust within an IT environment, organizations can similarly reduce the risk of malicious presence and behaviors.

WHAT'S MISSING FROM ZERO TRUST GUIDANCE?

For Zero Trust to be widely and successfully adopted, organizations must understand it. Several issues stand in the way of this, notably:

1. A lack of common and agreed terms, components, and meanings

We've already noted the relatively vague Zero Trust definitions provided by leading analysts and regulators. When combined with an overload of unhelpful and often contradictory marketing messages from cybersecurity vendors, this has created a general air of confusion.

Most concerningly, while NIST SP 800-207 does an excellent job of outlining the core tenets of Zero Trust, it doesn't explicitly list the underlying capabilities required to deliver Zero Trust in practice. There are some arguments in favor of this approach. However, it has left the floor open for some cybersecurity vendors to claim Zero Trust benefits for unrelated solutions, creating further confusion.

> *"There's a big misconception, probably caused by vendors misusing the term, that Zero Trust is just a marketing buzzword. Zero Trust is a crucial concept for organizations to adopt, and I'm concerned that its overuse and misuse in a marketing context could get in the way of its adoption."*
>
> **— Kathleen Moriarty, CTO**
> **Center for Internet Security**

2. A lack of individual vendors that can "deliver" Zero Trust

In the past, many cybersecurity "wins" have been achievable by implementing a single solution. For example, Multi-Factor Authentication (MFA) is a substantial improvement on traditional password authentication—and can be implemented with relative ease by purchasing a single solution.

Zero Trust does not fall into this category. NIST SP 800-207 goes so far as to state: *"[...] no one vendor offers a single solution that will provide zero trust. Furthermore, it might not be desirable to use a single-vendor solution to achieve zero trust and thereby risk vendor lock-in."*

While this isn't a "fault" with Zero Trust, it makes it more challenging, resource-intensive, and time-consuming for organizations to implement.

3. An over-focus on access and authorization

One of the top misconceptions about Zero Trust is that it's purely about access and authorization. NIST SP 800-207 may be partly to blame for this misconception, as it directly states:

"The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges [...] needed to perform the mission."

The publication goes on to highlight other components of Zero Trust—and it is evident from reviewing the prescribed tenets that there is more to Zero Trust. However, the heavy focus on access and authorization throughout the document may have influenced broader industry messaging that frequently leaves out vital capabilities.

BEYOND ACCESS AND AUTHORIZATION

A Zero Trust Architecture should eliminate assumed trust throughout an IT environment. This requires enforcing dynamic cybersecurity policies across four layers:

1. Identity
2. Device/Workload
3. Access
4. Transaction

Most discussion of Zero Trust covers the Identity and Access layers at length and the Device layer in passing. However, the Workload or Transaction layers are rarely mentioned. This is a problem—only by enforcing policies at all four layers can an organization achieve the full Zero Trust value proposition.

For every request or action within an IT environment, several queries must be answered with a high degree of confidence. These include:

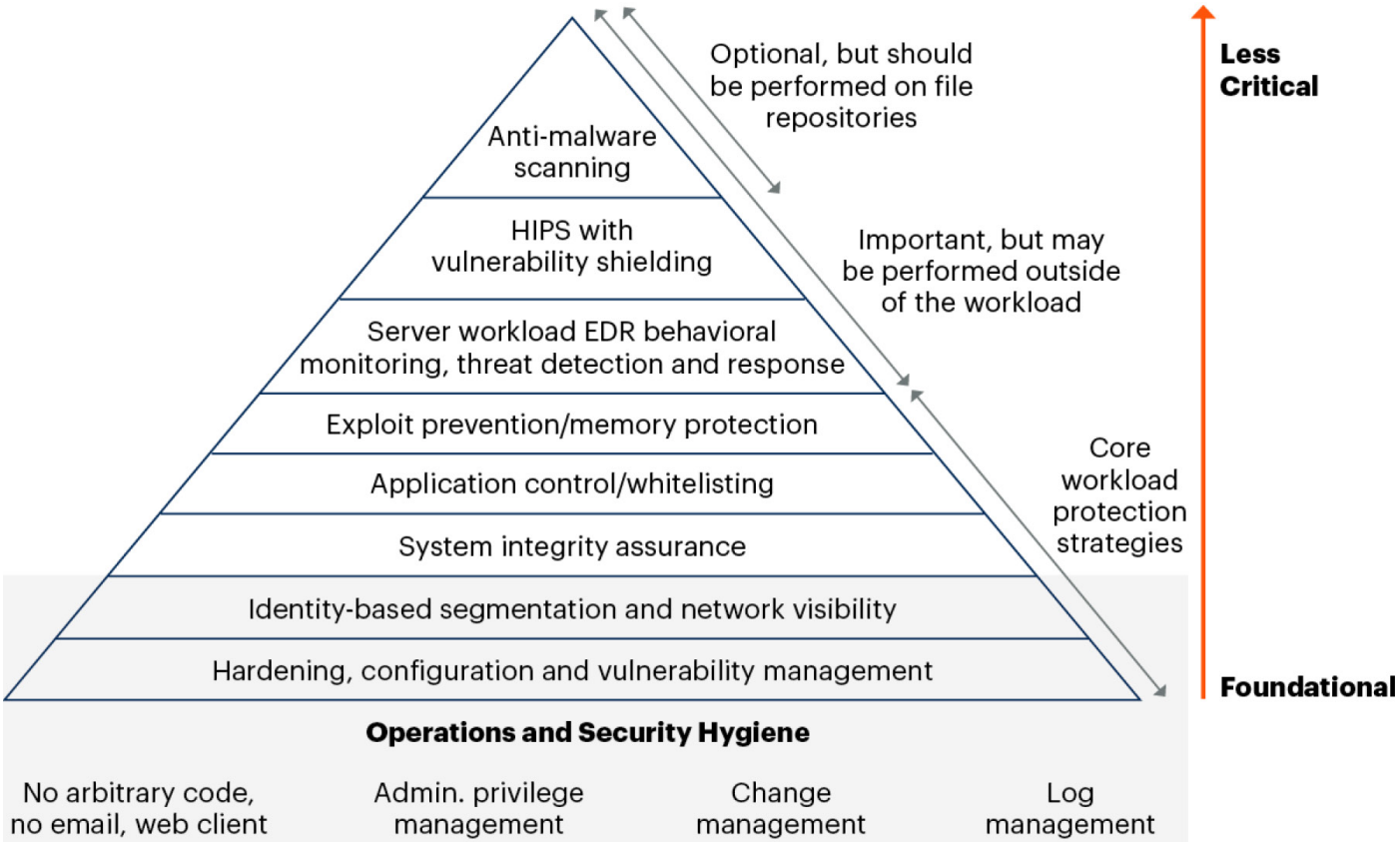
Query	Layer
Is the subject (user, application, service) expected, legitimate, and allowed to access a resource?	Identity
Are the subject's recent behaviors in-line with expectations and historic records?	Identity
What is the least privilege the subject can be granted that will allow it to fulfill its function?	Access
Is the device or infrastructure the request originates from in the expected, securely configured state AND free from compromise?	Device/Workload
Are device/infrastructure's behaviors in-line with expectations and historic records?	Device/Workload
Are the changes being made by the subject or device allowable within the environment?	Transaction

If the answer to any of these queries is negative OR there is insufficient confidence in the data, the request or action should be blocked. This is regardless of whether it's a request for access to a resource or an attempt to change a resource in an unauthorized manner following successful authentication.

ZERO TRUST IS ABOUT THE FUNDAMENTALS

For all the grandiose terminology and technical challenges it poses, Zero Trust is a logical extension of cybersecurity concepts that have been around for decades. The diagram below has been issued repeatedly by Gartner for years and has remained predominantly unchanged since 2018.

Risk-Based Hierarchy of Workload Protection Controls



Notice that “critical, cutting edge” tools—many of which rely on denylisting—are at the top of the pyramid and considered the least important factors in reducing cyber risk, while the basics are considered essential. These basics boil down to concepts that everybody in cybersecurity should learn, internalize, and operationalize within their first year:

- Least privilege access management
- System integrity
- System hardening and configuration management
- Vulnerability management
- Network visibility and monitoring
- Change and log management

In addition to being essential components of any cybersecurity strategy, these concepts lie at the heart of Zero Trust. The only way to eliminate reliance on assumed trust is to have complete oversight of an IT environment and control over what is allowed to happen within it.

To put this more simply, a true Zero Trust Architecture requires an organization to:

- Know everything that should be allowed to connect to corporate infrastructure—and disallow everything else.
- Know the expected, secure configuration state of all assets, devices, applications, cloud instances, infrastructure, etc.—and disallow access if these states aren't met.
- Monitor everything that happens to or within a corporate resource or environment—and block anything that isn't expressly allowed.
- Ensure all subjects and assets remain in the most secure state possible—i.e., by enforcing secure configuration and remediating vulnerabilities.

This requires a full-stack approach that combines widely understood Zero Trust access and authorization controls with more fundamental integrity assurance and cyber hygiene capabilities to address the four layers mentioned earlier.

	Device/Workload	Identity	Access	Transaction
User	Identify & verify user integrity	User authentication	Enforce least privilege to users	Manage transaction / consent security per session
Application	Identify & verify application integrity	DevOps authentication	Enforce least privilege to applications	Manage transaction / consent security per session
Infrastructure	Identify & verify device integrity	Admin authentication	Enforce least privilege to infrastructure	Manage transaction / consent security per session
NIST SP 800-207 Tenet(s)	#1, #5, #7	#1, #3	#4, #6, #7	#2

INTEGRITY: THE MISSING COMPONENT OF ZERO TRUST

To deliver Zero Trust principles at all four layers, organizations need three things:

1. Zero Trust-style access and authorization capabilities
2. A foundation in basic cyber hygiene
3. System integrity

Zero Trust access and authorization is well understood. Basic cyber hygiene—while sometimes challenging to implement—is simple to understand. But how does system integrity fit in?

> *"One of the biggest shifts needed for Zero Trust is an increased focus on the data layer. In traditional cybersecurity, data is assumed to be safe if the external layers are secure. This simply isn't true. Organizations need granular insight at the data level to maintain confidentiality and integrity."*
>
> **— Stefan Lesaru**
> **IDSA Zero Trust Technical Working Group Lead**
> **Big Data and Security Director**
> **Atos**

WHAT IS INTEGRITY?

Integrity is a core concept within cybersecurity—one pillar of the coveted CIA Triad.

- **Confidentiality:** only those who are authorized can access data.
- **Integrity:** data is in a trusted, accurate, and complete state and is only altered in expected ways.
- **Availability:** data (and the systems and applications that rely on it) remain accessible.

Note that data doesn't just mean documents and databases. Everything that allows an IT environment to function is stored in a file somewhere as data. This includes data stored in configuration files, system files, network devices, endpoints, directory services, cloud instances, etc. So long as data stays in the correct configuration and isn't tampered with, everything will function as intended.

Ensuring integrity within an IT environment means ensuring that no matter what service, device, or user accesses, stores, processes, transmits, or receives data, it remains accurate and complete.

This requires four capabilities:

1. An authoritative baseline of what data should look like.
2. A means of identifying and protecting data from unauthorized change.
3. A mechanism to roll back unauthorized changes not blocked at the source.
4. A way to verify that controls 1-3 are functioning correctly.

Without these capabilities being delivered on a continuous basis, integrity drift will become eminent, and the core foundation of a Zero Trust Architecture (ZTA) could be called into question.

The above closed-loop integrity assurance cycle demonstrates how this works in the real world. This loop may appear time-consuming. However, so long as an organization has a trusted, authoritative baseline—a record of what is allowed to be and happen within the environment—the loop only needs to occur for unknown changes. Further, with the right technology, most of the loop can be automated.

Note: For a more thorough explanation of system integrity assurance and its role in improving cybersecurity outcomes, read the Authoritative Guide to System Integrity Assurance.

INTEGRITY IN ZERO TRUST

Integrity is called out expressly in NIST SP 800-207 several times, including the following statements:

- "The enterprise monitors and measures the integrity and security posture of all owned and associated assets." (Zero Trust Tenet #5)
- "All connection requests should be authenticated and authorized, and all communications should be secured (i.e., provide confidentiality, integrity protection, and source authentication)."

The publication also highlights the value of Continuous Diagnostics and Mitigation (CDM), which aims to monitor the state of enterprise assets and enforce the integrity of asset configurations and software.

Put simply, organizations should monitor and protect the integrity of all assets, communications, and resources. However—as is commonly the case in cybersecurity documentation and frameworks—while organizations are advised to pursue integrity, there is little guidance on how to do so.

WHAT DOES INTEGRITY LOOK LIKE IN ZERO TRUST?

An expression commonly associated with Zero Trust is, "never trust, always verify." The implication is clear—to eliminate assumed trust from an IT environment, an organization must be able to verify the legitimacy (or not) of everything within the environment. Some of the most important subcomponents of integrity in this context include:

Visibility

An organization must be able to see and communicate with all subjects, assets, and resources within its IT environment. This is a foundational concept in both IT operations and cybersecurity—but many organizations aren't able to achieve it.

