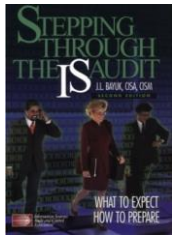
Stepping Through Cybersecurity Risk Management

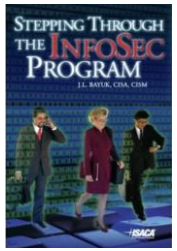
a systems-thinking approach

February 21, 2024

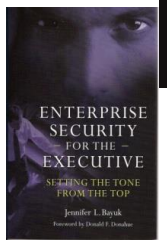
Introduction



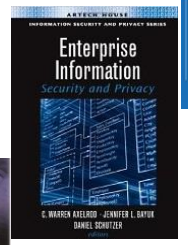
2004



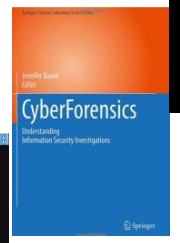
2007



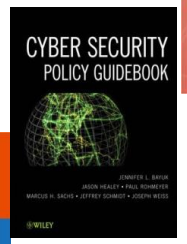
2009



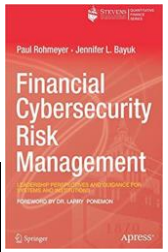
2009



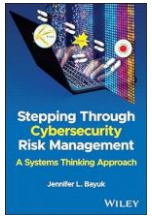
2010



2012



2019



2024

President & CEO
Decision Framework Systems, Inc.

Managing Director, Cybersecurity Risk
JPMorgan Chase

Managing Director, Enterprise Risk
Citi

Independent Technology
Risk Management Consultant

Associate Professor
Stevens Institute of Technology

Senior Managing Director, CISO
Bear Stearns, Inc.

Manager, IS Business Controls
AT&T Capital Corporation

Information Systems Risk Manager
Price Waterhouse

Member of Technical Staff
AT&T Bell Laboratories

PhD Systems Engineering,
Stevens Institute of Technology

Certified Information Systems
Security Professional (CISSP)

Certified in the Governance
of Enterprise IT (CGEIT)

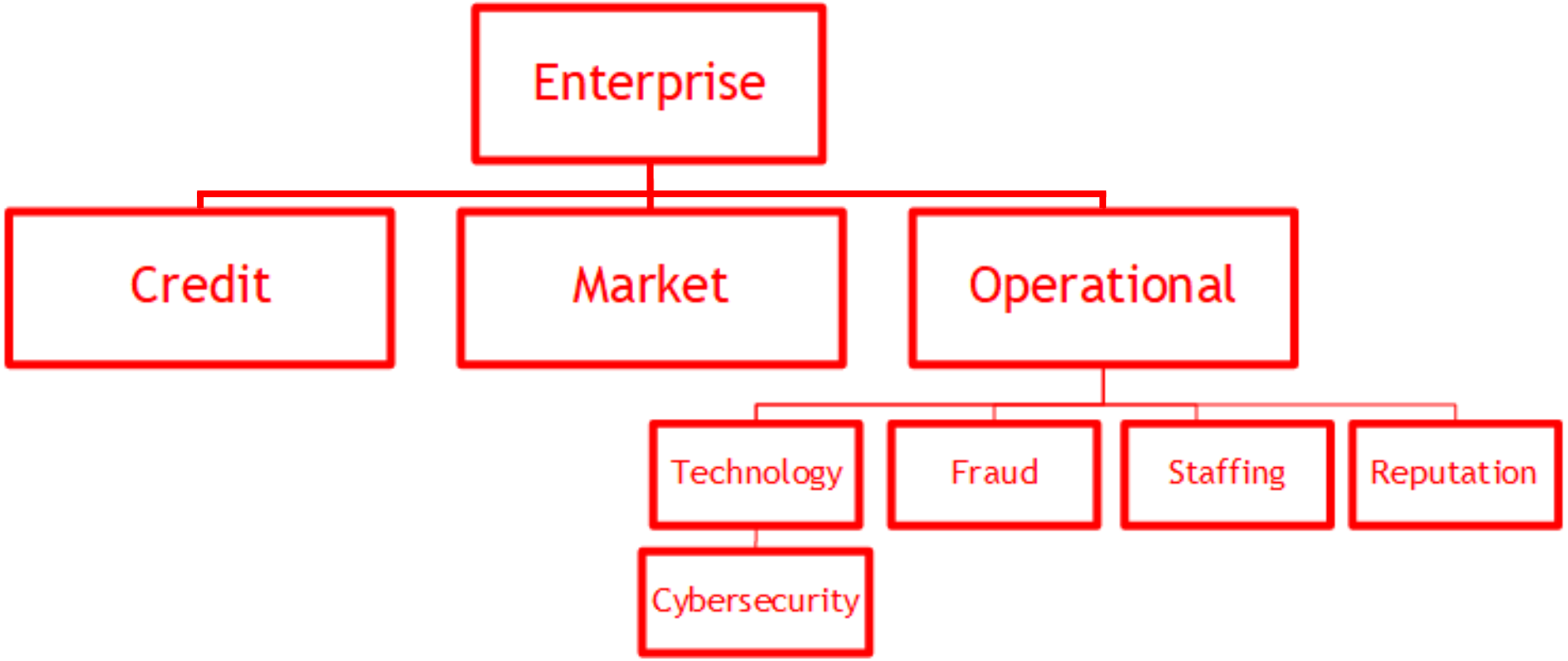
Certified Information Security Manager (CISM)

Certified Information Systems Auditor (CISA)

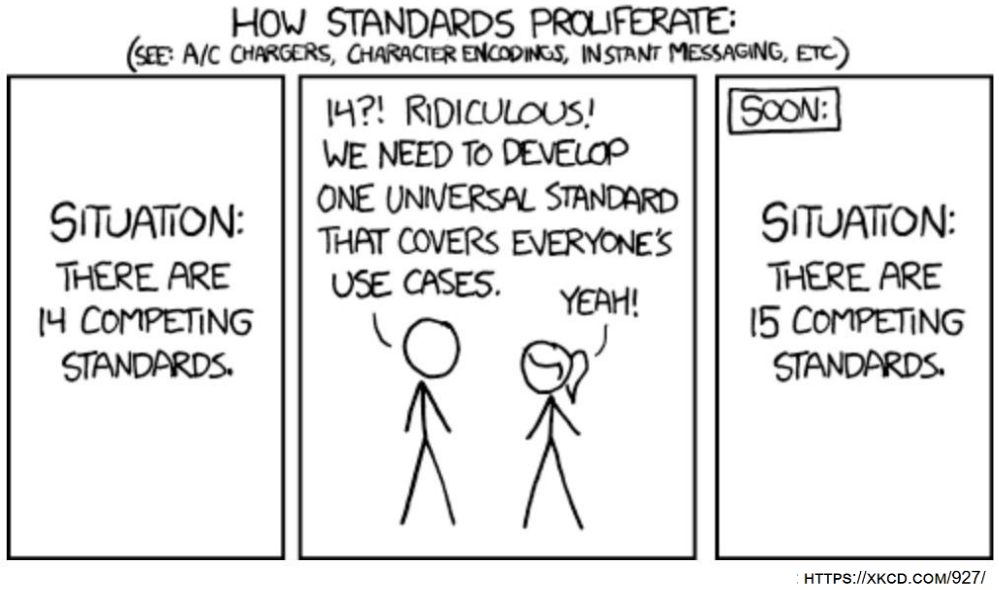
MS Computer Science, Stevens Institute of Technology

BA Computer Science & Philosophy, Rutgers College, Rutgers University

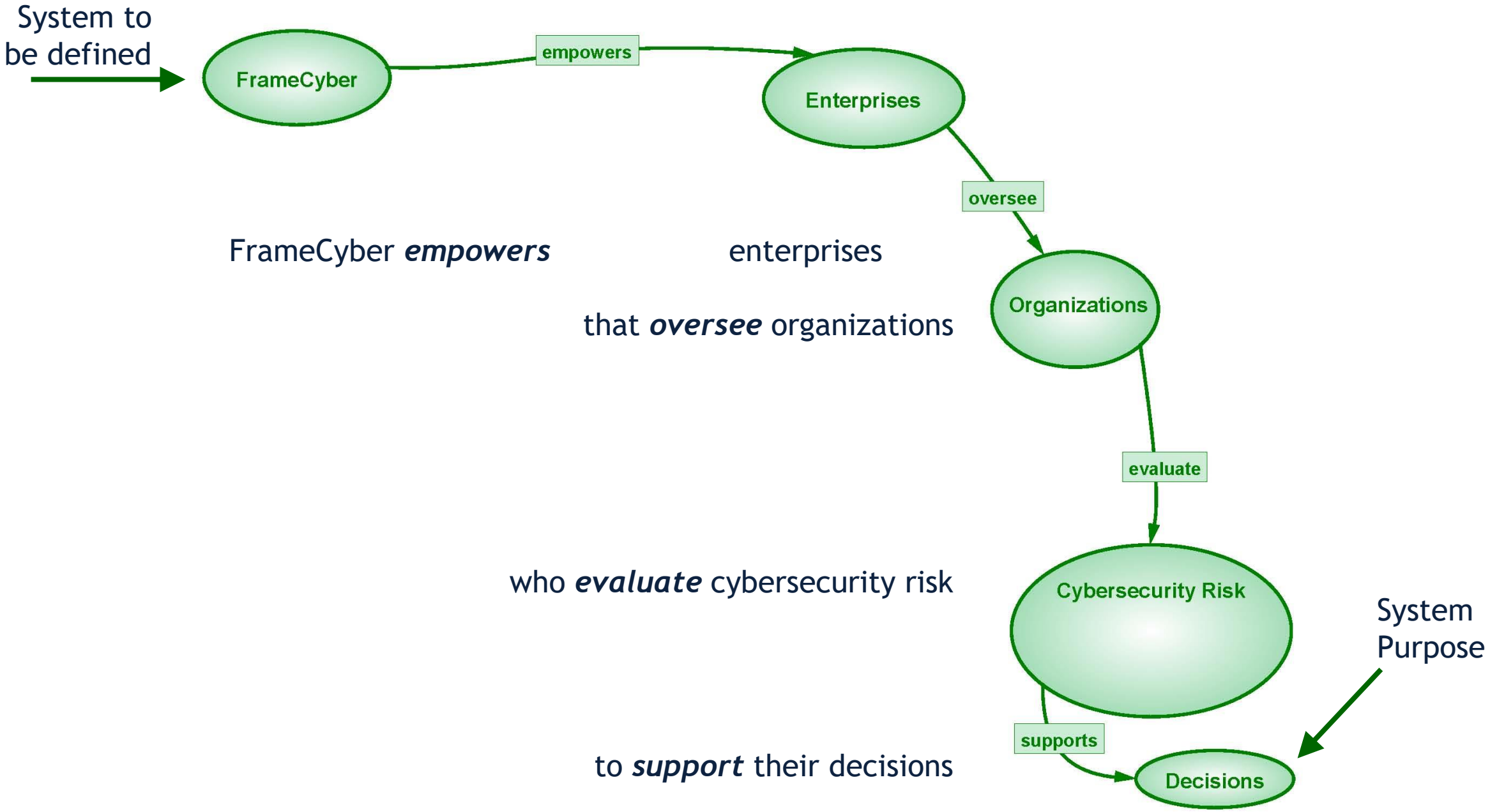
Enterprise Risk Hierarchy



FrameCyber® simplifies cybersecurity risk management *so you can focus on your cybersecurity risk profile!*



FrameCyber® is not a new standard, it is a *framework* of *Information and Logic for Cybersecurity Decision Support*