Change Monitoring and Management

Similarly, an organization must oversee everything that happens—i.e., changes—within the IT environment. This is essential to detect malicious activity.

Allowlist permissions

At every level, organizations should favor allowlists over denylists—not just for identity and access but for everything within the environment. This means:

- A device or asset should only be present in the environment if it is expressly permitted.
- Only permitted software and services should only be allowed to run.
- Only expected changes to data and files should occur—everything else is blocked.
- Permitted subjects are allowed access to defined resources—all other requests are denied.

Naturally, this approach requires a greater upfront investment of resources to establish comprehensive allowlists. However, from that point on, maintenance becomes much less resource-intensive as only unexpected subjects, resources, and changes must be reviewed. If an unexpected subject, resource, or change appears and is deemed acceptable, the relevant allowlist is updated accordingly.

An example of effective allowlists in action is Trusted Computing, which allows hardware manufacturers to control which software can run on a system by blocking unsigned software.

Configuration enforcement

Zero Trust tenet #5 requires organizations to "monitor and measure the integrity and security posture of all owned and associated assets." The organization must know what an asset's configuration should be and continuously monitor for discrepancies. Ideally, configuration should be enforced so any changes to secure baseline configurations are blocked or automatically rolled back.

The simplest way to achieve this is to ensure all enterprise assets are hardened, in line with an accepted standard—for example, DISA STIGS or CIS Benchmarks—and track or prevent deviations from these standards using a system integrity assurance tool.

> *"Zero Trust Architecture (ZTA) is more than just by tying logical access to a user's identity and should take into account the validated integrity of systems, applications and services across the supply chain."*
>
> **— Zero Trust Continuous Configuration Enforcement (ZT-CCE) by metaSCRM ComplianceForge LLC & CIMCOR, Defcert & BDO**

BENEFITS OF TRUE ZERO TRUST

To obtain the full Zero Trust value proposition, an organization must implement the entire strategy. This journey will take time, and there will be an upfront investment of resources required to design and implement a Zero Trust Architecture. However, the benefits cannot be understated.

Recall that Zero Trust has two primary purposes:

1. Minimize malicious access to resources.
2. Limit an attacker's ability to reside, traverse, and act within an IT environment.

If an organization has dynamic Zero Trust-style access and authorization, a complete understanding and overview of its IT environment and assets, and the ability to control all change within the environment, it becomes extremely difficult for an attacker to gain access to network resources or act on objectives.
The benefits include:

- Attacker dwell time/Mean Time To Containment (MTTC) reduced from weeks to seconds.
- Automated prevention of unknown malware, exploits, and malicious behaviors.
- Substantial reduction in manual effort required for system maintenance and incident response.
- Security and IT architecture that can scale rapidly within minimal change to human effort.

HOW CIMTRAK HELPS

CIMTRAK IS TENET 5: MONITORING & MEASUREMENT OF INTEGRITY

The core mission of CimTrak is to identify changes and categorize those changes as good or bad. This is done based on a zero-trust-based philosophy. If there is not a clear audit trail related to the change(s), it will be considered harmful. If a clear audit trail is found, the change can be classified as good. In CimTrak, this audit trail is based on digital signatures, authoritative baselines based on one-way hash algorithms, hash-based allow-list technology, and a workflow that has coupled the necessary detective controls to create a closed-loop environment for change. This means that when CimTrak indicates that

	Device/Workload	Identity	Access	Transaction
User	Identify & verify user integrity	User authentication	Enforce least privilege to users	Manage transaction / consent security per session
Application	Identify & verify application integrity	DevOps authentication	Enforce least privilege to applications	Manage transaction / consent security per session
Infrastructure	Identify & verify device integrity	Admin authentication	Enforce least privilege to infrastructure	Manage transaction / consent security per session
NIST SP 800-207 Tenet(s)	#1, #5, #7	#1, #3	#4, #6, #7	#2

The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

Tenet #5

a file is “good,” it is definitely good, and if it indicates that the file is “bad,” that means there is no “proof” that the file or the change is authorized. This is a very deterministic and transparent way of differentiating good changes from bad. When a “bad” or “unknown” change is identified, it is the result of two types of activities; 1) a trusted person circumvented a process for some unforeseen reason or issue, or 2) it’s a change (add/modification/deletion) with malicious intent.

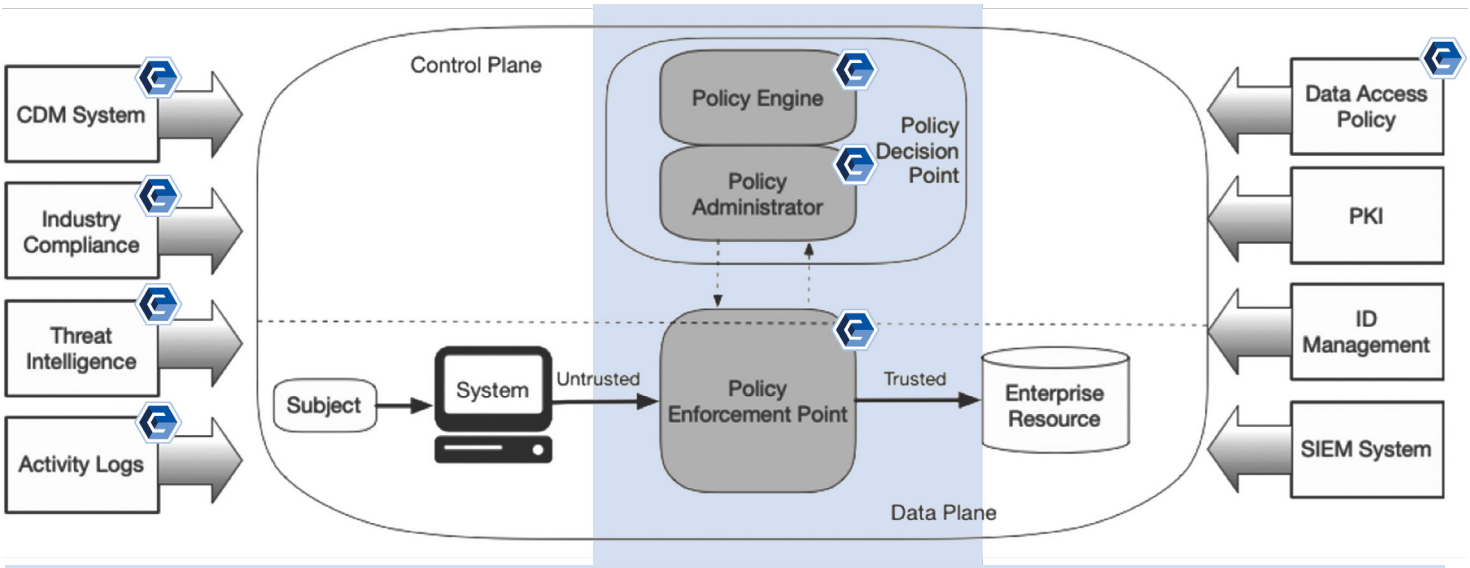
Due to the very nature that integrity is a horizontal thread through almost every best practice and framework, the same holds true for the Zero Trust Architecture (ZTA). Integrity functionality can also be seen in Tenets #1 and in #7.

All Security Issues Start with a Change or a Need for Change

It is invaluable to users to know, without a doubt, if a change is authorized or not. If a new piece of malware is created today and targeted to a system protected by CimTrak, it would detect it. Why? Because there is no proof, there is no audit trail for that malware that would be classified as unauthorized. The result is a clear, binary view of the disposition of changes. CimTrak identifies, prohibits, and remediates (roll-back) unauthorized modifications of files, directories, and configurations and uses the same methodology to manage users, groups, policies, active directories, database schemas, containers, cloud configurations, hypervisors, network devices, and more…

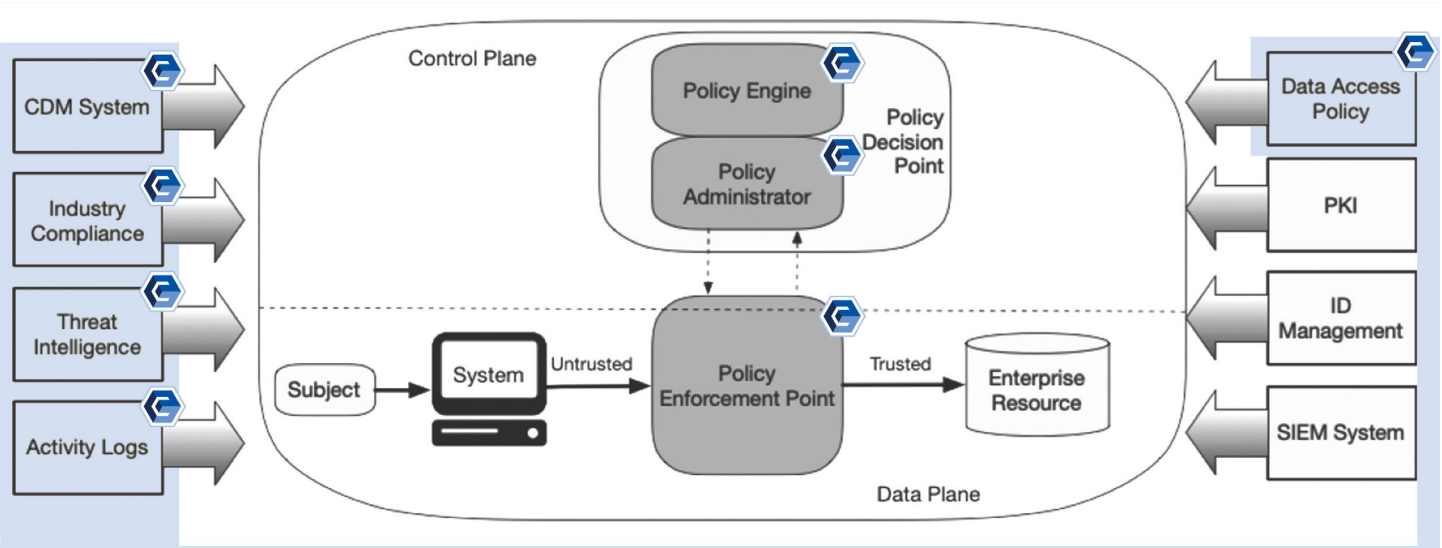
800-207 Zero Trust Architecture & CimTrak

There are three main components to the Zero Trust Architecture: Policy Engine, Policy Administrator, and Policy Enforcement Point. CimTrak supports these architectural components as it pertains to the core objectives of Tenet #5 relative to the device/workload layer.



- ✓ **Policy Engine** CimTrak is responsible for the decision to grant access to a workload resource that could add/modify/delete system files, directories, configurations, users, groups, policies, active directory, database schema, cloud configuration, hypervisors, network devices, and more…
- ✓ **Policy Administrator** CimTrak provides a workflow for change control, change prevention, and roll-back capability to ensure system integrity assurance.
- ✓ **Policy Enforcement Point** CimTrak is ultimately responsible for enabling and monitoring the integrity of an enterprise resource in real-time.

In addition to the core components in an enterprise implementing a ZTA, several data sources provide input and policy rules used by the policy engine when making access decisions.



CimTrak provides functionality that supports **5 of the 8 supplementary data sources.**

✓ **CDM System** CimTrak was the 1st integrity management product to receive Continuous Diagnostics & Mitigation (CDM) approval.

✓ **Industry Compliance** CimTrak provides the necessary evidence for 800-53, PCI, CMMC, HITRUST, SWIFT, HIPAA, and dozens of other compliance mandates.

✓ **Threat Intelligence** CimTrak can digest STIX & TAXII feeds to analyze and evaluate real-time security decisions and vulnerability risks.

✓ **Activity Logs** CimTrak provides in real-time a comprehensive view of all change activities with an ability to restore unwanted or unexpected changes back to a known and trusted state of operation.

✓ **Data Access Policy** CimTrak provides granular detail of who made changes and what process/approval was linked to that authorized change.

SUMMARY

Zero Trust is an end-to-end cybersecurity strategy and capability that touches every part of an organization's IT environment. To realize the full value proposition, organizations must understand that Zero Trust goes beyond the widely-publicized access and authorization components to include a range of fundamental capabilities, including:

- System integrity
- System hardening and configuration management
- Vulnerability management
- Network visibility and monitoring

Zero Trust is not a perfect solution to cybersecurity. Cyber risk is unavoidable, and organizations must adapt as new threats arise. However, a true Zero Trust Architecture that incorporates all necessary capabilities is a huge improvement over the denylist-oriented perimeter defense strategies that have dominated cybersecurity for decades.

FURTHER READING

National Institute for Standards and Technology (NIST) publications on Zero Trust

NIST SP 800-207: Zero Trust Architecture
Planning for a Zero Trust Architecture: A Starting Guide for Administrators

Executive Order 14028, Improving the Nation's Cybersecurity

EO 14028

Cybersecurity and Infrastructure Security Agency (CISA)

Zero Trust Maturity Model

U.S. Department of Defense (DoD)

Zero Trust Reference Architecture

Center for Internet Security

Where Does Zero Trust Begin and Why is it Important?
Prioritizing a Zero Trust Journey Using CIS Controls v8

Other

Zero Trust Continuous Configuration Enforcement (ZT-CCE)

SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, SUSE, Ubuntu, others
SUN SOLARIS: x86, SPARC
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server, MySQL
PARAMETERS MONITORED: Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, others

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.


F1
FIX CAR ERROR

Zero Trust Continuous Configuration Enforcement (ZT-CCE)

Change Kill Chain: A Phase-Based Model To Prioritize Supply Chain Risk Management (SCRM) Activities

Version 2022.1

Table of Contents

EXECUTIVE SUMMARY

The premise of the Zero Trust Continuous Configuration Enforcement (**ZT-CCE**) model was to create a proof of concept for an efficient way to plan out a roadmap to successfully implement robust Zero Trust and Supply Chain Risk Management (**ZT/SCRM**) cybersecurity and privacy practices that focus on prevention and automated remediation. The ZT-CCE is essentially a "Change Kill Chain" for how this model highlights the nature of preventative security controls as an efficient way to protect an organization from the expense and operational disruptions associated with incident response and business continuity activities. The result is a viable approach for organizations to use in order to create a prioritized project plan for ZT/SCRM-focused secure practices.

The concept of a "kill chain" adopts the premise that it is easier to stop and prevent further damage if malicious activities are discovered earlier, rather than later. The intention of using the Change Kill Chain is:

(1) By applying a prioritized, phased approach towards ZT/SCRM-related activities, it is possible to avoid rework and cascading failures by addressing dependencies earlier in the process; and

(2) Focusing resources and efforts on preventative controls, rather than detective controls. Prevention, tied with automated, reactive technologies can minimize operational disruptions from either hostile or accidental incidents.

The **Change Kill Chain** breaks the concept of ZT/SCRM down into 24 major steps, which can then be translated into a project plan. This project was approached from the question of, *"If a consultant was hired to build a ZT/SCRM program, what would the plan be to start from nothing to get a company to where it has operational ZT/SCRM capabilities?"* While the Change Kill Chain maps controls from NIST SP 800-161 to the steps in the model, it is important to emphasize that the prioritization and "bucketing" of controls into phases is a subjective endeavor and not everyone may agree with this approach. If you choose to use the Change Kill Chain, you will invariably need to modify the approach to fit your organization's unique business practices and specific needs.

The Change Kill Chain leverages the principles of the Integrated Controls Management (**ICM**) model.[1] The premise of ICM is that controls are central to cybersecurity and privacy operations, as well as the overall business rhythm of an organization. The ICM is supported by the Security & Privacy Risk Management Model (**SP-RMM**)[2] that describes the central nature of controls, where beyond just policies and standards, but procedures, metrics, threats and risks map to controls, as well.

"Zero Trust Architecture (ZTA) is more than just by tying logical access to a user's identity and should take into account the validated integrity of systems, applications and services across the supply chain."

Special thanks goes to the following contributors, since this document would not exist without their applied expertise:

Tom Cornelius
Senior Partner
ComplianceForge

Mark Allers
VP, Business Development
Cimcor

Ryan Bonner
Founder & CEO
Defcert

Tim Trickett
CTO, Public Sector
BDO

[1] *ComplianceForge's Integrated Controls Management (**ICM**) model - https://graphics.complianceforge.com/icm/ICM-PCDA.pdf*

[2] *SCF's Security & Privacy Risk Management Model (**SP-RMM**) - https://www.securecontrolsframework.com/sp-rmm*

RESILIENT VS. REACTIVE OPERATIONAL MINDSET

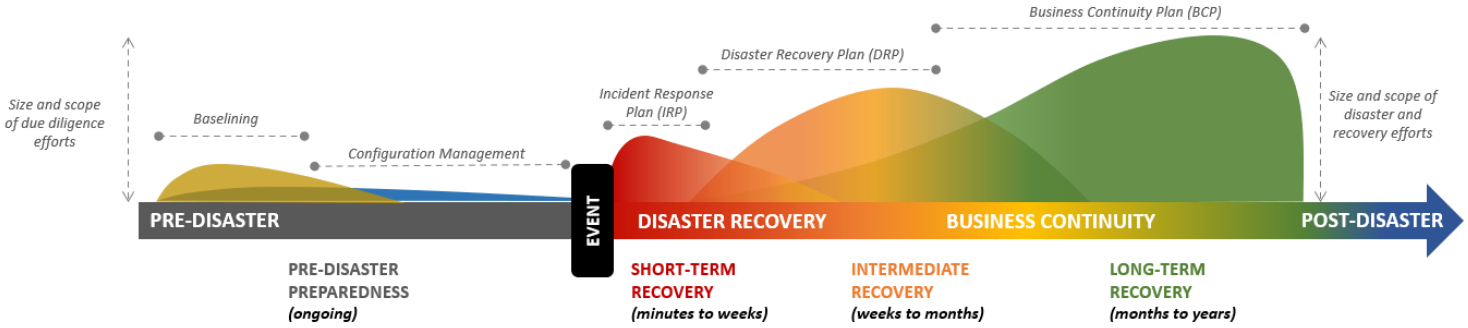
National Institute of Standards and Technology (**NIST**) Special Publication 800-160 focuses on "cyber resiliency engineering" and is the authoritative source for secure engineering principles within the realm of cybersecurity and data protection.[3] A common definition of *resilience* is "*the capacity to quickly recover from difficulties*." Resilience is a measure of an organization's elasticity – being able to spring back into a pre-determined operational state following an incident. Organizations should strive to be resilient to IT and cybersecurity-related incidents both internally and across the supply chain.

Traditional incident response and recovery operations are not designed with resilience in mind. Recovery is absolutely possible and Service Level Agreement (**SLAs**) help establish acceptable data loss parameters, maximum outages, etc. However, this is more of a way to bracket risk management decisions and while is an efficient manner to justify budgets for Continuity of Operations (**COOP**)-related technologies and staffing, it is not sustainable. While reactive operations are often viewed as heroic endeavors that "saved the organization from doom," it does not mean that reactive model is the best methodology or least expensive path to follow. Resiliency is.

REACTIVE-FOCUSED SECURITY OPERATIONS

If you study the graphic below, there are a few key takeaways:

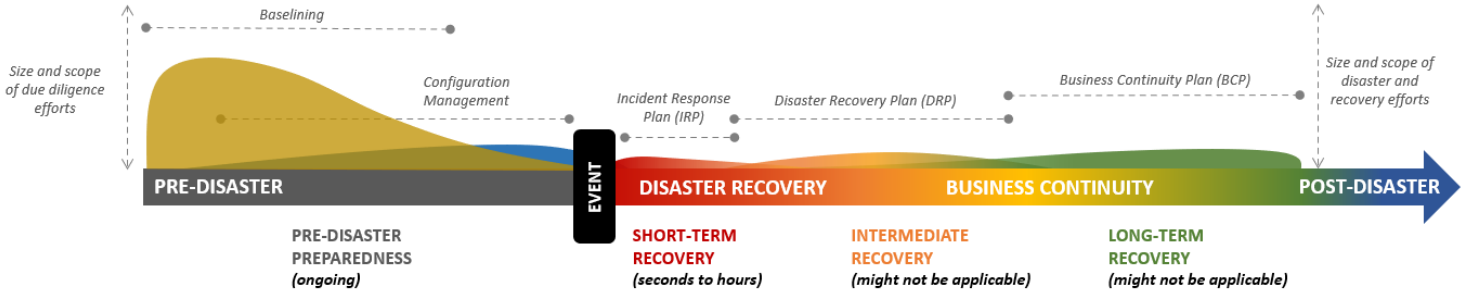
- Effort is on the "right side" of an incident or event – it is reactive. Baselining and configuration management on the "left side" of an incident or event is often compliance-focused and are not directly tied to response/recovery operations.
- The traditional, reactive model has minimal focus on baselining and configuration management.
- When an incident occurs, there are structured plans to respond that span from minutes to years in duration:
  - Incident Response Plan (**IRP**)
  - Disaster Recovery Plan (**DRP**)
  - Business Continuity Plan (**BCP**)
- Expense is primarily associated with event detection, response, remediation and recovery operations.



RESILIENCY-FOCUSED SECURITY OPERATIONS

If you study the graphic below, there are a few key takeaways:

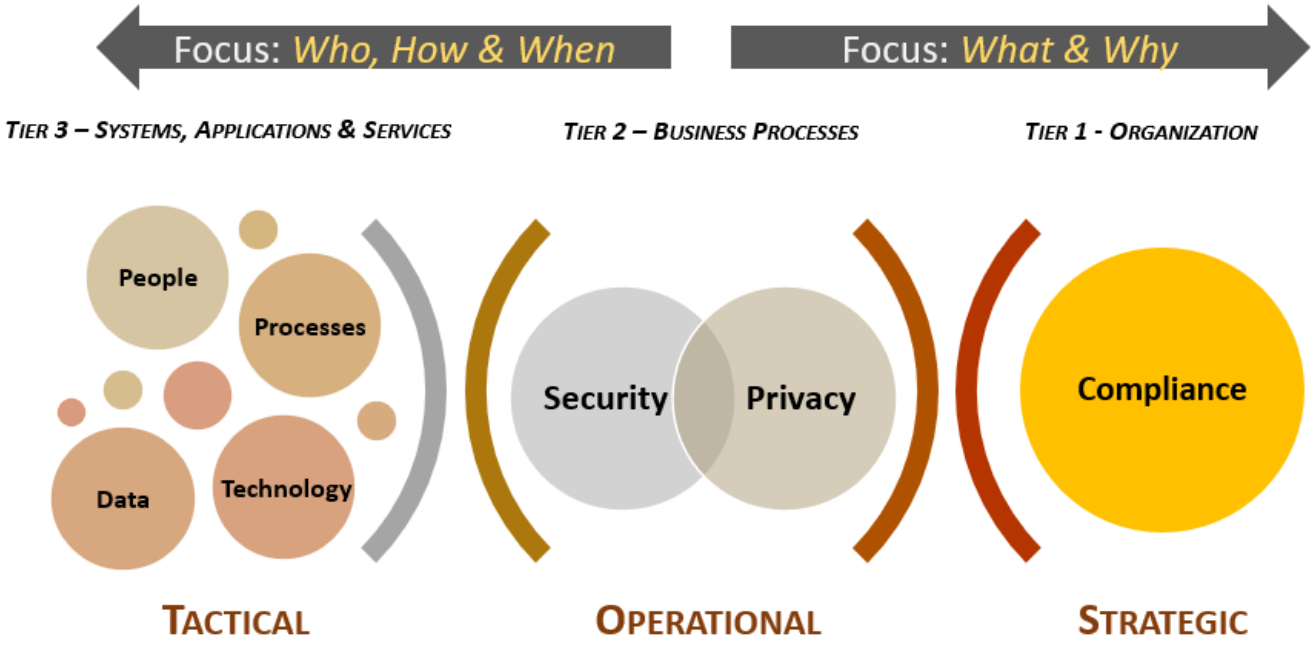
- Effort is on the "left side" of an incident or event is prevention-focused. A decrease in effort on the "left side", will likely result in a decreased operational impact on the "right side" of the event occurrence.
- There is significant effort placed on baselining and automating configuration management operations.
- When an incident occurs, the automated remediation actions minimize impact and the necessity to activate IRPs, DRPs and BCPs.
- Expense is primarily associated with tightly-controlled configuration management practices.



[3] *NIST SP 800-160 "Developing Cyber Resilient Systems: A Systems Security Engineering Approach" - https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Understanding Necessary Building Blocks For Implementing Zero Trust & SCRM

If truth be told, controls exist to protect an organization's data. For instance, requirements for asset management do not *primarily* exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but data residing on those devices cannot. This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity and privacy program that addresses Zero Trust and Supply Chain Risk Management (**ZT/SCRM**) concepts. Zero Trust Architecture (**ZTA**) is more than just by tying logical access to a user's identity and should take into account the validated integrity of systems, applications and services ***across the supply chain***.

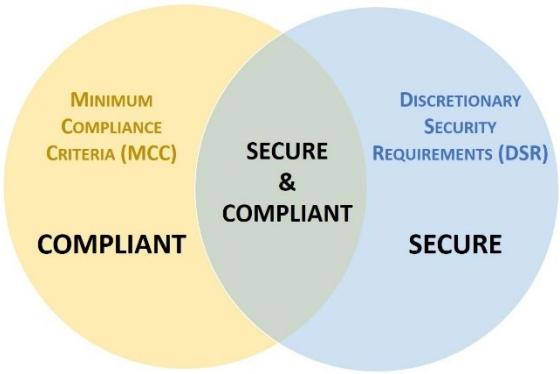


Zero Trust & SCRM Goals - Secure, Compliant or Both?

For ZT/SCRM, controls must be designed to proactively address the (1) strategic, (2) operational and (3) tactical nature of operating an organization's cybersecurity and privacy program. ZT/SCRM must be designed to address both internal controls that are directly under the influence of the organization, as well as third-party operated controls that directory or indirectly influence ZT/SCRM for the organization. Organizations need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions with affected stakeholders.