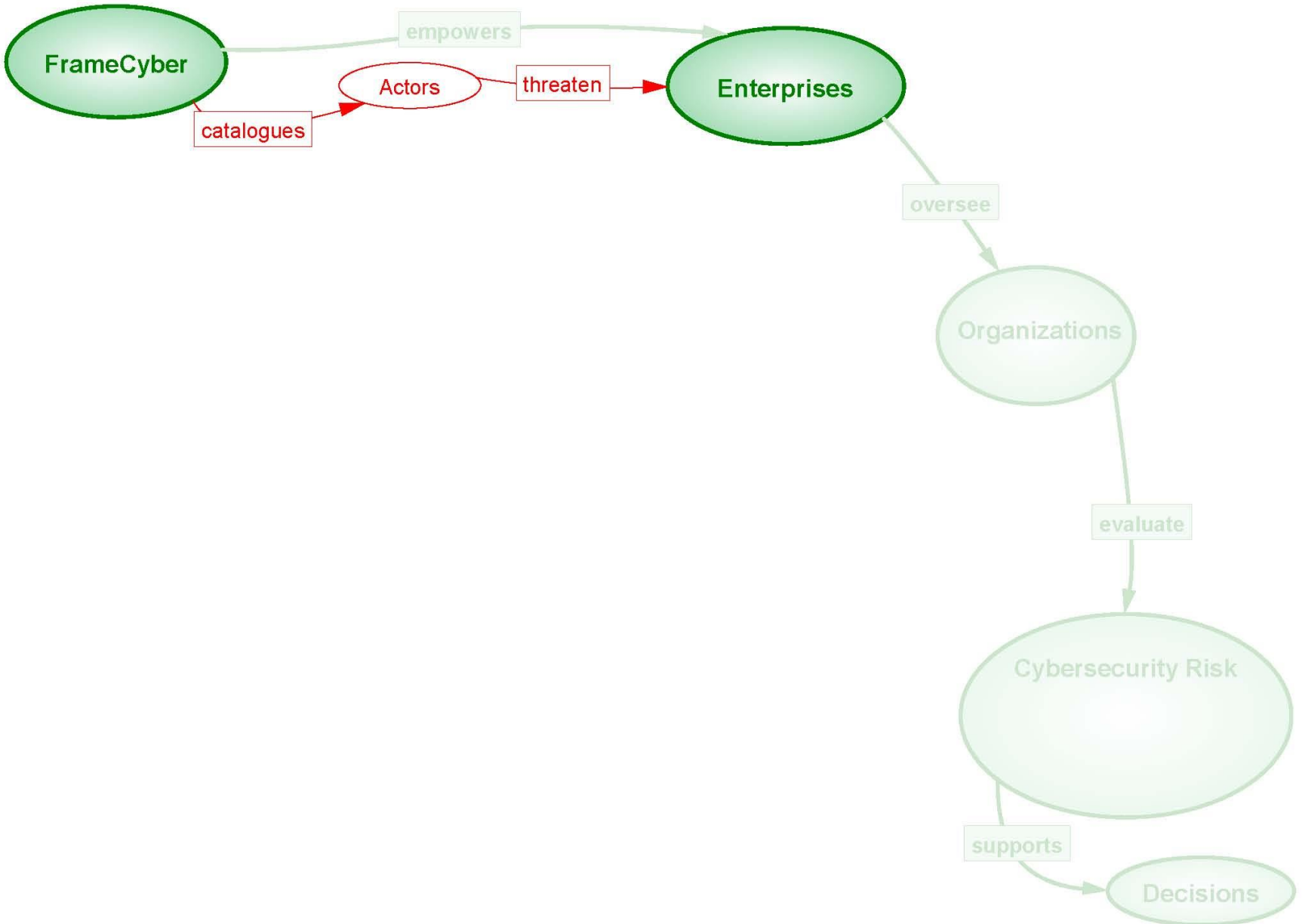
FrameCyber ***empowers*** enterprises

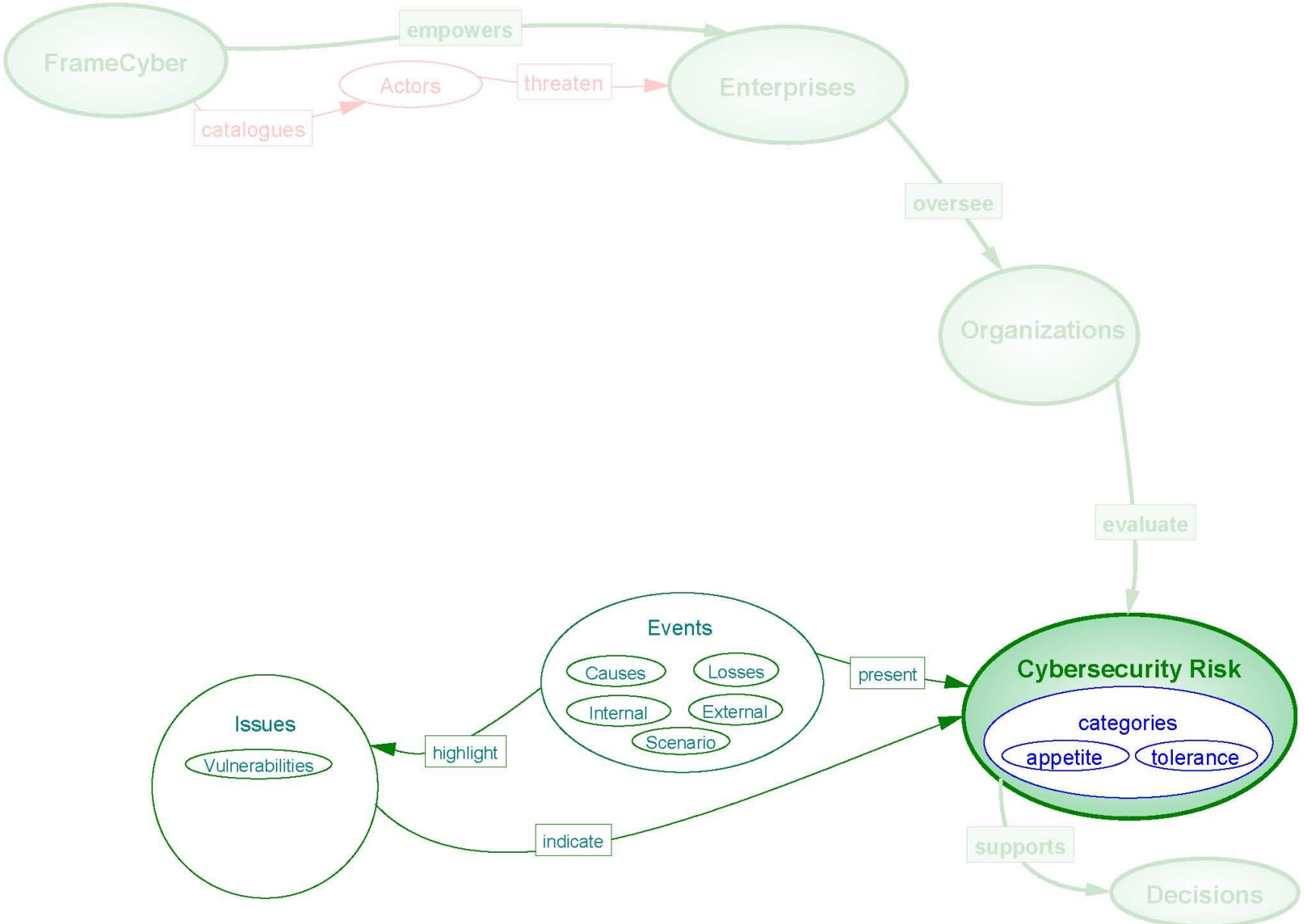
that ***oversee*** organizations

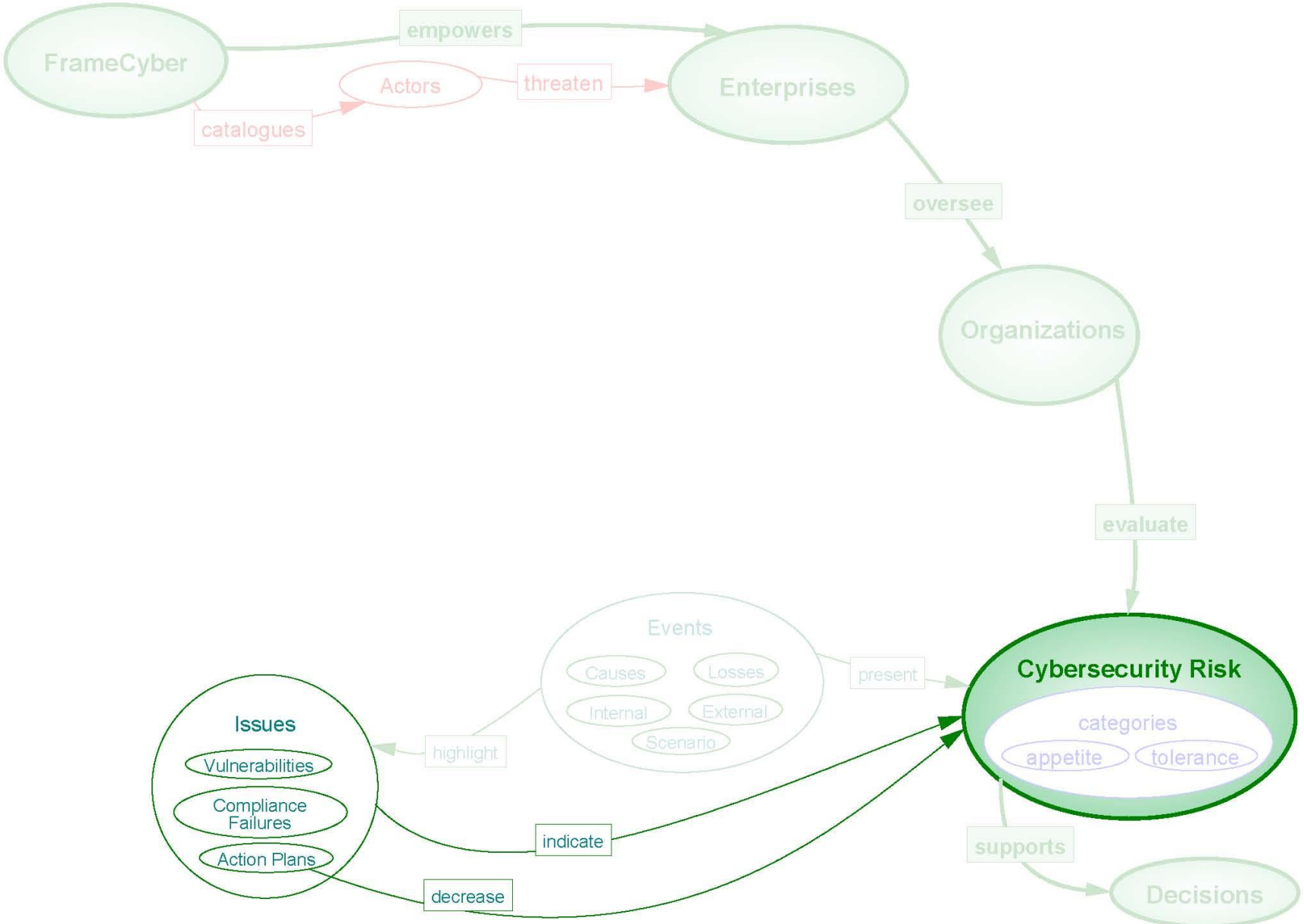
who ***evaluate*** cybersecurity risk

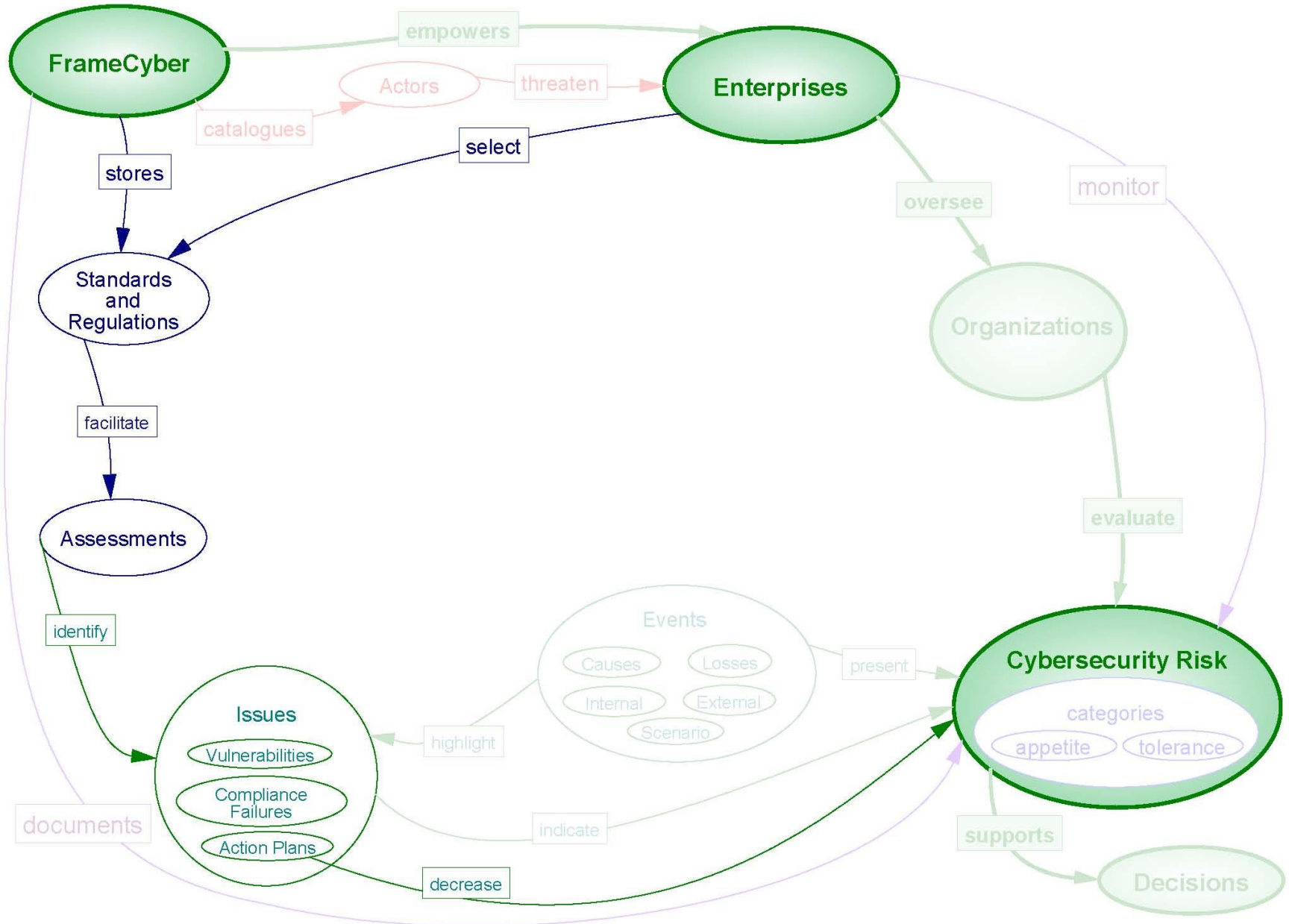
to ***support*** their decisions

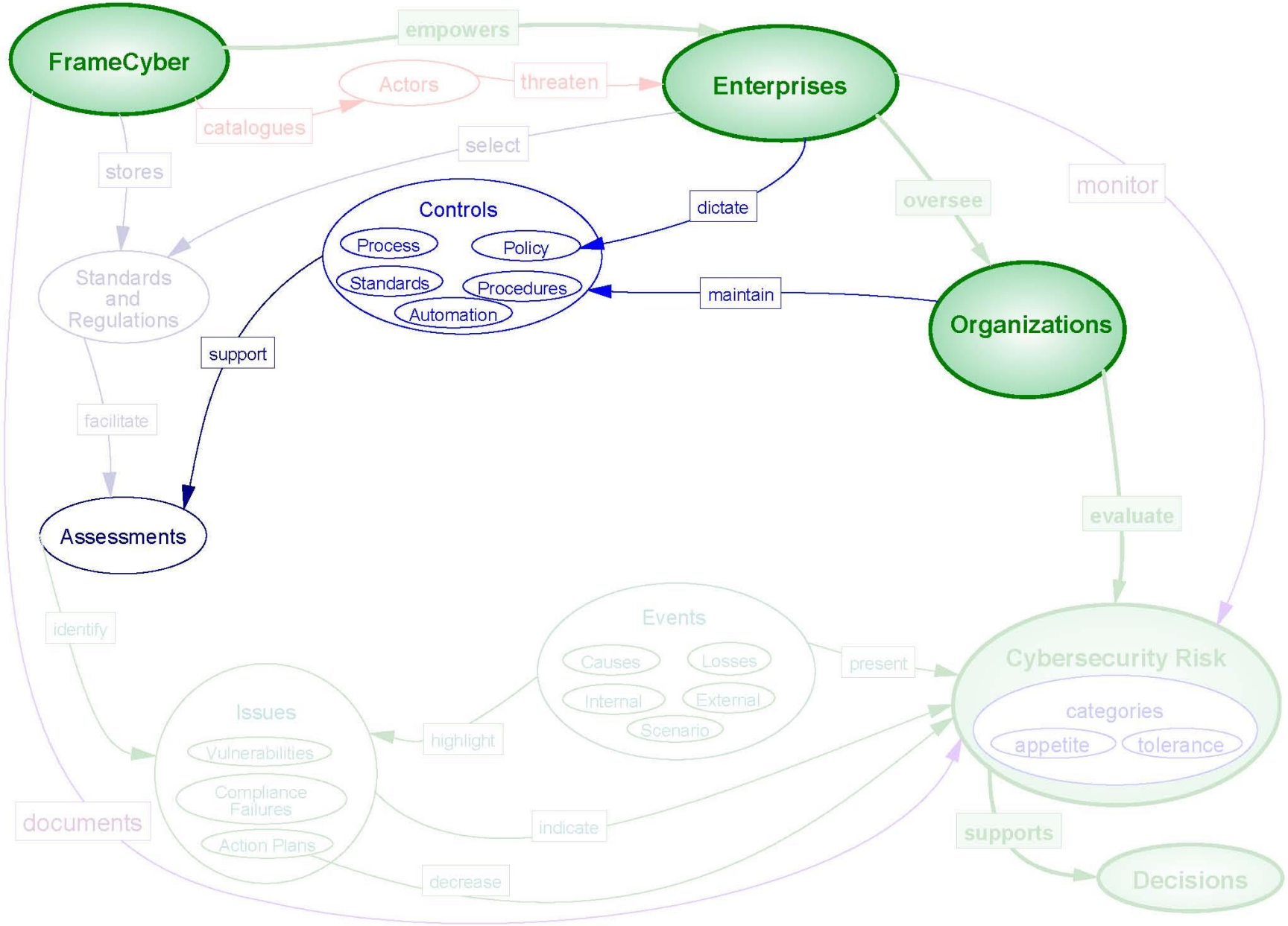
Most figures sourced from: Bayuk, Stepping Through Cybersecurity Risk Management, Wiley 2024

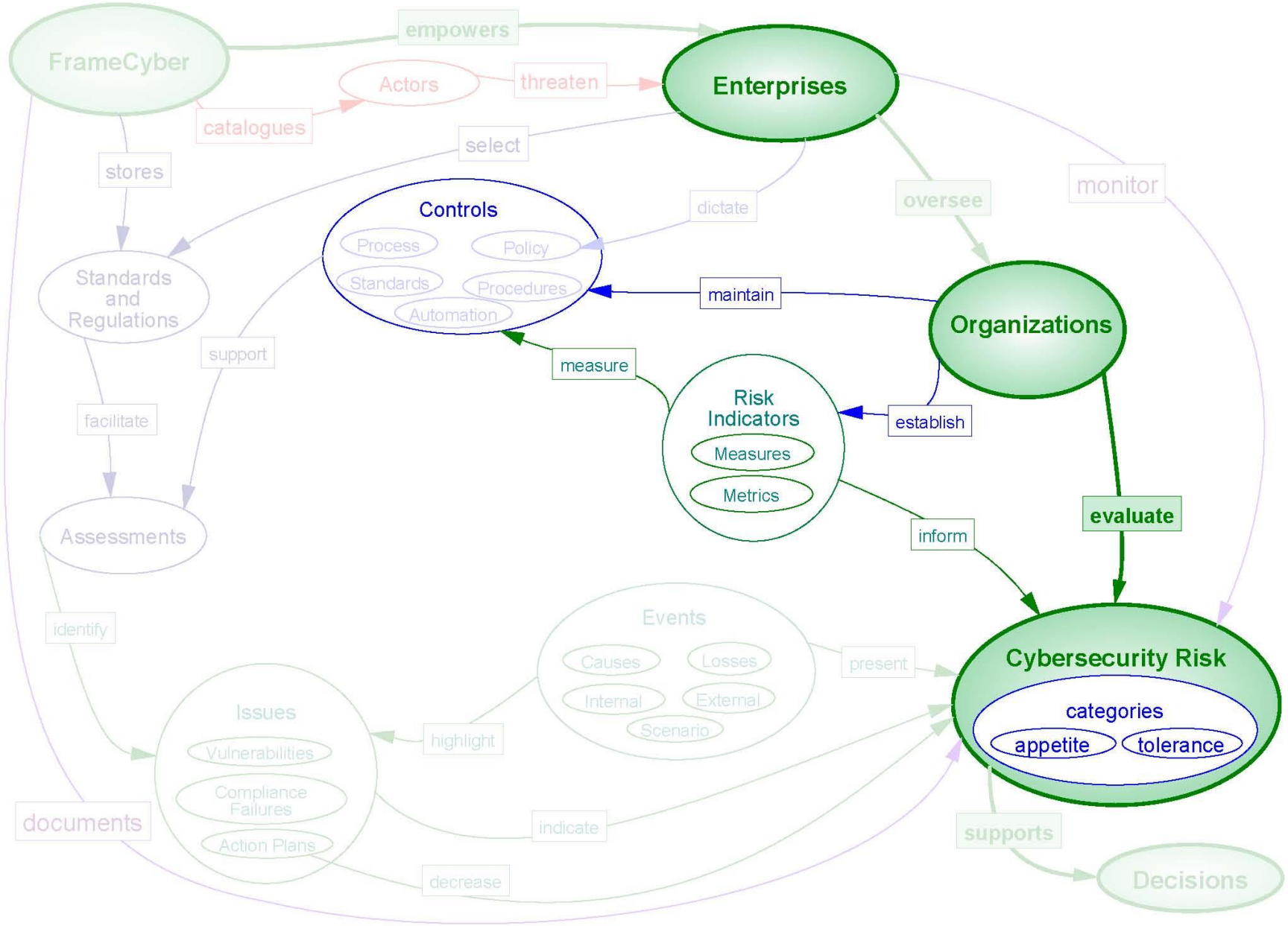

FrameCyber
empowers
Enterprises
Actors
threaten
catalogues
oversee
Organizations
evaluate
Cybersecurity Risk
supports
Decisions

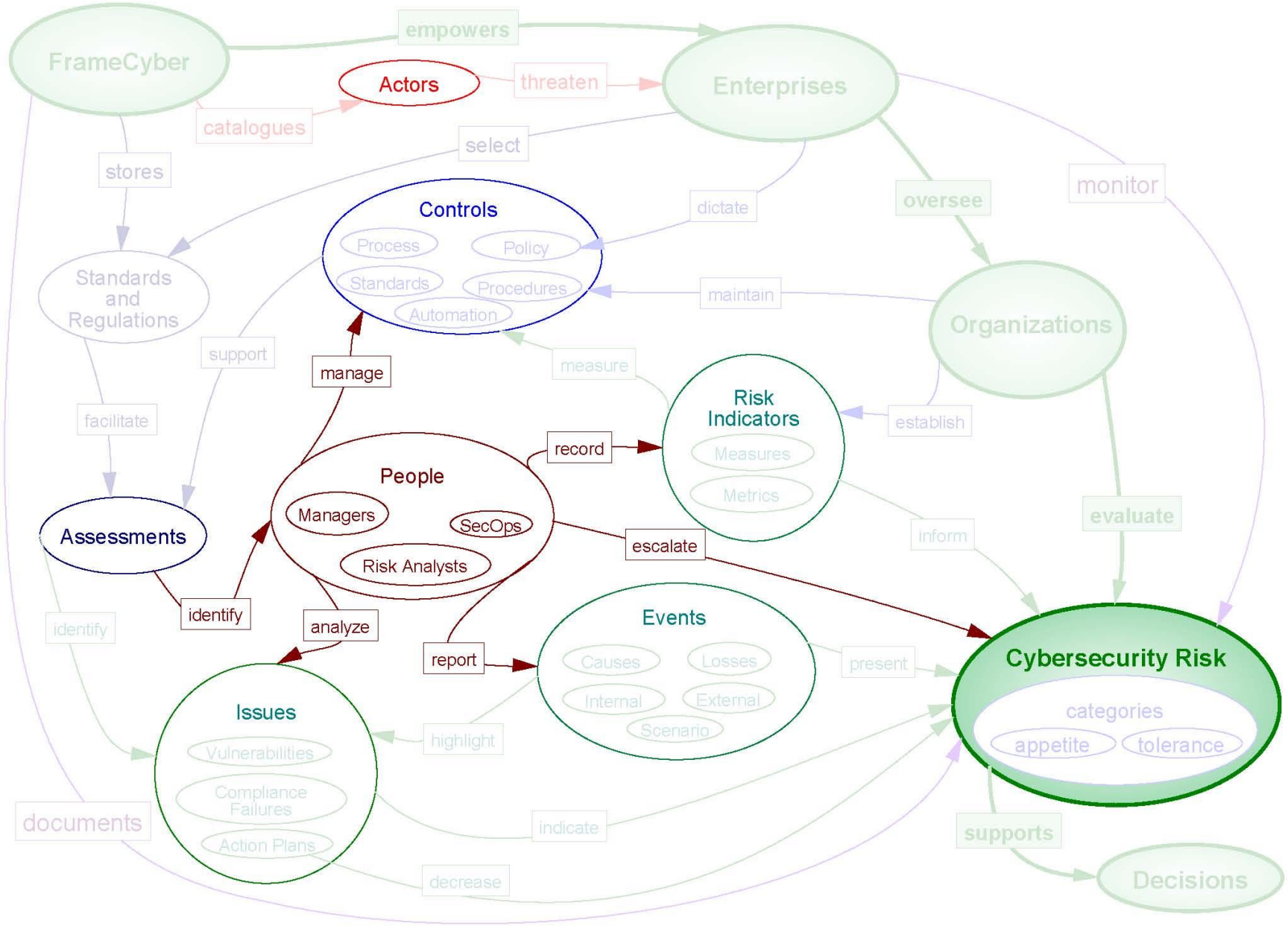

FrameCyber
empowers
Actors
threaten
Enterprises
catalogues
oversee
Organizations
evaluate
Events
Causes
Losses
Internal
External
Scenario
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
Vulnerabilities
highlight
indicate
supports
Decisions

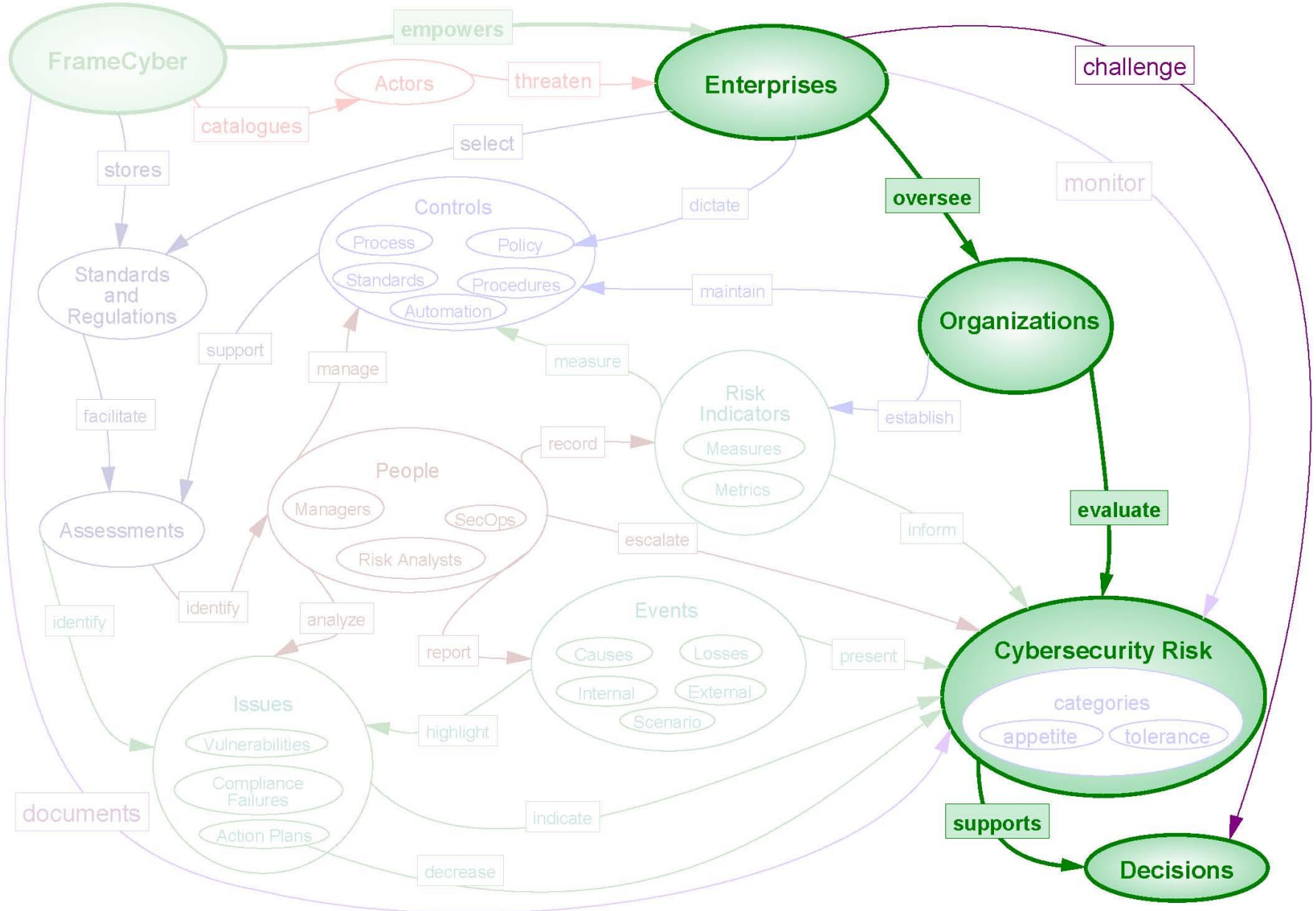

FrameCyber
empowers
Actors
threaten
Enterprises
catalogues
oversee
Organizations
evaluate
Events
Causes
Losses
Internal
External
Scenario
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
Vulnerabilities
Compliance Failures
Action Plans
highlight
indicate
decrease
supports
Decisions