To assist in this process, an organization's applicable controls should be categorized according to "must have" vs "nice to have" requirements:

- Minimum Compliance Criteria (**MCC**) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (**DSR**) are tied to the organization's risk appetite since DSR are "above and beyond" MCC, where the organization self-identifies additional cybersecurity and data protection (privacy) controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



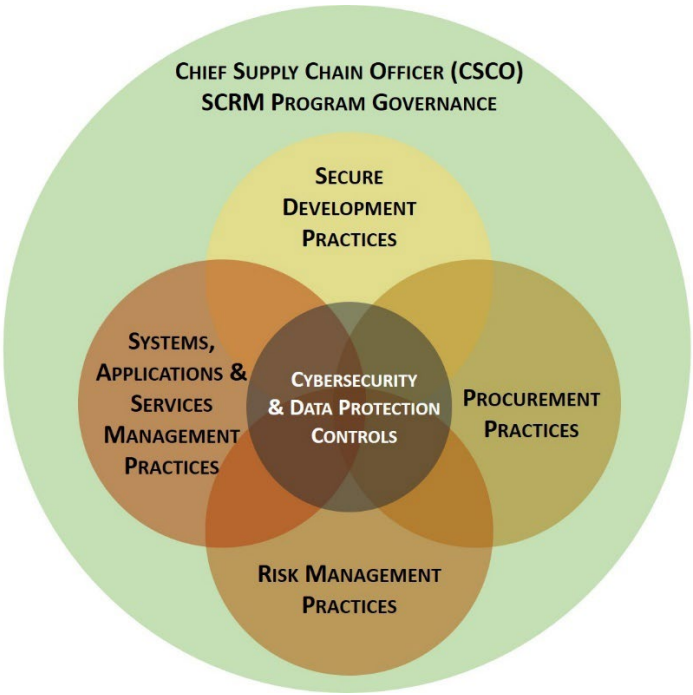
Secure and compliant operations exist when both MCC and DSR are implemented and properly governed:

- MCC are primarily externally-influenced, based on industry, government, state and local regulations. MCC should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCC establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

When you start looking at how you "do zero trust & supply chain risk management" in a practical manner, it is more than just a control set. In fact, a ZT/SCRM program needs to also have authority over several key business functions that impact supply chain security:

- Secure Development Practices
- Procurement Practices
- Risk Management Practices
- Systems, Applications & Services Management Practices

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, is the "gold standard" for SCRM-related concepts and this guide heavily relies on that body of work.[4]



Operational Leadership

For ZT/SCRM to be successful, operational leadership is essential. This "active participation" by a Chief Supply Chain Officer (**CSCO**) and his/her staff, ensures that processes are effectively carried out on a day-to-day basis. In many industries, the CSCO is often designated as the Chief Operations Officer (**COO**). Regardless of the official title, the CSCO is responsible for internal and external supply chain processes. This scope ranges beyond simple logistics and manufacturing activities to include:

- Innovation and development.
- Onboarding new technologies/services.
- Business operations (e.g., manufacturing, service delivery, etc.).
- Business Continuity & Disaster Recovery (**BCDR**).
- Third-party relationship onboarding and management (e.g., vendors, service providers, contractors, etc.).
- Decommissioning technologies, services and third-party relationships.

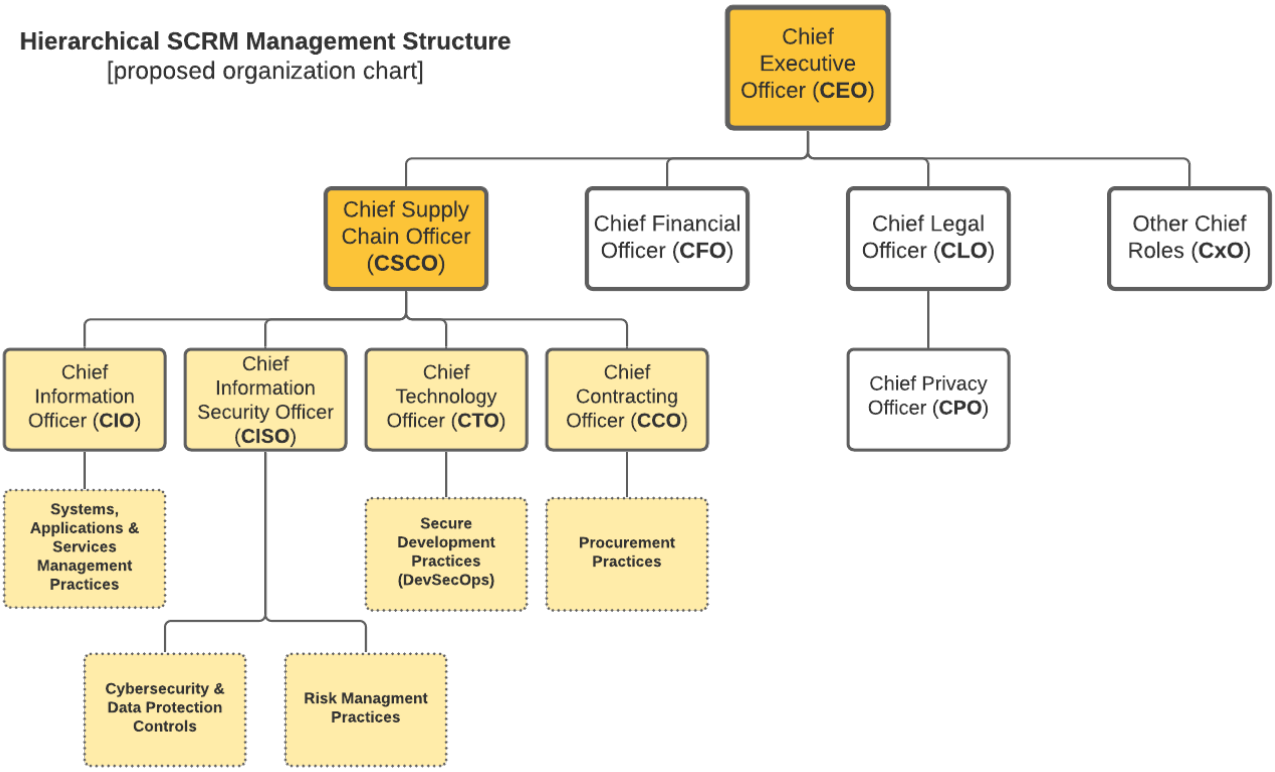
Efficient operational leadership requires the organization to structure roles that are complementary and not counterproductive. For the CSCO role to be successful in executing the organization's ZT/SCRM program:

- The CSCO needs to report directly to the organization's Chief Executive Officer (**CEO**) to eliminate conflicts of interests among leadership representing Lines of Business (**LOB**) within the organization.
- The CSCO must be able to influence cybersecurity and data protection controls by being part of the organization's cybersecurity steering committee.
- Due to the reliance on risk management practices and the underlying cybersecurity and data protection controls that enable a ZT/SCRM program to function, the Chief Information Security Officer (**CISO**) should directly report to the CSCO.
- Due to the supply chain nature of DevSecOps, the Chief Technology Officer (**CTO**) role should directly report to the CSCO.
- Due to the external focus of the ZT/SCRM program, the Chief Contracting Officer (**CCO**) role should directly report to the CSCO to ensure contracts and procurement actions are in-line with the ZT/SCRM program.

[4] *NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf*

- Due to how technology is so integral to business operations, the Chief Information Officer (**CIO**) role should directly report to the CSCO.
- The CISO, CIO, CTO and CCO need to be viewed as peers, each with an equal role of importance in the ZT/SCRM program, where the CSCO provides operational leadership to orchestrate ZT/SCRM activities across the enterprise and its supply chain.

It should be needless to say, but corporate "buy-in" is essential for the overall program to function accordingly. The "message from the top" must be from the Board of Directors (**BoD**) and CEO so that corporate executives (**CxO**) will be forced to adopt the practices within their Lines of Business (**LoB**) to address their inherent risk with technology and the supply chain. SCRM is a multi-player effort, so the organization must adopt a "One Team. One Fight" mentality that is driven by senior leadership first and foremost. Additionally, the organization's Internal Audit (**IA**) plays a crucial role in maintaining internal accountability, where there is a neutral system of checks and balances.



Secure Development Practices

ZT/SCRM is an enterprise-wide activity that is implemented throughout the System Development Life Cycle (**SDLC**). Within the concept of secure development practices, in order to ensure ZT/SCRM is operational it takes the following to exist and be functional:

- Maintain close working relationships through frequent visits and communications.
- Mentor and coach suppliers on ZT/SCRM and actively help suppliers improve their cybersecurity and supply chain practices.
- Invest in common solutions.
- Require the use of the same standards within the acquirer organizations and by suppliers, thereby simplifying communications about cybersecurity risk and mitigations and helping to achieve a uniform level of quality throughout the ecosystem.
- Restrict the use of open-source software to projects for which there is clear oversight and accountability. If this is not possible, then code audits/reviews should be performed for open-source project.

Resilience and improvement activities include:

- Rules and protocols for information sharing between acquirers and suppliers.
- Joint development, review and revision of incident response, business continuity and disaster recovery plans.
- Protocols for communicating vulnerabilities and incidents.
- Responsibilities for responding to cybersecurity incidents.
- Coordinated communication methods and protocols.
- Coordinated restoration and recovery procedures.
- Collaborative processes to review lessons learned.
- Updates of coordinated response and recovery plans based on lessons learned.

PROCUREMENT PRACTICES

ZT/SCRM lies at the intersection of cybersecurity and supply chain risk management. Existing supply chain and cybersecurity practices provide a foundation for building an effective Risk Management Program (**RMP**). Therefore, within the concept of procurement practices, in order to ensure ZT/SCRM is operational it takes the following to exist and be functional:

- Increased executive leadership or Board of Directors (**BoD**) involvement for establishing ZT/SCRM as a top business priority and to ensure proper oversight.
- ZT/SCRM intersects with the BoD fiduciary "duty of care" and BoD-level training should be provided to board members understand the current state and weaknesses of the organization's supply chain, including the BoD's responsibilities in executing a ZT/SCRM strategy.
- Clear governance of ZT/SCRM activities that includes cross-organizational roles and responsibilities with clear definitions and designation/distribution of these roles among enterprise risk management, supply chain, cybersecurity, product management and product security (if applicable) and other relevant functions appropriate for the organization's business.
- Leading framework-based policies, standards and procedures that provide guidance to different business units detailing their ZT/SCRM activities.
- Same policies used internally and with suppliers.
- Integration of cybersecurity considerations into the system and product development life cycle.
- Use of cross-functional teams to address specific, enterprise-wide risks.
- Clear definition of roles of individuals responsible for cybersecurity aspects of supplier relationships (which may be different than those responsible for procurement activities with specific suppliers).
- Establishment of Centers of Excellence (**CoE**) to identify and manage best practices.
- A set of measures of success used to facilitate decision-making, accountability and improvement.
- Approved and banned supplier lists.
- Use of software and hardware component inventory (e.g., bill of materials) for third-party components.
- Prioritization of suppliers based on their criticality.
- Establishment of testing procedures for the most critical components.
- Establishment of a known set of security requirements or controls for all suppliers, especially robust security requirements for critical suppliers to be used in procurement (sometimes known as master specifications).
- Service-Level Agreements (**SLA**) with suppliers that state the requirements for adhering to the organization's cybersecurity policy and any controls required of the supplier.
- Establishment of intellectual property rights agreements.
- Shared supplier questionnaires across like organizations, such as within the same critical infrastructure sector.
- Upstream propagation of acquirer's security requirements within the supply chain to sub-tier suppliers.
- Assurance that suppliers have only the access they need in terms of data, capability, functionality and infrastructure; bounding this access by specific time frames during which suppliers need it.
- Use of escrow services for suppliers with a questionable or risky track record.
- Provision of organization-wide training for all relevant stakeholders within the organization, such as supply chain, legal, product development and procurement; this training may also be extended to key suppliers.
- Identification of alternative sources of critical components to ensure uninterrupted production and delivery of products.
- Secure requirements guiding disposal of hardware that contains regulated data (e.g., CUI, FCI, PII, CHD, PHI, etc.) or otherwise sensitive information (e.g., Intellectual Property (**IP**)).
- Protocols for securely terminating supplier relationships to ensure that all hardware containing acquirer's data has been properly disposed of and that the risks of data leakage have been minimized.
- Establishment of formalized vendor management process, including a vendor management platform to track the state of SCRM-related controls across the supply chain.

RISK MANAGEMENT PRACTICES

ZT/SCRM needs to be implemented as part of an organization's overall Enterprise Risk Management (**ERM**) activities (e.g., NIST SP 800-39 & NISTIR 8286). These risk management practices involve identifying and assessing applicable risks, determining appropriate response actions and developing a ZT/SCRM strategy. Within the concept of risk management practices, in order to ensure ZT/SCRM is operational it takes the following to exist and be functional:

- Activities should involve identifying and assessing applicable risks, as well as determining appropriate response actions.
- Developing a ZT/SCRM strategy and implementation plan to document selected response actions and monitoring performance against that plan.
- Manage risks. Cyber supply chain risk is associated with a lack of visibility into, understanding of and control over many of the processes and decisions involved in the development and delivery of cyber products and services.
- Manage threats and vulnerabilities. Effectively managing cyber supply chain risks requires a comprehensive view of threats and

vulnerabilities.
    - Threats can be either “adversarial” (e.g., tampering, counterfeits) or “non-adversarial” (e.g., poor quality, natural disasters).
    - Vulnerabilities can be “internal” (e.g., organizational procedures) or “external” (e.g., part of an organization’s supply chain).
- The ZT/SCRM strategy should be periodically reviewed by the BoD’s risk or audit committee.