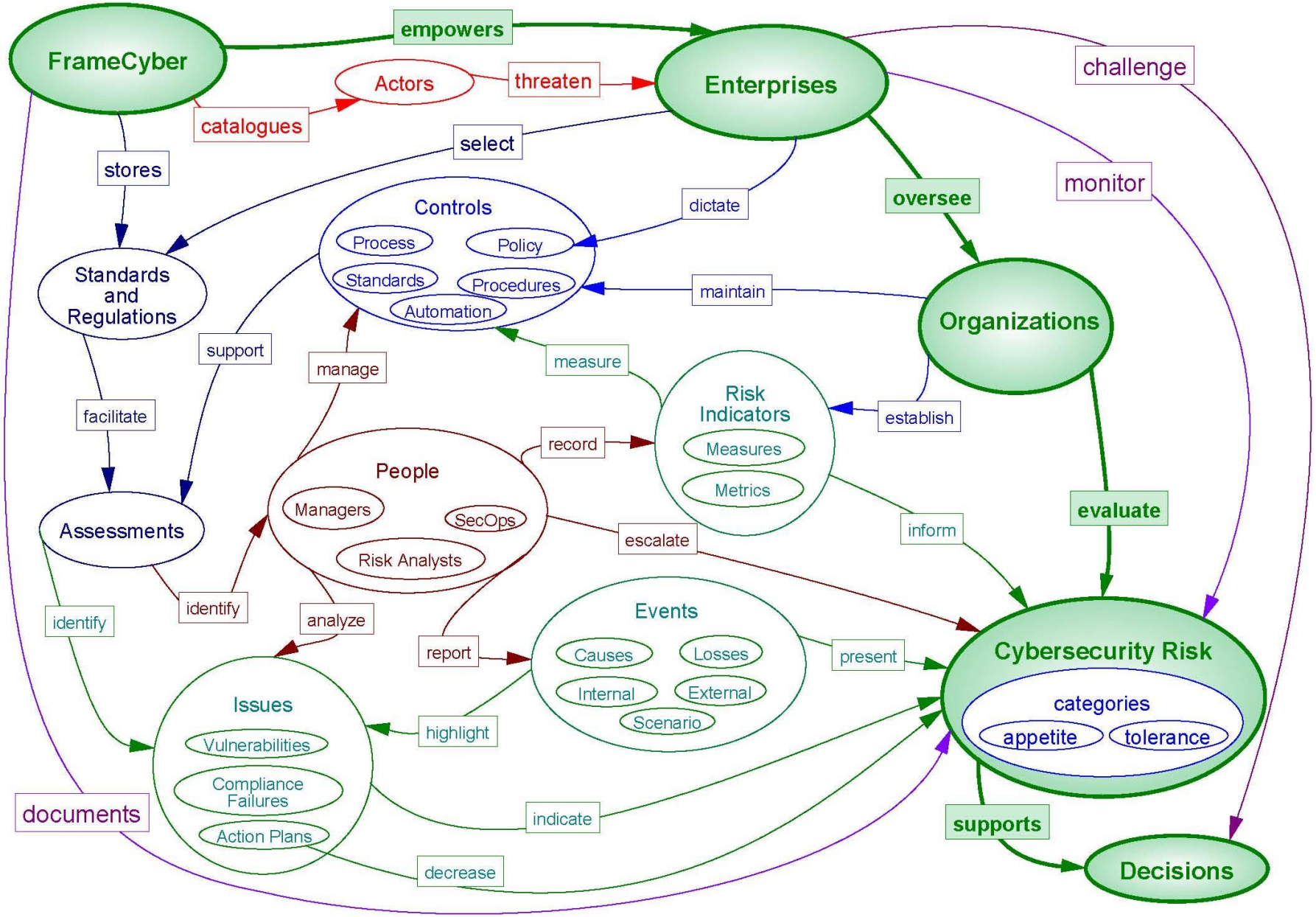

FrameCyber
empowers
Enterprises
Actors
threaten
catalogues
select
stores
Standards and Regulations
oversee
monitor
Organizations
facilitate
Assessments
evaluate
identify
Events
Causes
Losses
present
Cybersecurity Risk
Internal
External
Scenario
categories
appetite
tolerance
Issues
highlight
Vulnerabilities
Compliance Failures
Action Plans
indicate
documents
supports
decrease
Decisions


FrameCyber
empowers
Enterprises
Actors
threaten
catalogues
select
stores
Controls
Process
Policy
Standards
Procedures
Automation
dictate
oversee
monitor
Standards and Regulations
maintain
Organizations
support
facilitate
Assessments
evaluate
identify
Events
Causes
Losses
Internal
External
Scenario
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
Vulnerabilities
Compliance Failures
Action Plans
highlight
documents
indicate
supports
decrease
Decisions


FrameCyber
empowers
Enterprises
Actors
threaten
catalogues
select
stores
monitor
oversee
Controls
Process
Policy
Standards
Procedures
Automation
dictate
Standards and Regulations
maintain
Organizations
support
measure
Risk Indicators
Measures
Metrics
establish
facilitate
evaluate
Assessments
inform
identify
Events
Causes
Losses
Internal
External
Scenario
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
Vulnerabilities
Compliance Failures
Action Plans
highlight
documents
indicate
supports
decrease
Decisions


FrameCyber
empowers
Actors
threaten
Enterprises
catalogues
select
stores
monitor
oversee
Controls
Process
Policy
Standards
Procedures
Automation
dictate
Standards and Regulations
maintain
Organizations
support
manage
measure
facilitate
Risk Indicators
establish
People
record
Managers
SecOps
Risk Analysts
Measures
Metrics
evaluate
Assessments
escalate
inform
identify
identify
analyze
Events
report
Causes
Losses
Internal
External
Scenario
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
highlight
Vulnerabilities
Compliance Failures
Action Plans
indicate
documents
supports
decrease
Decisions


FrameCyber
empowers
Actors
threaten
Enterprises
challenge
catalogues
select
stores
monitor
oversee
Controls
dictate
Process
Policy
Standards
Procedures
Automation
Standards and Regulations
maintain
Organizations
support
manage
measure
Risk Indicators
facilitate
establish
record
People
Measures
Metrics
Managers
SecOps
evaluate
Assessments
inform
escalate
Risk Analysts
identify
identify
analyze
Events
Cybersecurity Risk
report
Causes
Losses
present
categories
Internal
External
Issues
appetite
tolerance
Scenario
highlight
Vulnerabilities
Compliance Failures
documents
indicate
supports
Action Plans
decrease
Decisions


FrameCyber
empowers
Enterprises
challenge
Actors
threaten
catalogues
select
stores
monitor
oversee
Controls
Process
Policy
Standards
Procedures
Automation
dictate
Standards and Regulations
maintain
Organizations
support
manage
measure
facilitate
Risk Indicators
Measures
Metrics
establish
record
People
Managers
SecOps
Risk Analysts
Assessments
evaluate
inform
escalate
identify
identify
analyze
Events
Causes
Losses
Internal
External
Scenario
report
present
Cybersecurity Risk
categories
appetite
tolerance
Issues
Vulnerabilities
Compliance Failures
Action Plans
highlight
documents
indicate
supports
decrease
Decisions

Cybersecurity Threats

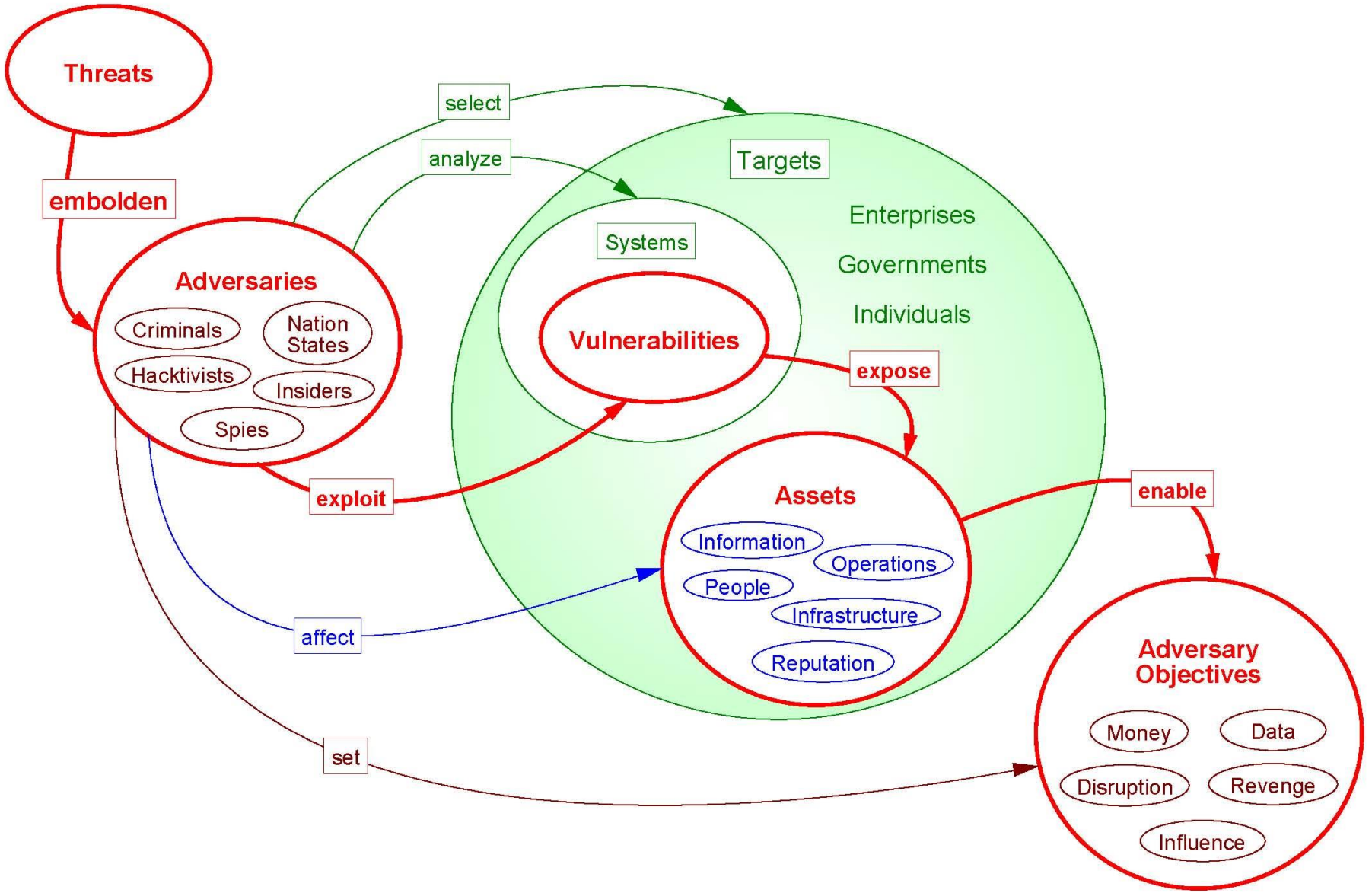
“If you know the enemy and know yourself,
you need not fear the result of a hundred battles.

If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself,
you will succumb in every battle.”

— Sun Tzu, The Art of War

Threat Intelligence



Threat Intelligence → Threat Catalog Entry

ID: APT-IS

Type: Nation-state

Role: Intrastructure-operator

Level: Innovator

Name: Indrik Spider

Geolocation: Russia

Aliases: Gold Drake, Evil Corp, Manatee Tempe

Description:

Indrik Spider has maintained criminal operations since at least 2014 when it is known to have used phishing techniques to persuade users to download compressed macros that, when activated, retrieved, and installed malware which infiltrated browsers and collected bank login credentials. In 2017, Indrik Spider began to operate ransomware. They exploit a wide variety of Windows vulnerabilities and target the financial industry avoiding detection via multi-stage persistence and installation processes in combination with code-obfuscation.

Tactics:

Among other phishing lures, Indrik Spider delivers fake browser updates to deliver malicious executables that, when activated, phone home with results. Once a foothold is established, it scans and traverses the network in search of an application data folder as a user with sufficient permissions to encrypt accessible file shares, deploying ransomware via PowerShell GPO. It sends a ransom note directing victims to TOR. In the process, it may exfiltrate information that can be directly exploited for financial gain.

Skills:

The organization is staffed with phishing, programming, and vulnerability exploitation expertise, as well ransomware programming and packaging in PowerShell and JavaScript. It has demonstrated competence in Windows operating system manipulation, and is also skilled in the used of BitPaymer, Cobalt Strike, Dried, Empire, Mimikatz, PsExec, WastedLocker and wmic. The activities of this threat actor are not limited by technological expertise.

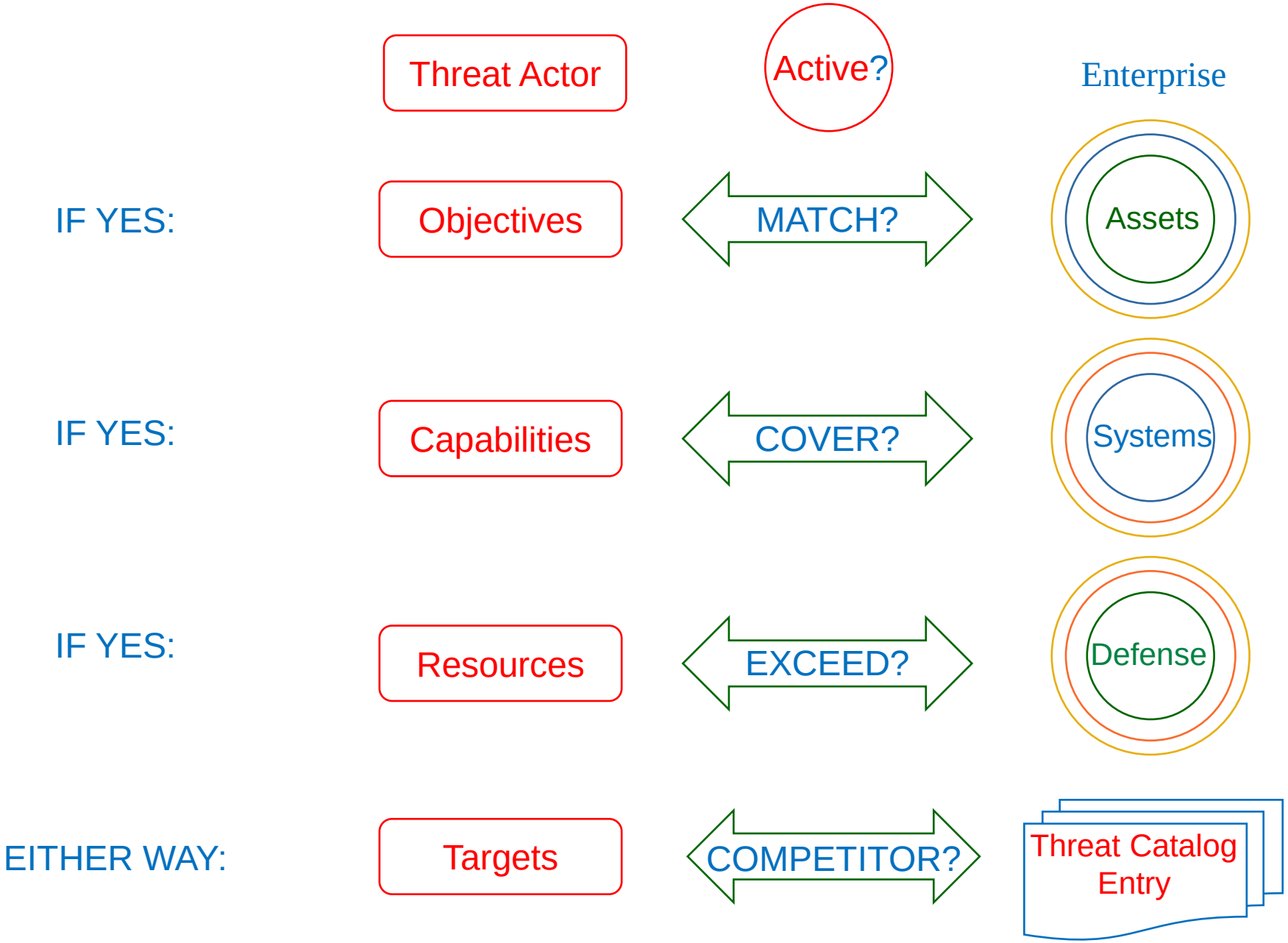
Goals:

Financial gain via credential hijacking or extortion from victims.

Resources:

Nationstate budget for this threat operation appears unlimited and its activities constantly add to its resources.

For each ***Threat Actor*** known to Threat Intelligence:



An ATT&CK Threat Vector Matrix

Initial Access → Execution → Persistence → Escalation → Evasion → Access → Discovery → Movement → Data → Commands → Exfiltration

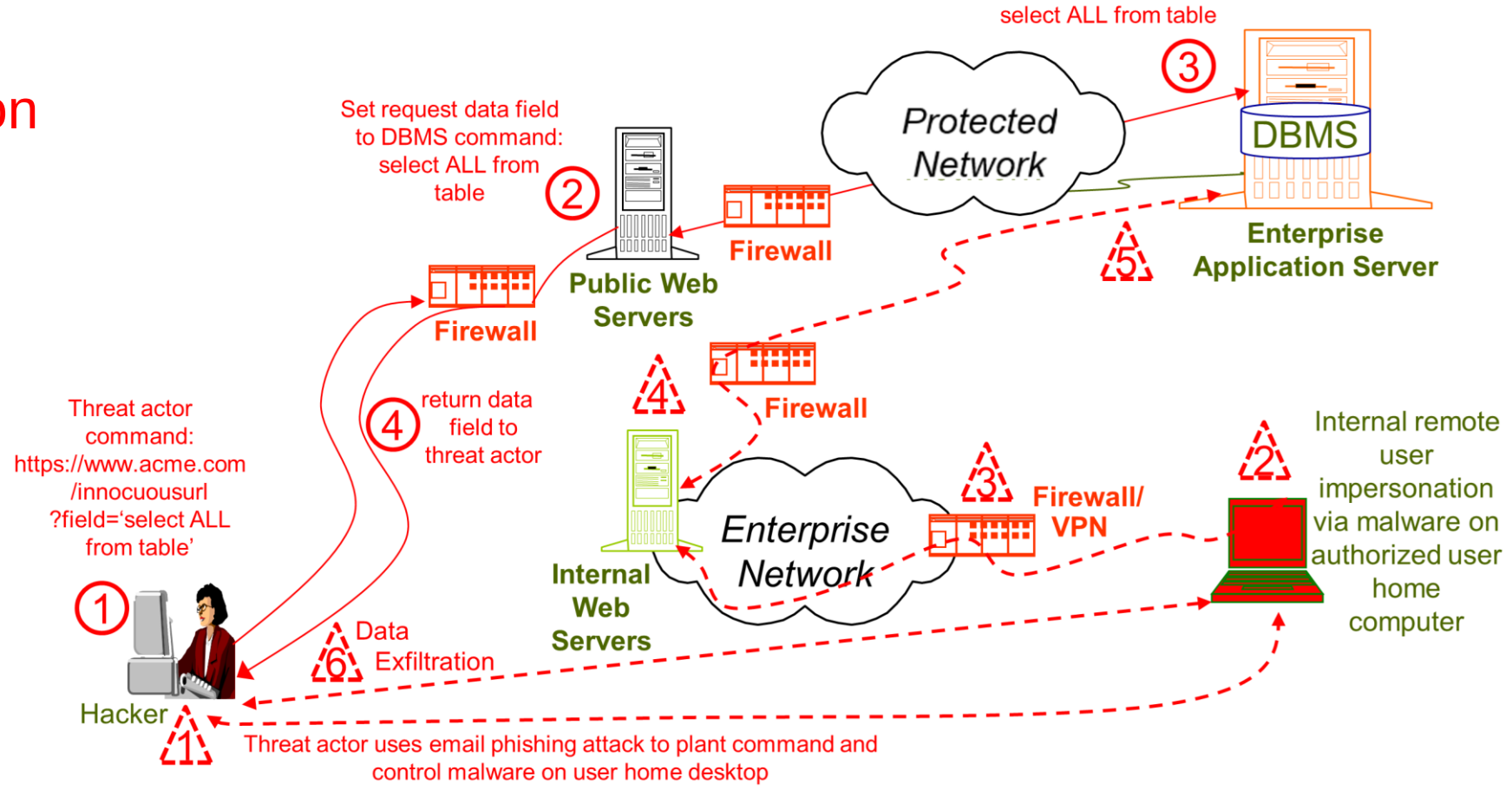
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Valid Accounts	Scheduled Task/Job	Valid Accounts	Valid Accounts	Modify Authentication Process	Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media	Windows Management Instrumentation	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Direct Volume Access	Input Capture	Replication Through Removable Media	Input Capture	Application Layer Protocol	Data Transfer Size Limits	Service Stop	
Supply Chain Compromise	Shared Modules	Create or Modify System Process	Create or Modify System Process	Rootkit	Brute Force	System Network Configuration Discovery	Internal Spearphishing	Data Staged	Communication Through Removable Media	Exfiltration Over C2 Channel	Inhibit System Recovery
Hardware Additions	User Execution	Event Triggered Execution	Event Triggered Execution	Obfuscated Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery	Use Alternate Authentication Material	Screen Capture	Web Service	Exfiltration Over Physical Medium	Defacement
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Process Injection	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer	Email Collection	Multi-Stage Channels	Exfiltration Over Alternative Protocol	Firmware Corruption
Phishing	System Services	Account Manipulation	Access Token Manipulation	Access Token Manipulation	Steal Web Session Cookie	Permission Groups Discovery	Taint Shared Content	Clipboard Data	Ingress Tool Transfer	Exfiltration Over Web Service	Resource Hijacking
External Remote Services	Command and Scripting Interpreter	External Remote Services	Group Policy Modification	Abuse Elevation Control Mechanism	Unsecured Credentials	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Data Encoding	Automated Exfiltration	Network Denial of Service
Drive-by Compromise	Native API	Office Application Startup	Exploitation for Privilege Escalation	Indicator Removal on Host	Credentials from Password Stores	Peripheral Device Discovery	Remote Service Session Hijacking	Audio Capture	Traffic Signaling	Exfiltration Over Physical Medium	Endpoint Denial of Service
	Inter-Process Communication	Create Account		Modify Registry	Steal or Forge Kerberos Tickets	Network Share Discovery		Video Capture	Remote Access Software	Transfer Data to Cloud Account	System Shutdown/Reboot
		Browser Extensions		Trusted Developer Utilities Proxy Execution	Steal Application Access Token	Password Policy Discovery		Man in the Browser	Dynamic Resolution		Account Access Removal
		Traffic Signaling		Traffic Signaling	Man-in-the-Middle	Browser Bookmark Discovery		Data from Information Repositories	Non-Standard Port		Disk Wipe
		BITS Jobs		Signed Script Proxy Execution	Forced Authentication	Virtualization/Sandbox Evasion		Man-in-the-Middle	Protocol Tunneling		Data Manipulation
		Server Software Component		Rogue Domain Controller		Cloud Service Dashboard		Archive Collected Data	Encrypted Channel		
		Pre-OS Boot		Indirect Command Execution		Software Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		
		Compromise Client Software Binary		BITS Jobs		Query Registry		Data from Cloud Storage Object			
		Implant Container Image		XSL Script Processing		Remote System Discovery					
				Template Injection		Network Service Scanning					
				File and Directory Permissions Modification		Process Discovery					
				Virtualization/Sandbox Evasion		System Information Discovery					
				Unused/Unsupported Cloud Regions		Account Discovery					
				Use Alternate Authentication Material		System Time Discovery					
				Impair Defenses		Domain Trust Discovery					
				Hide Artifacts		Cloud Service Discovery					
				Masquerading							
				Deobfuscate/Decode Files or Information							
				Signed Binary Proxy Execution							
				Exploitation for Defense Evasion							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

Legend	
	High Confidence of Detection
	Some Confidence of Detection
	Low Confidence of Detection

Source: attack.mitre.org/matrices/enterprise/

Common Attack Vectors

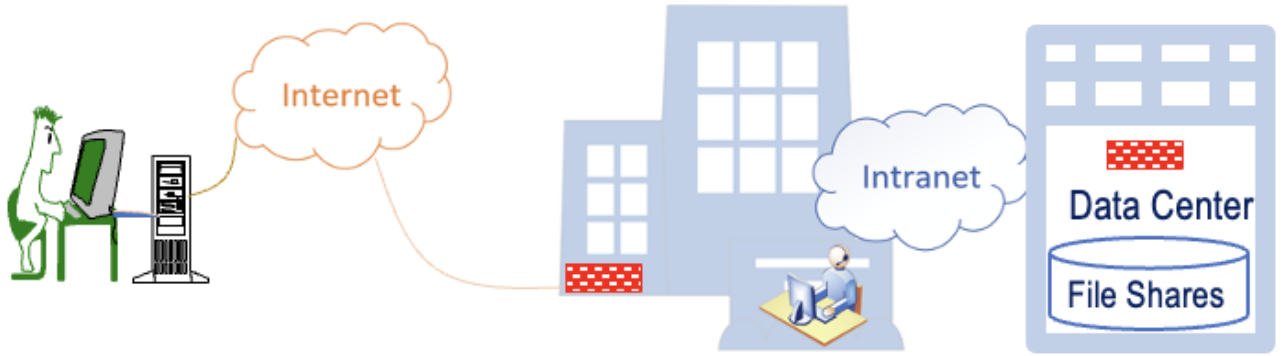
SQL Injection



1. Send Website malicious URL
2. Web Server executes DBMS command in URL
3. DBMS returns requested data
4. Website returns requested data

1. Send malicious URL to staff home
2. Staff unwittingly downloads and executes malware from URL
3. Piggyback on authorized user connection to VPN
4. Impersonate user on internal website and send malicious URL
5. Application returns data
6. Retrieve data from user home desktop