Systems, Applications & Services Management Practices

ZT/SCRM requires organizations to identify critical systems, applications and services, as well as sensitive data, that are most vulnerable and can cause the largest organizational impact if compromised. Within the concept of systems, applications & services management practices, in order to ensure ZT/SCRM is operational it takes the following to exist and be functional:

- Developing Data Flow Diagrams (**DFDs**) that track where regulated data (e.g., CUI, FCI, PII, CHD, PHI, etc.) or “crown jewels” IP is stored, transmitted and processed.
- Identifying suppliers that process regulated data or “crown jewels” IP.
- Developing network diagrams that identify suppliers that have access to the acquirer’s system and network infrastructure.
- Threat modeling to determine whether a supplier can become an attack vector by being compromised and allowing threat actors access to the acquirer’s organization.
- For technology companies, whether a supplier can become an attack vector for the technology company’s products or services delivered to customers.
- Controlling the volume of data a supplier has access to or hosts.
- Controlling the physical location of data to ensure compliance with the organization’s data governance requirements.
- Monitoring the revenue contribution of suppliers (e.g., criticality).

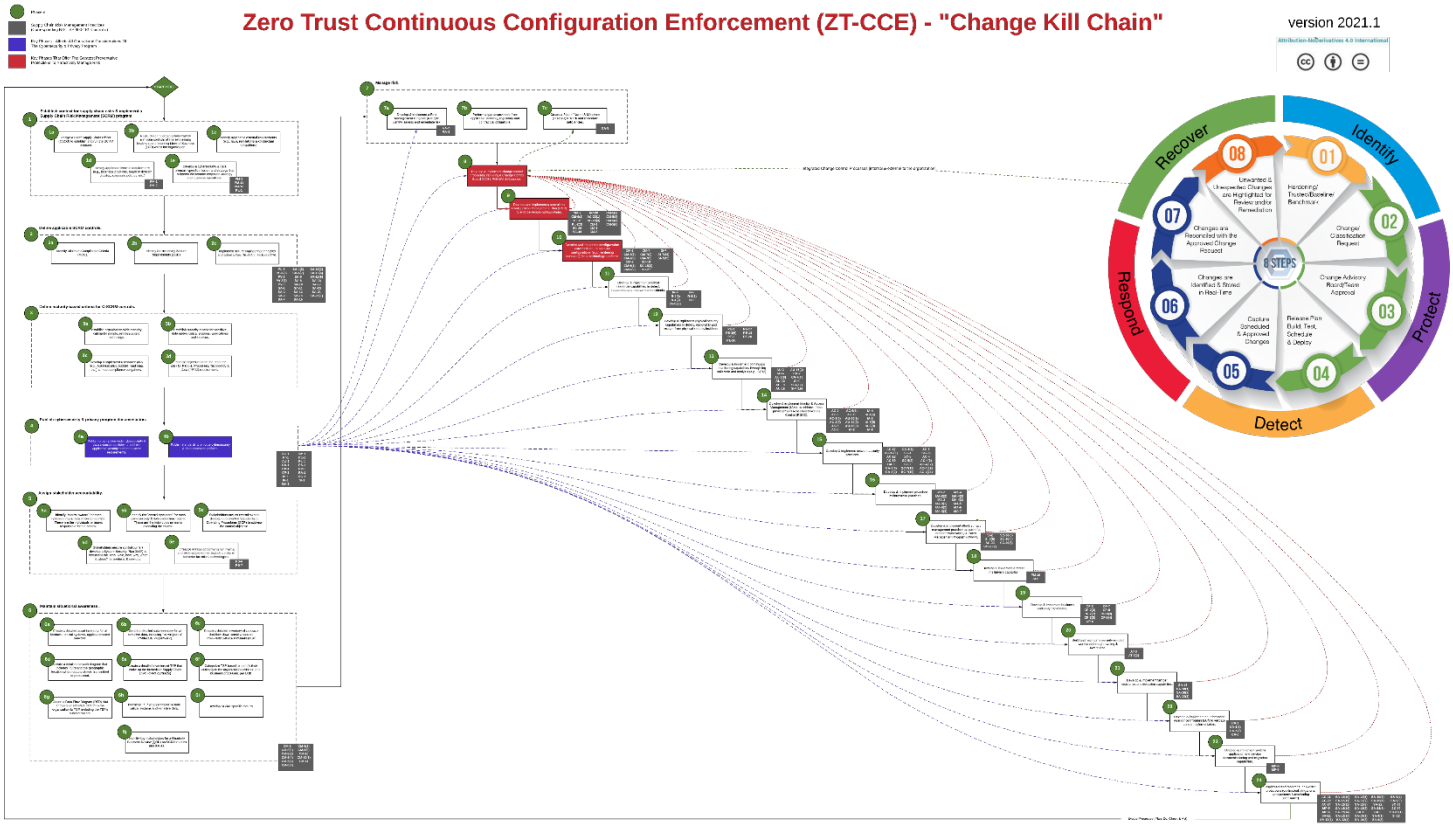
APPLYING THE KILL CHAIN MODEL TO ZERO TRUST & SCRM

You might be asking yourself how a “kill chain” model applies to ZT/SCRM. The root issue that is being addressed pertains to how many IT & cybersecurity professionals who are looking at the near future and beyond with dread. With ZT/SCRM, these front-line IT/cybersecurity practitioners currently do not know where to start, let alone what path they need to follow to align with ZT/SCRM. The Change Kill Chain provides a prioritized project plan approach to ZT/SCRM.

There is an abundance of *"What is ZT & SCRM?"* guidance on the Internet, but there is a lack of practical guidance of HOW you are actually supposed to "do ZT & SCRM" in realistic terms. The Change Kill Chain is designed to provide a roadmap that would be usable for anyone:

(1) Starting out on ZT or SCRM journey for their organization; or
(2) Wanting to double check their approach to implementing ZT or SCRM.

The graphical approach to the Change Kill Chain is shown below and is downloadable as a separate PDF for that infographic.



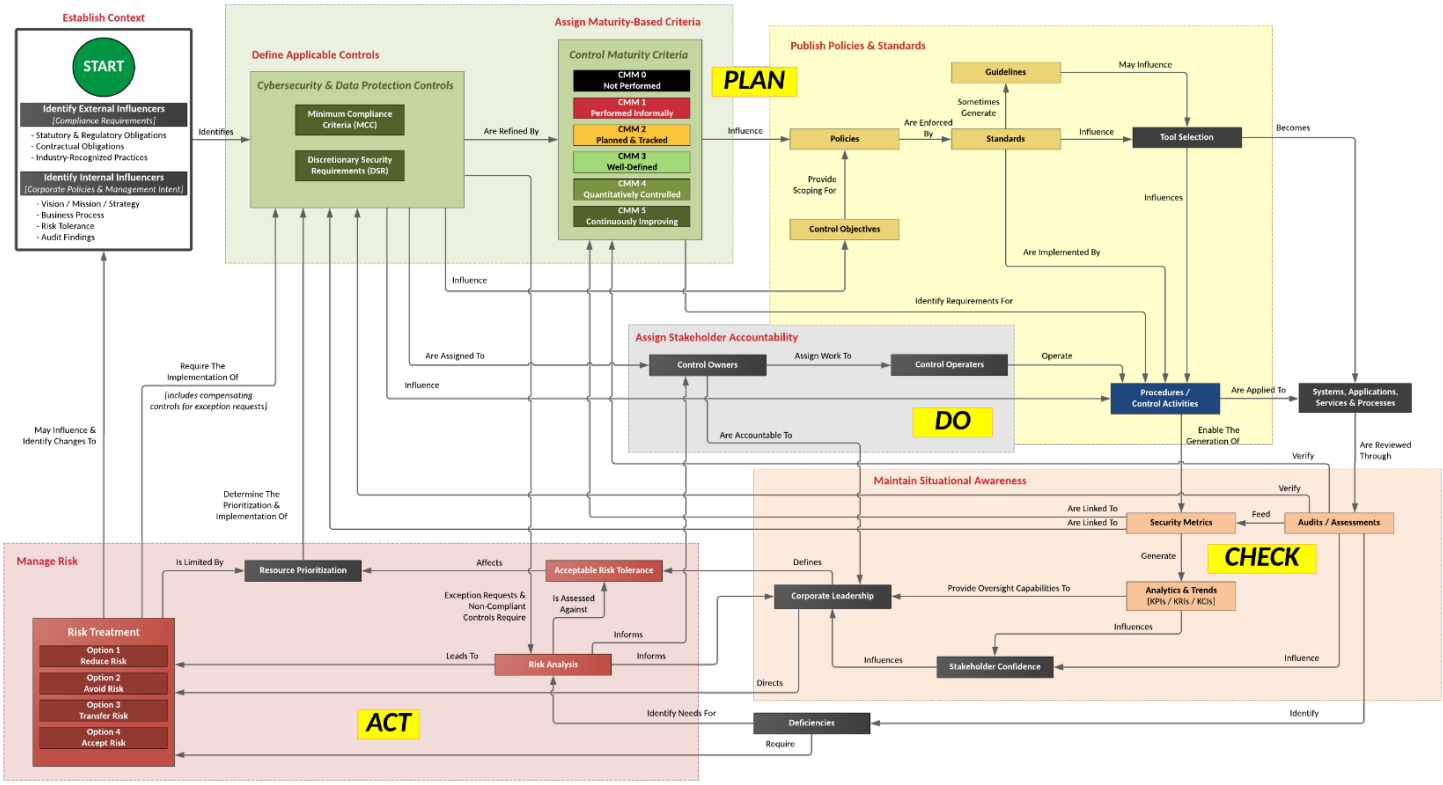
[image is downloadable from http://www.change-kill-chain.com]

ZERO TRUST & SCRM PROJECT PLANNING TOOL

The premise of the Change Kill Chain is to build viable approach for organization to use in order to create a prioritized project plan for implementing a ZT/SCRM program. The intention of using the Change Kill Chain is that if you apply a prioritized, phased approach towards ZT/SCRM-related activities, it is possible to avoid rework and cascading failures by addressing dependencies earlier in the process. The bottom line is this model breaks down ZT/SCRM into 24 major steps, which can then be translated into a project plan.

The Change Kill Chain leverages the principles of the Integrated Controls Management (**ICM**) model:[5]

(1) Establish context;
(2) Define applicable controls;
(3) Assign maturity-based criteria;
(4) Publish policies & standards;
(5) Assign stakeholder accountability;
(6) Maintain situational awareness;
(7) Manage risk; and
(8) Evolve process.



[image is downloadable from https://graphics.complianceforge.com/icm/ICM-PCDA.pdf]

[5] *ComplianceForge's Integrated Controls Management (ICM) model - https://graphics.complianceforge.com/icm/ICM-PCDA.pdf*

Background On The Logic Used In This Model

It is important to explain the thought process that went through the prioritization of the model's phases. This is a quick explanation on some of the reasoning used to determine prioritization:

- There are fundamental steps that must occur to establish the basis to be able to implement ZT/SCRM-related steps. This groundwork is essentially the first 6 steps.
- You cannot legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management and a defined risk threshold. Risk management is the key building block that other practices rely upon.
- Once you have solid risk management practices, change control is the second most important phase to address, since that is needed to legitimately alter other practices and you need to be able to document your changes and track open issues in a Plan of Action & Milestones (**POA&M**) (e.g., evidence of due care).
- Secure configurations and centralized configuration management (e.g., Group Policies, hardening scripts, etc.) almost go hand-in-hand, but before you can centrally manage configurations, they need to be defined and standardized. Configuration management supports steps going forward.
- From there, the assumption is that you will discover issues so incident response capability needs to exist.
- Since ZT/SCRM spans more than just cybersecurity, there is a necessity to have physical security practices in place. These physical security capabilities should support the organization's overall incident response plans.
- Event logging (continuous monitoring) is next and needs to exist before secure configurations, since logs need to get sent somewhere. You need to have this logging infrastructure in place before you get into secure configurations.
- Next, Identity and Access Management (**IAM**) needs to be locked down to ensure aspects of least privilege and Role Based Access Control (**RBAC**) are implemented. The reason IAM comes after secure configurations is due to troubleshooting - if you have "gold standard" secure builds to work from, it is easier to then assign permissions/RBAC that will work with those builds. The alternative is your new configurations break IAM/RBAC practices, which is something that should be avoided.
- Network security practices are somewhat covered through secure configurations and IAM practices, but aspects such as remote access and network architecture (e.g., Zero Trust Architecture (**ZTA**), jump boxes, segmentation, etc.) need to be standardized and enforced uniformly.
- You realistically can't do vulnerability management without first having solid maintenance capabilities, so maintenance needs to be formalized with change control integrations. Maintenance needs to be tied into change management, which has a risk management component to it.
- The concept of vulnerability management is broad and is best summed up by the term "attack surface management" where you are doing what you can to minimize the ways an adversary can attack. This relies on maintenance practices and change management being in place and operating.
- From there, the remaining phases are relatively subjective in the order the steps are implemented until you reach the step where an Information Assurance Program (**IAP**) will help assist the intern audit function by performing Control Validation Testing (**CVT**) operations. This is often done for pre-production testing, but can be done after major changes to evaluate control implementation before "go live" of the updated system, application or service.
- Realistically, your organization needs to have the first 23 steps well-managed before actions are taken to provide stringent oversight on third-party practices. This is why supply chain protections are the 24th step in this kill chain.