Hypothetical Events



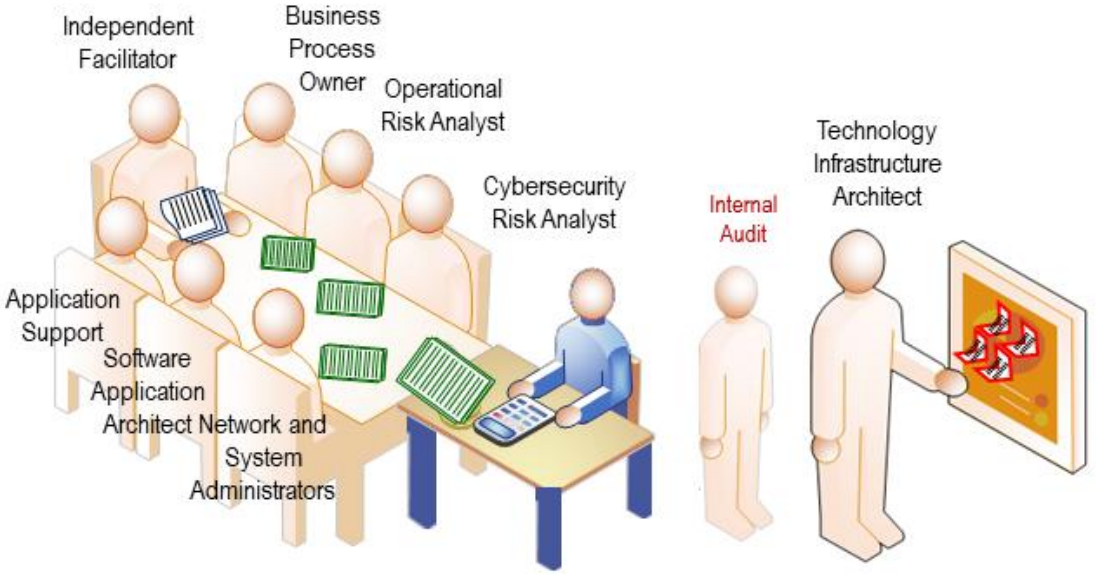
PHISHING

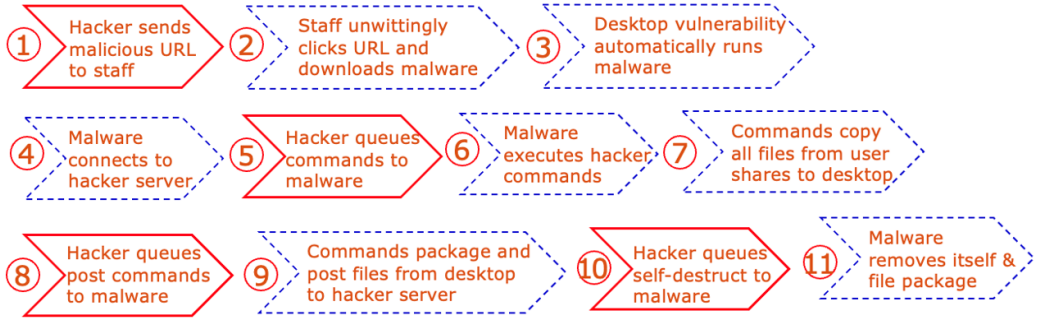
1. Hacker sends malicious URL to staff
2. Staff unwittingly clicks URL and downloads malware
3. Desktop vulnerability automatically runs malware
4. Malware connects to hacker server
5. Hacker queues commands to malware
6. Malware executes hacker commands
7. Commands copy all files from user shares to desktop
8. Hacker queues post commands to malware
9. Commands package and post files from desktop to hacker server
10. Hacker queues self-destruct to malware
11. Malware removes itself & file package

Hypothetical Events

Also known as *Cybersecurity Scenario Analysis.*

Outages	Minutes	Hour	Min	Avg Payment Fee	# Waived	Goodwill Loss
File Share 1 - Storage Only	21	0	21			
Payment Processing	22	0	22	$34.00	684	**$23,256.00**
General Ledger	823	13	43			
Payment Processing Full Recovery	184	3	4			
Lost Payments Recovered	446	7	26			
Technology Staff Expense				**Rate**	**# Staff**	**IT Expense**
Overtime Level 1	419	6	59	$50	2	$698.33
Overtime Level 2	42	0	42	$100	3	$210.00
Overtime Level 3	420	7	0	$200	2	$2,800.00
Forensics Team	35	0	35	$600		$350.00
						$4,058.33
					Total Loss:	**$27,314.33**

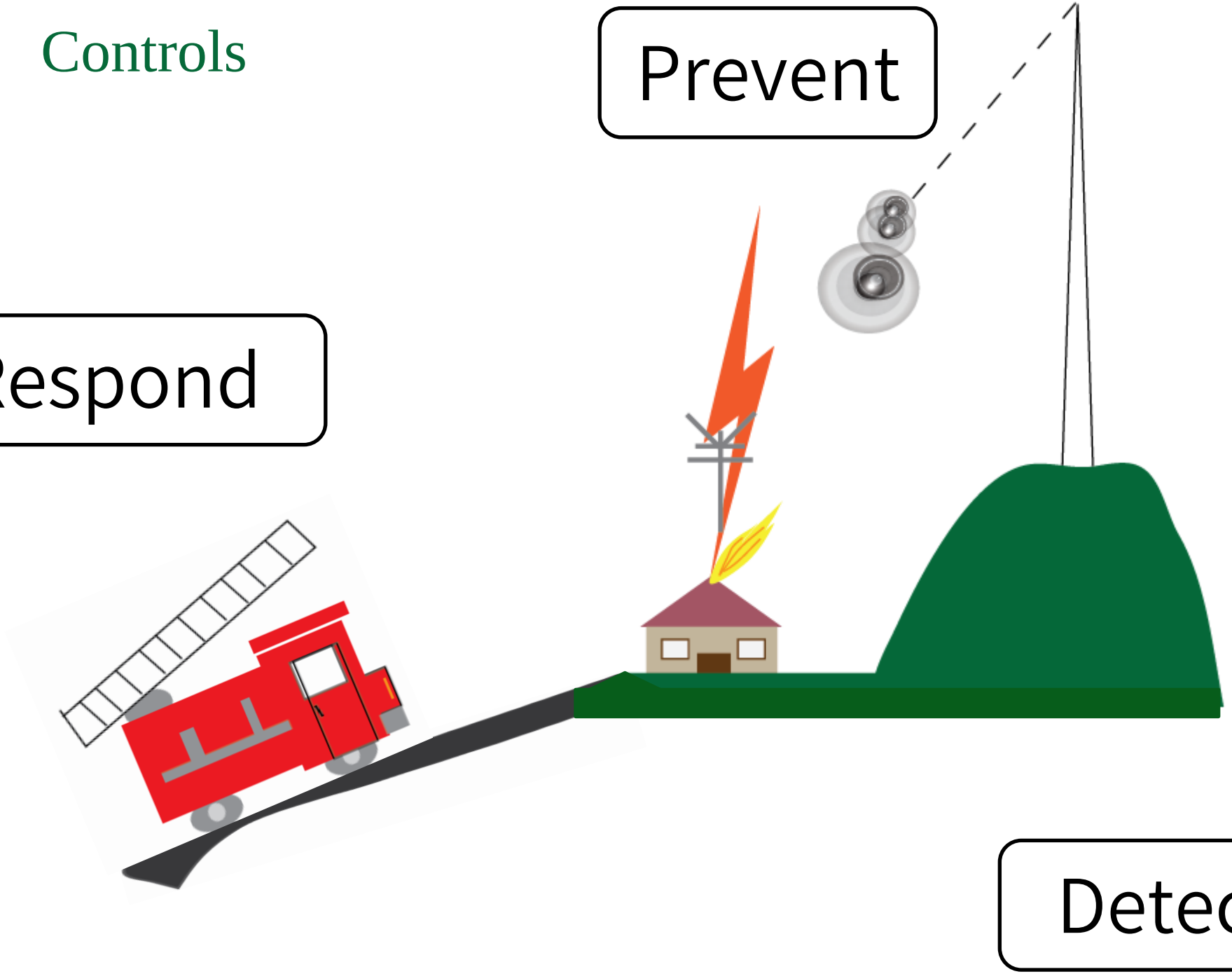




Controls

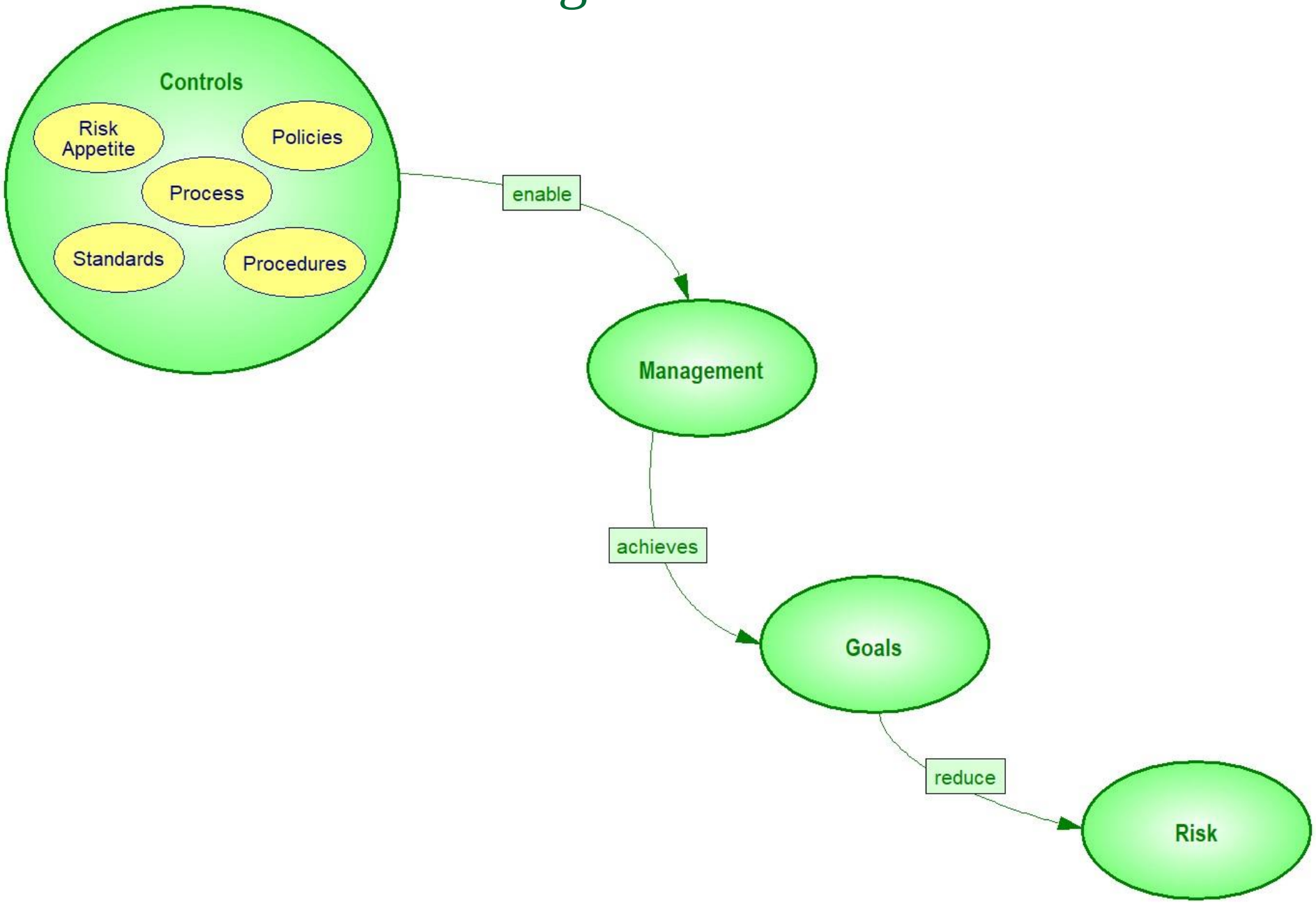
Prevent

Respond



Detect

Management Controls



Tone at the Top

CYBERSECURITY IS A MAJOR CONCERN.

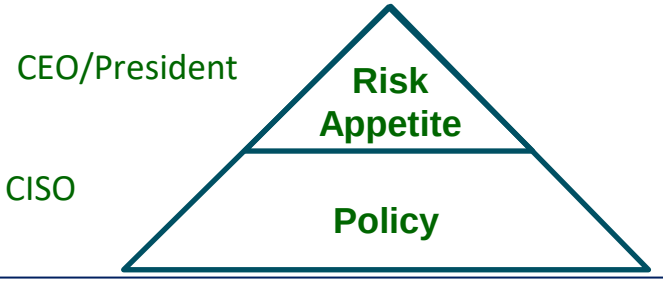
THE ENTERPRISE HAS NO TOLERANCE FOR KNOWN VULNERABILITIES IN ITS SYSTEMS, NO TOLERANCE FOR DATA BREACHES, AND LOW TOLERANCE FOR UNKNOWN VULNERABILITIES.

CEO/President

Tone at the Top

CYBERSECURITY IS A MAJOR CONCERN.

THE ENTERPRISE HAS NO TOLERANCE FOR KNOWN VULNERABILITIES IN ITS SYSTEMS, NO TOLERANCE FOR DATA BREACHES, AND LOW TOLERANCE FOR UNKNOWN VULNERABILITIES.



Section B: Authorized Use

B.1: Business Purpose

All information technology at Firm shall be associated with an "Application." The application is the business purpose of the technology that is recorded in Application Inventory.

B.2: Least Privilege

Where individuals require access to an organization's facilities, operational processes, technology systems, and information ("resources") in order to ensure the success of the enterprise mission, this access shall be:

(i) limited to least privilege with respect to the individual's function; and

(ii) provisioned only after receipt of a successful background check approved by Legal that may be customized for that function.

B.2.1: User Classification

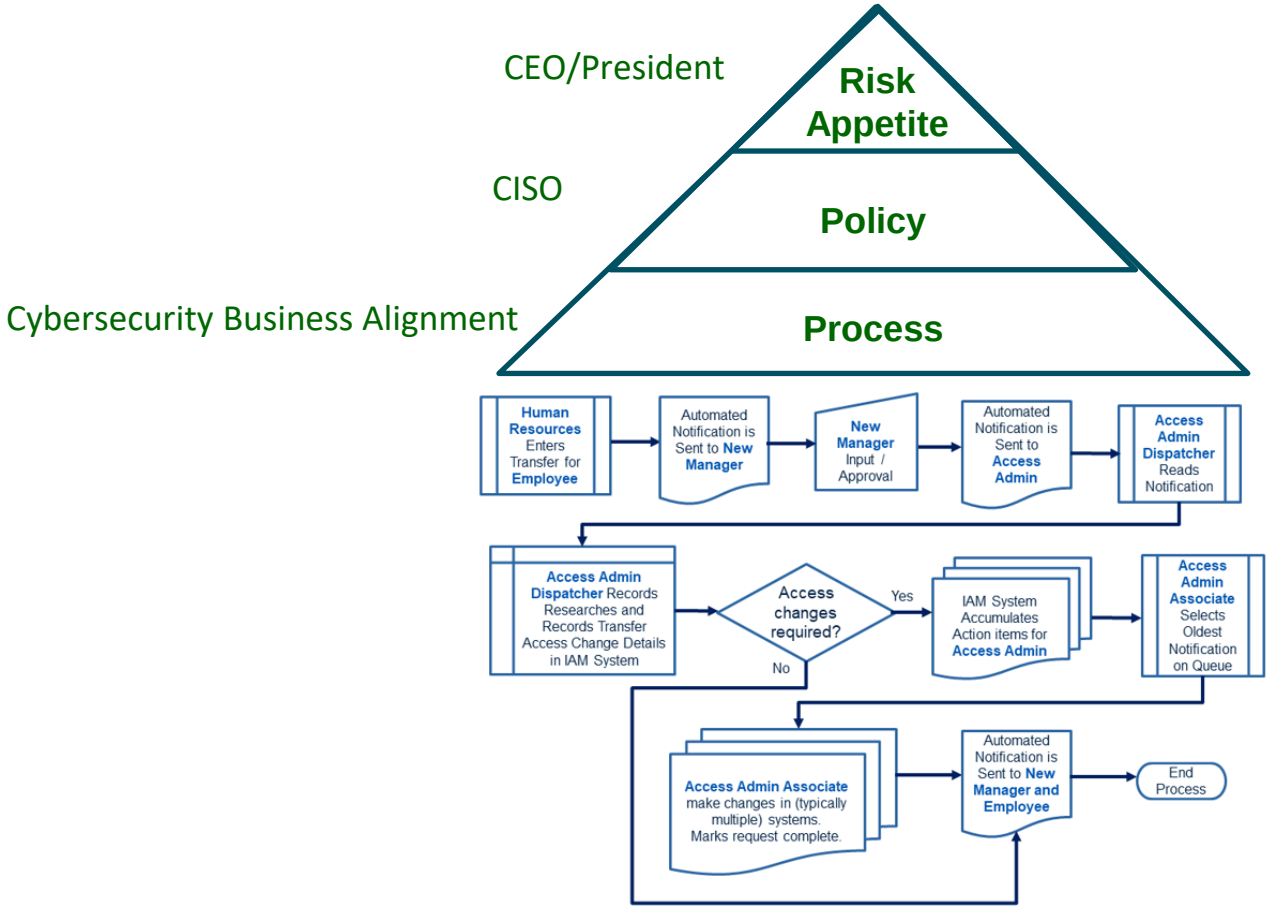
Responsibility for determining the minimum possible access requirements for an individual's function is allocated based on user classification. Individuals who do not have a business relationship with the enterprise that falls into a defined user classes shall have no authorized access and all individuals who are granted systems access shall endeavor to ensure that such unclassified individuals are unable to access enterprise resources that are not declared by Legal to be publicly accessible (e.g. advertising and corporate investor websites).

B.2.2: Departmental Responsibility

Tone at the Top

CYBERSECURITY IS A MAJOR CONCERN.

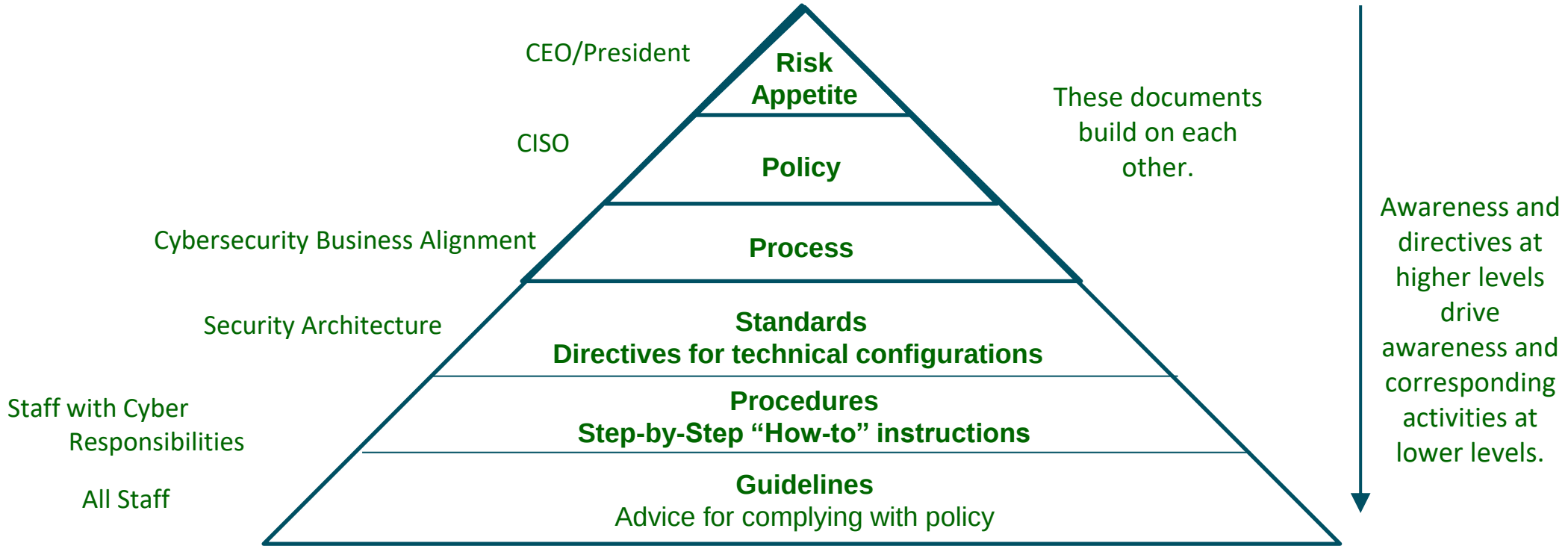
THE ENTERPRISE HAS NO TOLERANCE FOR KNOWN VULNERABILITIES IN ITS SYSTEMS, NO TOLERANCE FOR DATA BREACHES, AND LOW TOLERANCE FOR UNKNOWN VULNERABILITIES.



Tone at the Top

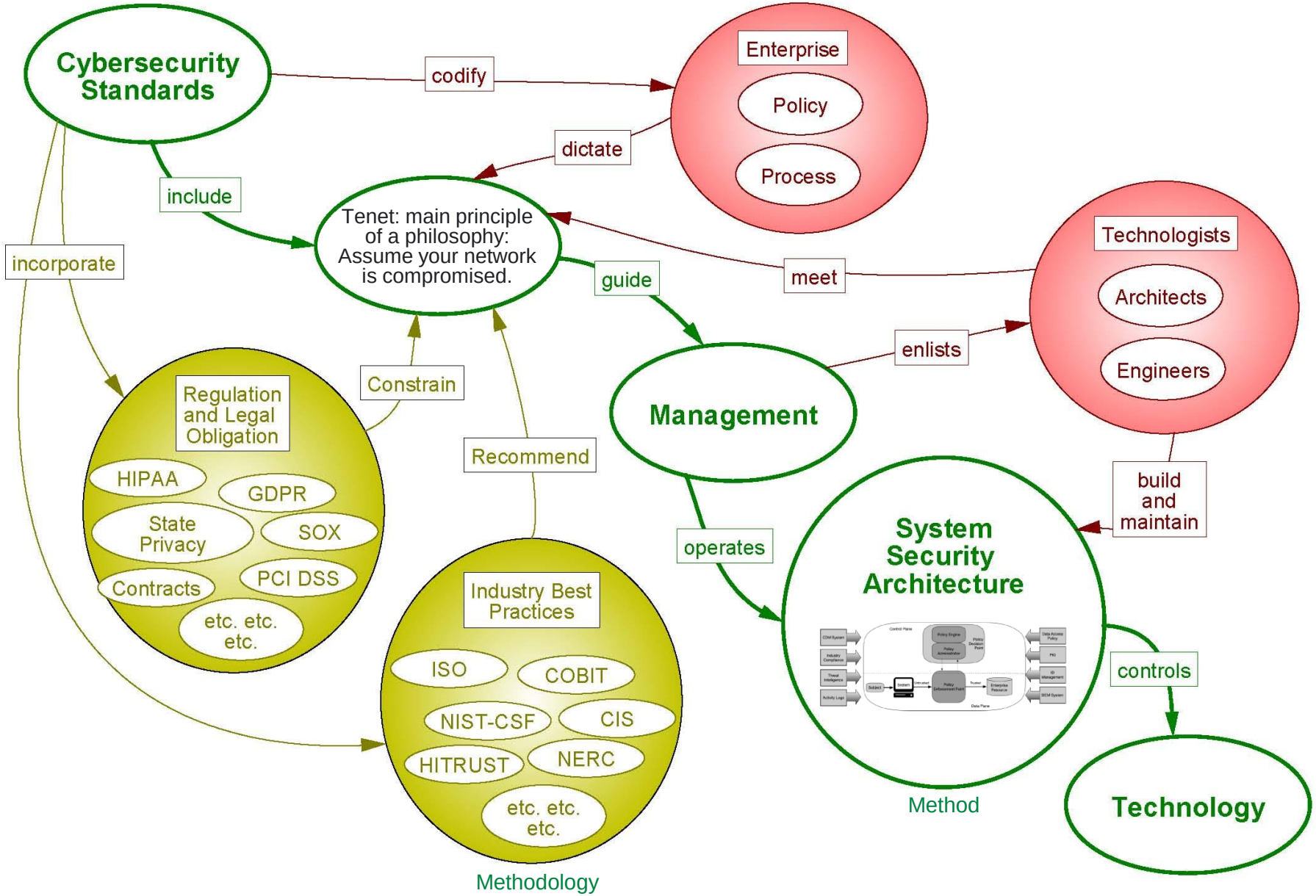
CYBERSECURITY IS A MAJOR CONCERN.

THE ENTERPRISE HAS NO TOLERANCE FOR KNOWN VULNERABILITIES IN ITS SYSTEMS, NO TOLERANCE FOR DATA BREACHES, AND LOW TOLERANCE FOR UNKNOWN VULNERABILITIES.



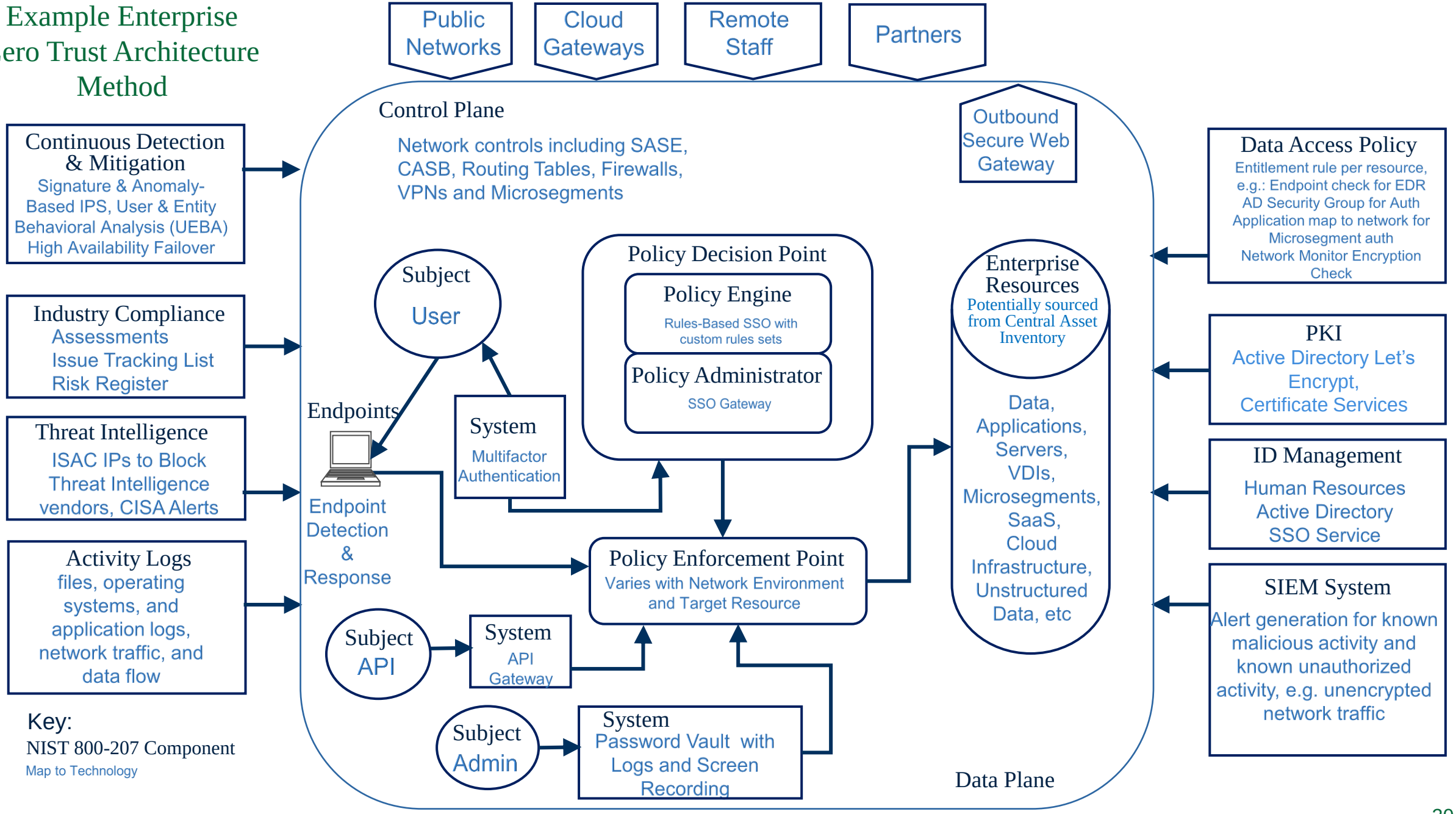
**Must also be consistent with legal obligations and contractual requirements!*