CHANGE KILL CHAIN PHASES

The Change Kill Chain is made up of 24 phases (these correspond to those shown in the associated infographic). It is important to note that these steps can be applied both to internal practices and Third-Party Service Providers (**TSP**). Realistically, an organization must first "master the fundamentals" and have its own ZT/SCRM practices in order before proactive oversight of TSPs is feasible.

1. ESTABLISH CONTEXT FOR SUPPLY CHAIN RISKS & IMPLEMENT A ZERO TRUST & SUPPLY CHAIN RISK MANAGEMENT (ZT/SCRM) PROGRAM.

To build and maintain efficient and effective operations, a ZT/SCRM program must have a hierarchical vision, mission and strategy that directly supports the organization's broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), as well as internal directives (e.g., Board of Directors (**BoD**), corporate policies, etc.). This is a due diligence element of the ZT/SCRM program.

This step has 5 subcomponent steps:

- **1a.** Assign a Chief Supply Chain Officer (**CSCO**) to establish and run the ZT/SCRM program.
- **1b.** Restructure the organization chart to eliminate conflicts of interests among leadership representing Lines of Business (**LOB**) within the organization.
- **1c.** Identify applicable external requirements (e.g., laws, regulations & contractual obligations)
- **1d.** Identify applicable internal requirements (e.g., business practices, BoD dictates, corporate policies, etc.)
- **1e.** Develop a cybersecurity & data program-specific mission and strategy that supports the broader corporate strategy and business operations.

2. DEFINE APPLICABLE ZERO TRUST & SCRM CONTROLS.

A tailored control set of cybersecurity and data protection controls must exist. This control set needs to be made of Minimum Compliance Criteria (**MCC**) and Discretionary Security Requirements (**DSR**). This blend of "must have" and "nice to have" requirements establish an organization's tailored control set to ensure both secure practices and compliance are designed for.

This step has 3 subcomponent steps:

- **2a.** Identify MCC.
- **2b.** Identify DSR.
- **2c.** Implement secure engineering principles and adopt a Zero Trust Architecture (**ZTA**).

3. DEFINE MATURITY-BASED CRITERIA FOR ZT/SCRM CONTROLS.

The cybersecurity & privacy program must assign maturity targets to define organization-specific "what right looks like" for controls. This establishes attainable criteria for People, Processes, Technology & Data (**PPTD**) requirements. Tailored maturity level criteria can be used to plan for, budget for and assess against. Maturity targets should support the organization's need for operational resiliency.

This step has 4 subcomponent steps:

- **3a.** Establish organization-wide maturity criteria for people, processes and technology.
- **3b.** Establish maturity criteria for sensitive data and/or critical systems, applications and services.
- **3c.** Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet compliance obligations.
- **3d.** Prioritize objectives from the resource plan for PPTD requirements.

4. PUBLISH POLICIES & STANDARDS FOR ZT/SCRM.

Documentation must exist, otherwise an organization's cybersecurity and data protection practices are unenforceable. Formalizing organization-specific requirements via policies and standards are necessary to operationalize controls. Documented policies and standards provide evidence of due diligence that the organization identified and implemented reasonable steps to address its applicable requirements.

This step has 2 subcomponent steps:

- **4a.** Publish organization-wide cybersecurity and privacy policies to address applicable security and data protection requirements.
- **4b.** Publish standards to enforce cybersecurity and privacy policies.

5. Assign Stakeholder Accountability.

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These "control owners" may assign the task of executing controls to "control operators" at the Individual Contributors (**IC**)-level. Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (**SOP**) that enable ICs to execute those controls. The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

This step has 5 subcomponent steps:

- **5a.** Identify "control owners" for all applicable cybersecurity and privacy controls. These are the individuals or teams responsible for the control.
- **5b.** Identify the "control operators" for all applicable cybersecurity and privacy controls. These are the individuals or teams executing the control.
- **5c.** Stakeholders ensure control owners develop documented SOP to address the control objective(s).
- **5d.** Stakeholders ensure control owners develop a System Security Plan (**SSP**) to document the "who, what, how, why, when & where" for products & services.
- **5e.** Formalize access agreements for internal and external personnel, including rules of behavior for critical technologies.

6. Maintain Situational Awareness - Establish An Internal Audit (IA) Capability

Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls' performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability information, this insight provides "situational awareness" that is necessary for organizational leadership to adjust plans to operate within the organization's risk threshold.

An organization's Internal Audit (**IA**) function provides quality control. This function can help validate the scope and impact of risk, which stakeholders may be unaware of. IA practices generate evidence of due care that reasonable steps are in place to validate stakeholder claims and assumptions.

This step has 10 subcomponent steps:

- **6a.** Create a detailed asset inventory for all business-critical systems, applications and services (internally hosted as well as those hosted by third-parties).
- **6b.** Create a detailed data inventory for all sensitive data, including "crown jewels" Intellectual Property (**IP**).
- **6c.** Create a detailed inventory of contracts that flow-down sensitive data to Third-Party Service Providers (**TSP**).
- **6d.** Create a detailed network diagram that includes TSPs and the geographic location where data is stored, transmitted and/or processed.
- **6e.** Create a detailed inventory of TSP that make up the Direct Supply Chain (**DSP**) (e.g., direct contracts).
- **6f.** Categorize TSP based to identify their criticality to the organization's mission and business processes, per LOB
- **6g.** Create a Data Flow Diagram (**DFD**) that shows how sensitive data from the organization to TSP, including the TSP's subcontractors.
- **6h.** Inventory TSP access control for both critical systems and sensitive data.
- **6i.** Develop ZT/SCRM -specific metrics.
- **6j.** Identify key stakeholders for a Quarterly Business Review (**QBR**) on ZT/SCRM metrics and issues.

7. Manage Risk.

Proactive risk management processes must exist across all phases of development/information/system life cycles to address confidentiality, integrity, availability and safety aspects. Risk management must address internal and external factors, including cybersecurity, privacy and ZT/SCRM considerations. To manage risk, it requires the organization to enforce a clearly defined risk threshold and ensure reasonably-expected secure practices are operational.

This step has 3 subcomponent steps:

- **7a.** Develop & implement a Risk Management Program (**RMP**) to identify, assess and remediate risk.
- **7b.** Perform a gap assessment from applicable statutory, regulatory and contractual obligations.
- **7c.** Create a Plan of Action & Milestone (**POA&M**) to track and remediate deficiencies.

8. Change Control.

Develop & implement change control processes and workflows, including a Change Control Board (**CCB**) that is technically competent to evaluate security ramifications for baseline security configuration deviations.

9. Centralized Configuration Management Plan (CMP).
Develop and implement a centralized Configuration Management Plan (**CMP**) to enforce secure configurations.

10. System Hardening.
Identify, build & implement secure baseline configurations (e.g., hardening standards) for all technology platforms.

11. Incident Response.
Develop & implement incident response capabilities to detect, respond to and recover from incidents.

12. Physical Security.
Develop & implement physical security capabilities to detect, respond to and recover from physical security incidents.

13. Continuous Monitoring.
Develop & implement continuous monitoring capabilities through log collection and analysis (e.g., SIEM).

14. Identity & Access Management (IAM).
Develop & implement Identity & Access Management (**IAM**) to address "least privilege" and Role-Based Access Control (**RBAC**).

15. Network Security.
Develop & implement network security practices.

16. Maintenance.
Develop & implement proactive maintenance practices.

17. Attack Surface Management (ASM).
Develop & implement Attack Surface Management (**ASM**) practices as part of a broader Vulnerability & Patch Management Program (**VPMP**).

18. Threat Intelligence.
Develop & implement a threat intelligence capability.

19. Business Continuity.
Develop & implement business continuity capabilities (e.g., Disaster Recovery (**DR**), Business Continuity (**BC**), Continuity of Operations (**COOP**), etc.).

20. Security Awareness Training.
Build and maintain a security-minded workforce through training & awareness.

21. Tamper Resistance & Detection.
Develop & implement tamper resistance and detection capabilities.

22. Information Assurance Program (IAP).
Develop & implement an Information Assurance Program (**IAP**) to validate control implementation.

23. Decommissioning & Migration.
Develop & implement system application and service decommissioning and migration capabilities.

24. Supply Chain Protections.
Implement and monitor supply chain protections (contractual obligations, assessments & monitoring compliance).

APPENDIX A: DOCUMENTATION TO SUPPORT ZERO TRUST & SUPPLY CHAIN RISK MANAGEMENT

The purpose of a company's cybersecurity documentation is to prescribe a comprehensive framework for:

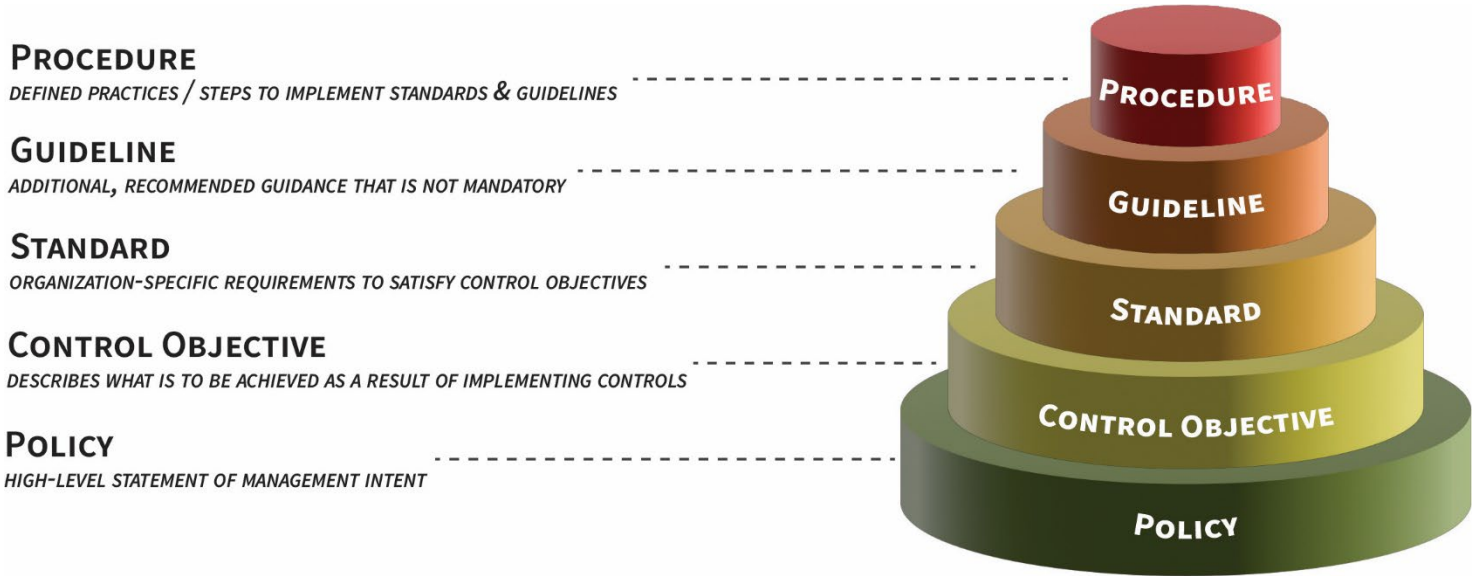
- Creating a clearly-articulated approach to how your organization handles cybersecurity and privacy practices.
- Protecting the confidentiality, integrity, availability and safety of data and systems across the enterprise.
- Providing guidance to help ensure the effectiveness of cybersecurity and privacy controls that are put in place to support your company's operations.
- Helping an organization's users recognize the highly-networked nature of the current computing environment to provide effective organization-wide management and oversight of those related cybersecurity and privacy controls.

Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for users to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off of the policy and all of the components of cybersecurity and privacy documentation building off each other to make a cohesive approach to addressing applicable requirements:

CYBERSECURITY DOCUMENTATION COMPONENTS

Cybersecurity and privacy documentation is comprised of five (5) core components:

(1) Policies are established by the organization's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support the organization's overall strategy and mission;
(2) Control Objectives identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide organization-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines are additional guidance that is recommended, but not mandatory.

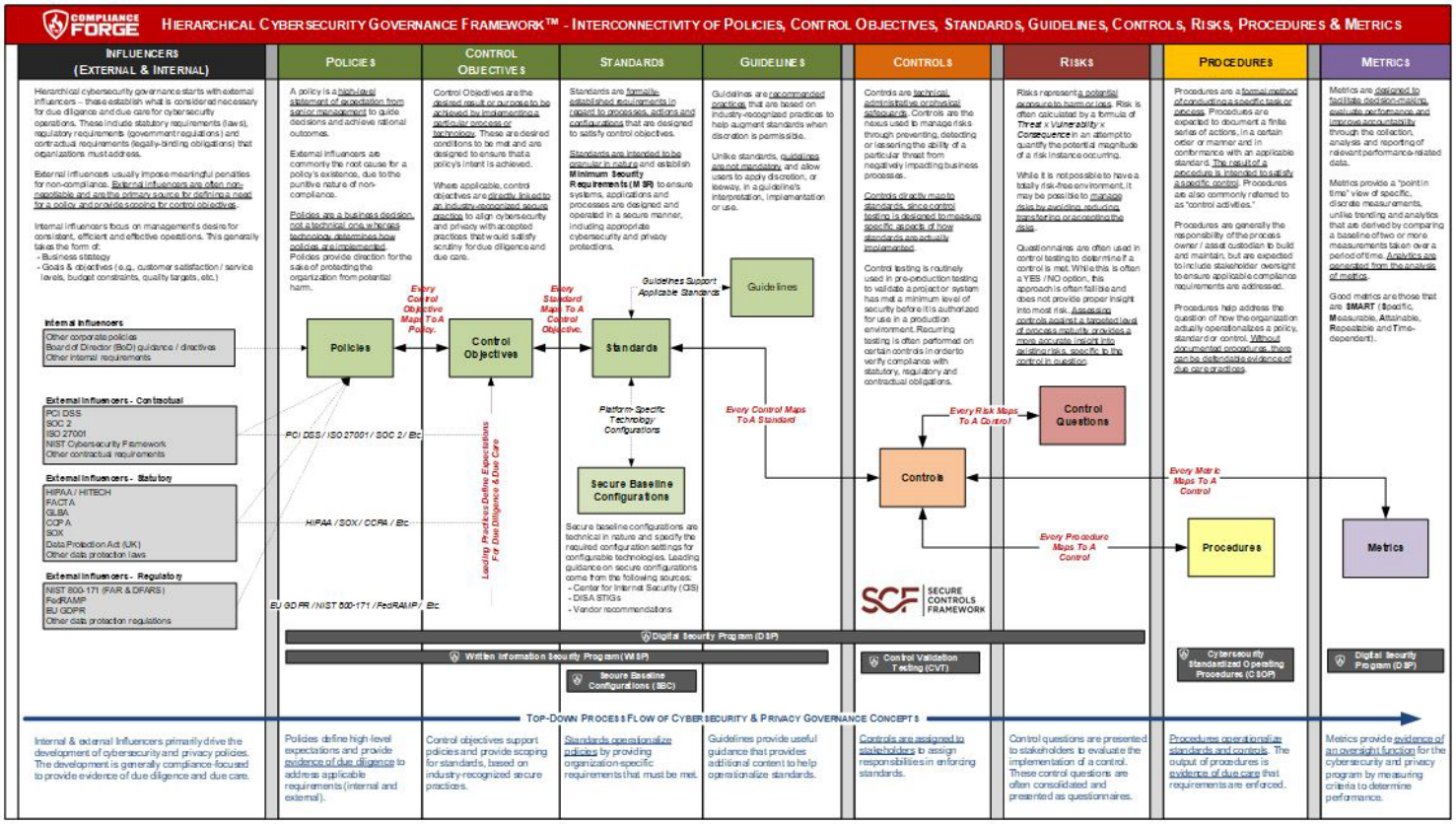


CYBERSECURITY DOCUMENTATION HIERARCHY – UNDERSTANDING HOW CYBERSECURITY DOCUMENTATION IS CONNECTED

When you look at establishing cybersecurity and privacy documentation, it all starts with influencers – these influencers set the tone and establish what is considered to be due care for cybersecurity and privacy practices:

- External Influencers - This includes a wide-range of compliance obligations that an organization has to address:
  - Statutory requirements (laws);
  - Regulatory requirements (government regulations); and
  - Contractual requirements (legally-binding agreements); and
- Internal Influencers - These are business-driven and the focus is more on executive management's desire for consistent, efficient and effective operations.

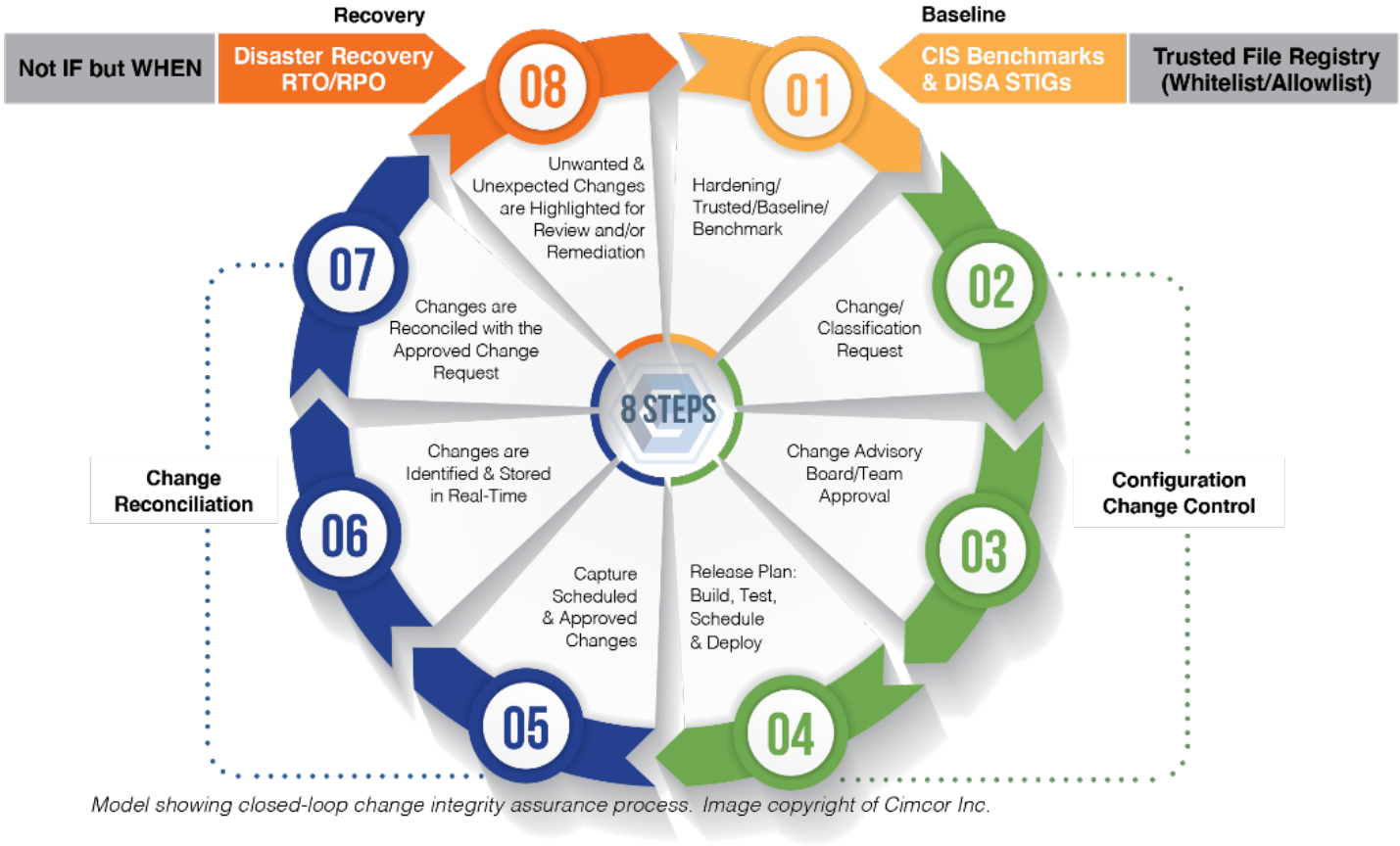
ComplianceForge developed the Hierarchical Cybersecurity Governance Framework (**HCGF**) to help visualize this. When documentation is all laid out properly, your company's cybersecurity documentation show flow like this where your policies are linked all the way down to metrics:



[image is downloadable from: https://graphics.complianceforge.com/graphics/ComplianceForge%20Hierarchical%20Cybersecurity%20Governance%20Framework.pdf]

APPENDIX B: BASELINES, CONFIGURATION CHANGE CONTROL, CHANGE RECONCILIATION & RECOVERY

What baselines (secure baseline configurations / hardening), configuration change control, change reconciliation and recovery have in common is these controls are requirements in almost all major security frameworks. Cimcor, Inc. developed an 8-step, closed-loop workflow that emphasizes detective controls and assembles those them into an industry-leading, practices-based process. When paired with automation, this workflow enables an unprecedented ability to identify unknown, unwanted and unauthorized changes to your IT and cloud assets in real-time and provides facilities to remediate either manually or automatically.



Model showing closed-loop change integrity assurance process. Image copyright of Cimcor Inc.

Four key areas where Cimcor's model supports the Zero Trust Continuous Configuration Enforcement (**ZT-CCE**) "Change Kill Chain" model includes:

(1) **Baselines (Secure Baseline Configurations / Hardening).** Validate and verify that your infrastructure is hardened and secure with industry-recognized security baselines as a mechanism to establish a trusted baseline configuration. Couple this with a whitelist/allowlist database that can verify the authenticity and integrity of the individual files provides additional assurances of system integrity.

(2) **Configuration Change Control**. The process of regulating and approving changes throughout the entire operational life cycle of an information system from an authoritative baseline. This is traditionally accomplished through traditional IT Service Management (**ITSM**) products. However, ideally, this functionality should also be included in security platforms or at a minimum, security platforms should be integrated in a manner to support the ticketing process.

(3) **Change Reconciliation**. Highlight, curate and triage observed changes against expected and authorized changes to create a closed-loop change control process. This best practice can drives Mean-Time-To-Identify (**MTTI**) breaches and Mean-Time-To-Detect (**MTTD**) breaches down to seconds. Real-time change detection is essential but having the functionality to rapidly respond and remediate those changes is what will ultimately help you achieve and maintain continuous integrity.

(4) **Recovery**. The ability to roll-back and remediate to a last know trusted baseline is a core function that will allows Mean-Time-To-Restore (**MTTR**) and Mean-Time-To Contain (**MTTC**) to be measured in seconds. Recovery should be configurable, in a matter that will allow the user to maintain a history of trusted baselines and to roll-back to the most appropriate baseline which will enable full recovery.

The reasons why this is important is straightforward:

(1) Cost. It is generally less expensive to prevent an incident (e.g., ransomware outbreak) that it is to respond to it; and

(2) Time. Automating response processes can both minimize impact and decrease the time associated with the incident, which can help mitigate associated costs.

BASELINES (SECURE BASELINE CONFIGURATIONS / HARDENING)

"Hardening" is the process of securing an asset by reducing its attack surface. That means configuring the asset in a way that reduces the number of tools, techniques and tactics that an attacker can utilize to gain access to it. Once an asset has been hardened, it becomes a trusted reference point from which to manage deviations from to ensure that only expected changes occur. These authorized changes are often referred to as configuration drift or infrastructure drift.

It is important for organizations to integrate CIS Benchmarks, DISA STIGs and Original Equipment Manufacturer (**OEM**) recommended security practices as a reference point to establish a "hardened" Secure Baseline Configuration (**SBC**). This reference point can be used to create a chain of evidence which can be produced to validate and verify the expected changes to the hardened state of an asset, system or device. This is where automation is crucial to leverage some form of "Trusted File Registry" database of known and trusted software. This database can be used to validate and verify the authenticity and integrity of the software files themselves through a chain of custody back to the software vendor that published the software.

CONFIGURATION CHANGE CONTROL

The management and control of configurations and baselines for systems, applications and services to enable security and facilitate the management of risk. Any and all deviations from a baseline configuration should be triaged and evaluated via an authorized change management process.

Automated tools, such as CimTrak, can ensure the security and integrity of your critical IT assets by detecting changes to your applications and infrastructure in real-time. When a change is detected, automated processes should provide a detailed audit trail of the incident, including a appropriate forensic information, including but not limited to:

- Who made the change?
- What was changed?
- Where the change was made?
- When the change took place?
- How the change was made?

CHANGE RECONCILIATION

The process of regulating and approving changes throughout the entire operational life cycle of an information system. The workflow process outlined above will be able to highlight and compare observed changes against expected/authorized changes. In the event of an unexpected, unauthorized and unwanted change, it should be immediately highlighted for analysis and remediated if necessary to create a trusted and resilient infrastructure. In the absence of this process, integrity, configuration drift, or infrastructure drift is inevitable!

Without a built-in ticketing system (which is also the integration mechanism to traditional ITSM products if deployed) to manage the process of classifying and approving change, it is nearly impossible to perform change reconciliation activities. This process provides the unique ability to capture the expected changes and reconcile/curate those changes with observed changes to then highlight everything that is unauthorized change on critical systems within your environment. Automated tools, such as CimTrak, should be configured to prevent changes entirely for those files and directories that should never change.

When changes to a system happen, those changes must be considered untrustworthy until a workflow process validates and verifies the integrity of those changes by determining if they were approved and authorized by an authoritative person or Change Advisory Board (**CAB**). Only until this happens will we be able to identify Zero Day Attacks and fulfill the concept of Zero Trust become a reality.

RESILIENCY / RECOVERY

Often, security professionals will remark, "It's not a matter of if, but when" a security event will occur. With this inevitability in mind, it is extremely important to ensure that the recovery is integrated into your security program. Recovery is the process of mitigating the scenario where the chain of trust is broken for some unforeseen reason. When this happens, having a defined process to ensure the trust and resiliency of the data and infrastructure is paramount. Traditional ITSM products implement recovery functionality for purposes of operational up-time and availability. The terminology of Recovery Time Objective (**RTO**) and Recovery Point Objective (**RPO**) are closely aligned with security objectives of Mean-Time-To-Contain (**MTTC**) as statistics show "change" is the most common cause of both operational downtime and security incidents.

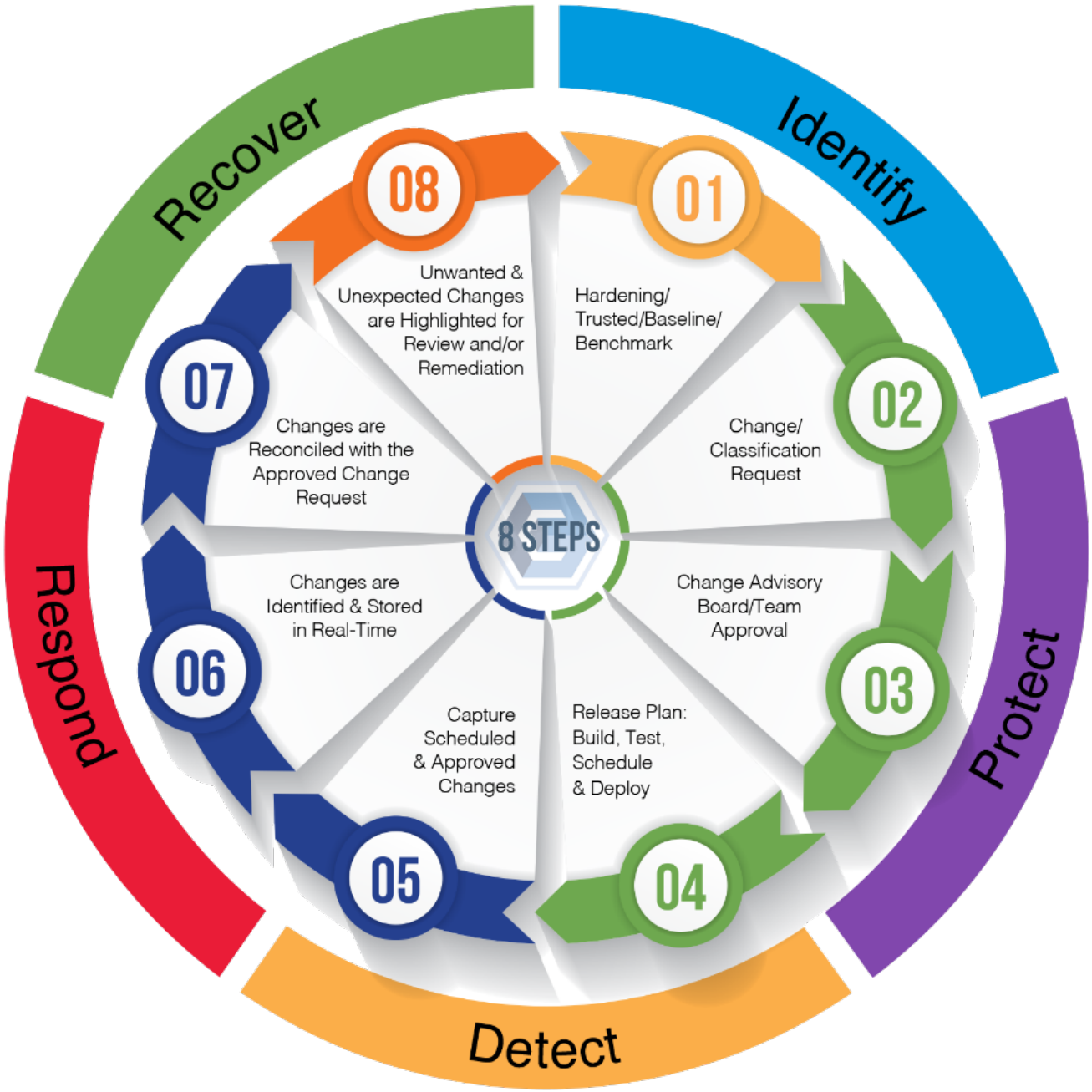
- Recovery Time Objective (**RTO**): The maximum amount of time that should pass before your IT systems recover.
- Recovery Point Objective (**RPO**): The maximum amount of time permissible since the most recent data backup in order for your IT systems to recover.

Automated tools, such as CimTrak, can restore and recover from unwanted change is measured in seconds which differs from traditional ITSM back-up and restoration functionality of reprovisioning. It is necessary to have the ability to discreetly identify and restore the necessary files from any number of previously trusted baselines to avoid the costly time and effort of reprovisioning an entire system. Automated tools should be configured to roll-back and remediate changes if and when necessary (manually or automatically), to any previous trusted state(s) as it securely stores the previous files associated with that state of operation in a compressed and encrypted format.

APPENDIX C: NIST CYBERSECURITY FRAMEWORK ALIGNMENT

Cimcor's 8-step, closed-loop security workflow also aligns effectively with the National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**). The NIST CSF's five functional requirements of (1) Identity, (2) Protect, (3) Detect, (4) Respond and (5) Recover overlay onto this model, which further supports the Zero Trust Continuous Configuration Enforcement (**ZT-CCE**) "Change Kill Chain" approach to prioritizing cybersecurity controls.

When viewed through against the NIST CSF, the Change Kill Chain, along with Cimcor's security workflow model, focus on the "Identify" and "Protect" nature of cybersecurity controls. The reason for this is it is more cost-effective in the long-term to perform due diligence steps that enact and enforce secure baseline configurations, rather than focusing efforts on "Detect" and "Respond" cybersecurity controls. While this approach does rely upon automated technologies to enforce configurations and revert unapproved changes, the focus on prevention is aimed at implementing and maintaining a sustainable approach to securing an organization's enterprise, regardless of the geographic location of the system, application or service.



APPENDIX D: CRITICAL RESOURCES & ACQUISITION PATH

The premise of the Zero Trust Continuous Configuration Enforcement (**ZT-CCE**) model was to create a proof of concept for an efficient way to plan out a roadmap to successfully implement robust Zero Trust and Supply Chain Risk Management (**ZT/SCRM**) cybersecurity and privacy practices that focus on prevention and automated remediation. The end result is a viable approach for organizations to use in order to create a prioritized project plan for ZT/SCRM-focused secure practices. This requires taking the organization's critical resources and the acquisition path (e.g., business processes) into consideration.

THEORY OF CONSTRAINTS

As with any process, an organization's cybersecurity & privacy compliance program is always vulnerable due to the ability of the "weakest link" (e.g., person, part, supplier and/or process) to cause damage and adversely affect the overall cybersecurity & privacy compliance program. The theory of constraints (**TOC**) is a management paradigm that views any manageable system as being limited in achieving more of its goals by a very small number of constraints. There is always at least one constraint in a project/initiative and TOC utilizes a process to identify the constraint(s) and restructure the rest of the organization/processes around it.

MANAGEMENT FOCUS

At the management level, TOC focuses on:

- Define business processes;
- Establish minimum quality requirements for people, processes and technologies;
- Establish, review and enforce contract requirements;
- Appropriately resource technical requirements; and
- Maintain situational awareness.

TECHNICAL FOCUS

At the individual contributor level (e.g., analyst, engineer, technician, etc.), TOC focuses on:

- Define technical requirements;
- Identify and implement "industry recognized practices" to design, build and maintain systems, applications and services; and
- Provide metrics to management to maintain situational awareness.

CHANGE MANAGEMENT WITHIN ZT/SCRM

As you work through security and privacy controls, it is common that new technology solutions are necessary. This is inevitable and your organization may need to re-factor the Change Kill Chain as guidance for time and resource constraints.

There are several factors that need to be considered when incorporating new technologies:

1. Define the appropriate technology solution(s) by identifying necessary People, Processes & Technology (**PPT**) (**step 3a**).
2. Identify suitable vendors based on the organization's:
    a. Knowledge of your organization's statutory, regulatory and contractual obligations (**step 2a**);
    b. Ability to fill gaps related to those obligations (**step 5**); and
    c. Ability to perform as expected (e.g., you want to avoid paying someone to be their "Guinea pig" to learn how to implement technologies and/or processes through on-the-job training).
3. Without exception, leverage your organization's change control processes to ensure the technology solutions are documented, reviewed and approved.
    a. Leverage the Change Kill Chain phases to identify where you will implement and operate the new technology solution to understand possible "cascading effects" of new technologies on other phases.
4. Whenever multiple technology implementations overlap in a Change Kill Chain phase, be aware of time and resource constraints.
    a. Add time allowances for the procurement, training, configuration and ongoing operation of the new technology solution;
    b. Plan for the possibility that overlapping implementations may:
        i. Extend the time spent in a particular phase of the Change Kill Chain; and
        ii. Increase labor-related expenses:
            1. Professional services from the vendor or managed IT service providers familiar with the solution; and/or
            2. Technical staff support from another internal team.
5. Integrate new technologies into internal audit practices (**phase 22**) to maintain your Information Assurance (IA) capability and controls governance.
    a. This is the optimal time to develop performance measures (e.g., metrics) for assessing the continued effectiveness of your newly-implemented technology solutions.

APPENDIX E: A CASE FOR ZERO TRUST CONTINUOUS CONFIGURATION ENFORCEMENT

The analogies between traditional supply chain functions (e.g., production, services, value delivery, etc.) and cybersecurity operations (e.g., confidentiality, integrity, availability and safety) may not be immediately apparent. However, as cybersecurity threats continue to disrupt supply chains and critical infrastructure, organizations may soon find the need to apply robust Supply Chain Risk Management (SCRM) practices as part of an overall business survival and resiliency strategy that leverages existing lean manufacturing principles.

In support of the concept of Zero Trust Continuous Configuration Enforcement (**ZT-CCE**), Toyota operates a supply chain management system designed with monitoring and risk management at its core. The automaker's lean "4P" model (*Philosophy, Process, People and Partners and Problem Solving*) results in a resilient supplier base that is less-affected by trends and short-term disruptions.

Toyota views its suppliers' challenges as its own challenges, since it impacts Toyota's own ability to produce. Toyota fully appreciates the concept that any challenge to Toyota's supply chain is inherently a Toyota problem. Toyota's model often leads to "joint improvement" activities where the automaker practices *genchi genbutsu*. *Note - It may be worthwhile to research the Toyota Production System for yourself to understand the challenge and difficulties Toyota faces, since that may be applicable to your specific business model.*

To help with problem-solving and continuous improvement, Toyota actively involves itself in its suppliers' operations to create a mutually-beneficial outcome. Toyota's involvement to directly monitor its supply chain allows it to understand whether those third-party suppliers can meet Toyota's production needs and that insight empowers Toyota to make adjustments, as necessary. Therefore, rather than being surprised by sudden shortages or disruptions, Toyota's supply chain acts as a sensor to allow it to detect trends well before becoming issues that crest the global horizon.

As with any supply chain, organizations can expect some suppliers to possess fewer resources, expertise and organizational maturity, based on the organization's size and industry. Therefore, during the ZT-CCE process, organizations have an opportunity to propagate new competencies and best practices throughout its supply chain. However, deciding to "find out for yourself" where suppliers struggle with cybersecurity is an unsettling proposition: "*What if I discover that my suppliers are less secure than anticipated?"* For the Toyota analogy, the worse option for the automaker is, "*What if I remain blind to supplier shortcomings*?" Toyota's model is aggressively proactive and that has served the organization extremely well. By teaching Toyota's philosophy and processes to its suppliers, Toyota developed more consistent practices among their disparate supply chain and identified threats before realizing those risks upstream.

Reasons why ZT-CCE implications from downstream suppliers matter include, but are not limited to:

- Software Bill of Materials (SBOM) security concerns (e.g., insecure protocols)
- Hardware Bill of Materials (HBOM) security concerns (e.g., alternate computer chips due to supply constraints)
- Covered telecommunications equipment or services (e.g., FAR 52.204-25 violation[6])
- Foreign ownership or knowledge-sharing agreements (e.g., intellectual property theft)
- Cross-border data transmission, processing and/or storage (e.g., compliance violation)
- Insecure data governance practices (e.g., compliance violation)
- Data sovereignty (data localization) requirements (e.g., compliance violation)

[6] *FAR52.204-25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment - https://www.acquisition.gov/far/52.204-25*