Enterprise Security Standards - Example Zero Trust Architecture



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Wiley 2024, ISBN: 9781394213955

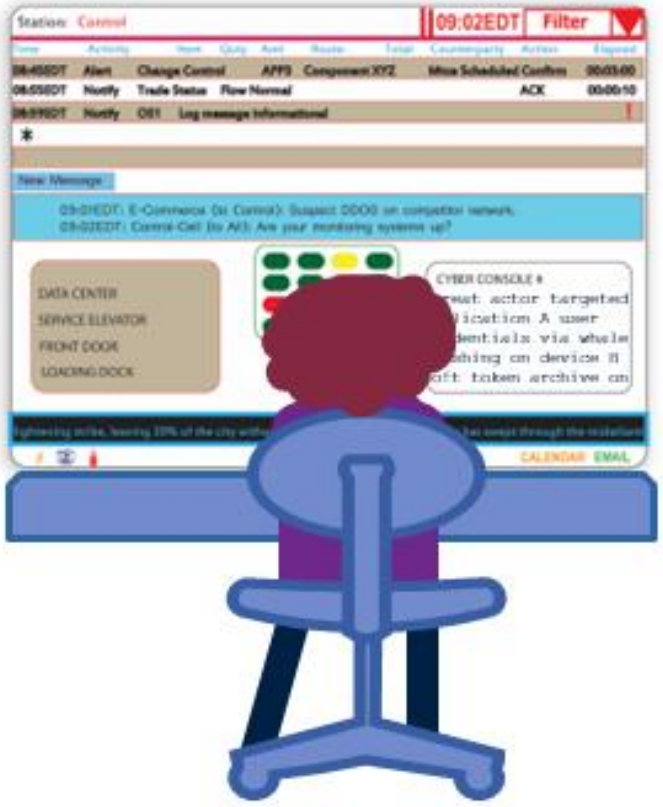
Example Enterprise Zero Trust Architecture Method



Example Procedure

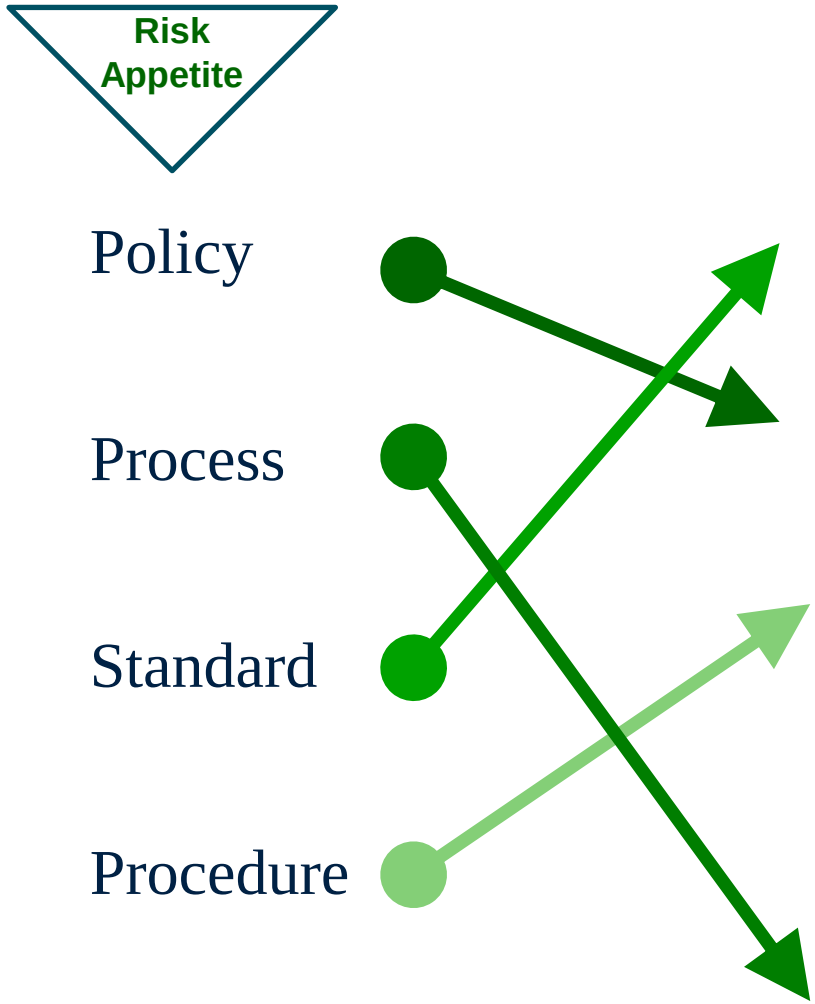
The Security Operations Center Analyst:

1. Select the highest priority alert in the queue
2. Ascertain context:
   - 2.a. app or data in alert, search application registry for app/data owner
   - 2.b. device or IP in alert, search asset inventory for device and/or network owner
3. If the priority is "critical", convene call with supervisor and app/data/device/net owners
4. Use data in alert to distinguish between anomaly and intrusion:
   - 3.a. if intrusion or cannot tell, make a note in the log asking supervisor for instruction
   - 3.b. anomaly, place alert on list for end-of-shift call with app/data/device/net owners



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Wiley 2024, ISBN: 9781394213955

Control Hierarchy



A. Personally identifiable information is encrypted using AES with 256 bit keys.

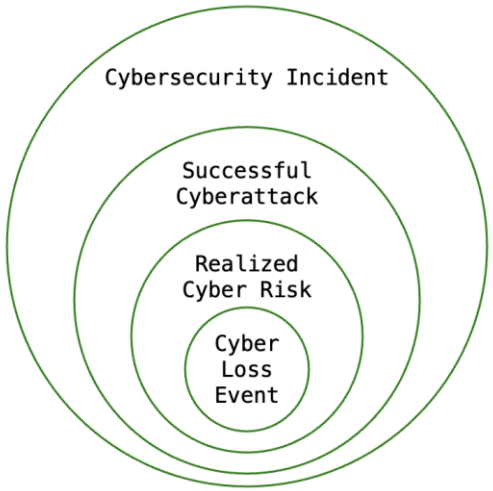
B. Personally identifiable information shall stay within the borders of the country.

C. The first step in responding to a request for permission for file access is to document the request in the incident management system.
The second step is to look up the user in the IAM system.

D. Personally identifiable information is collected by customer service, encrypted by application development, and disseminated by compliance

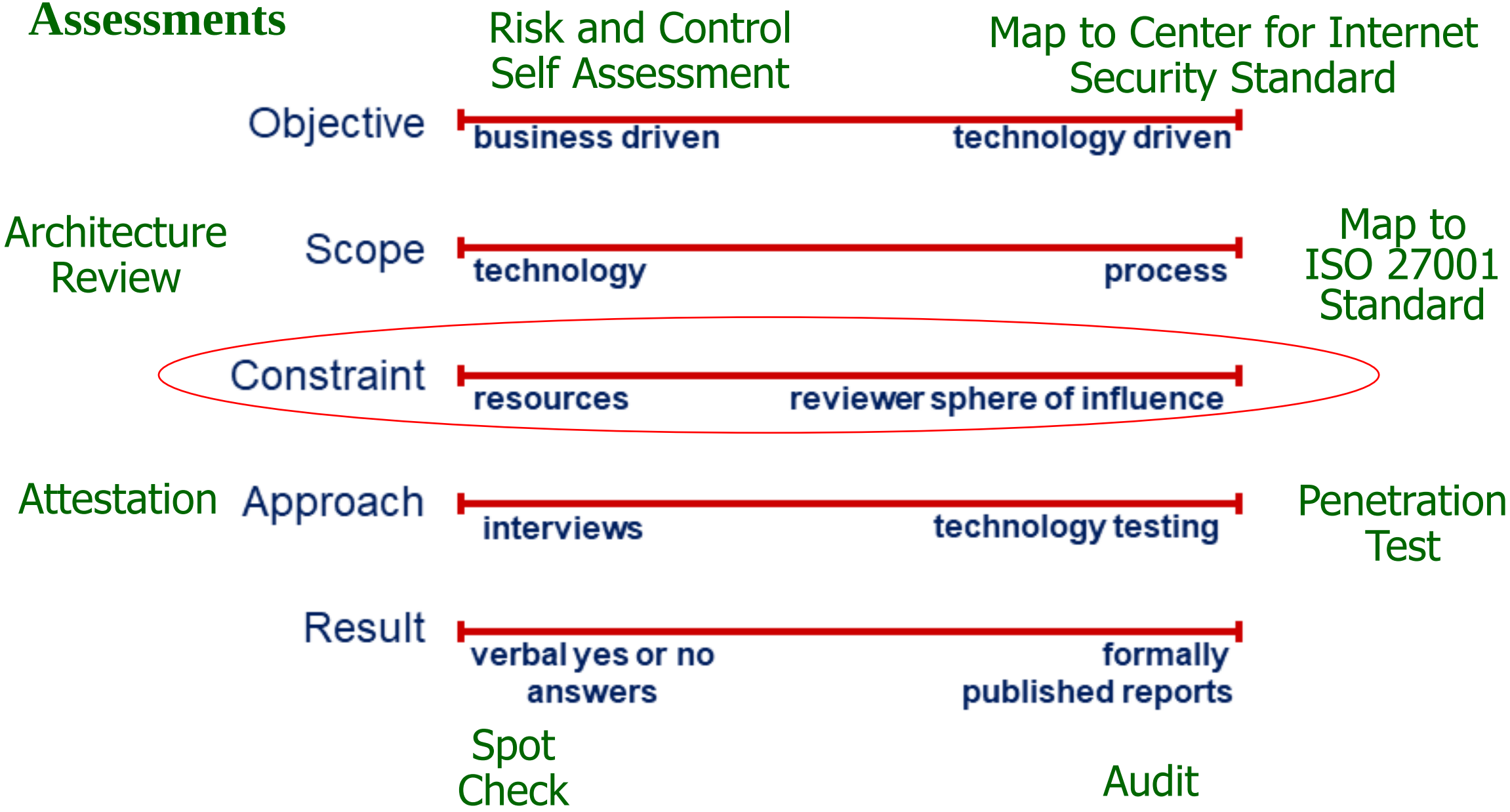
The Chief Information Security Officer (CISO) Equation

Threats	!=	Exploits
Vulnerabilities	!=	Exploits
Vulnerabilities + Threats	!=	Exploits
Vulnerabilities + Threats	allow	Exploits
Vulnerabilities + Threats + Prevent Process	minimize	Exploits



Exploits	!=	Damage
Exploits + Service/Data/Financial Loss	=	Damage
Exploits + Service/Data /Financial Loss + Detection and Respond Process	minimize	Damage
Damage + Remediation	=	Recovery

Assessments

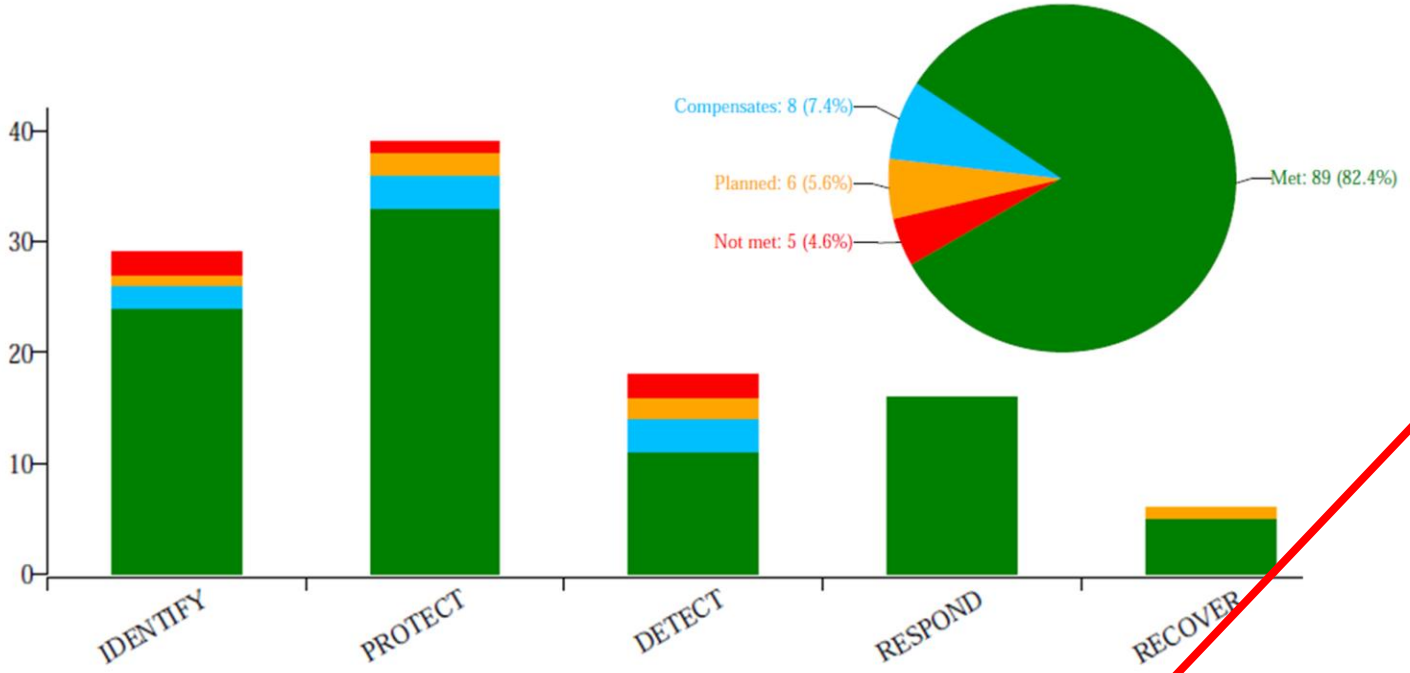


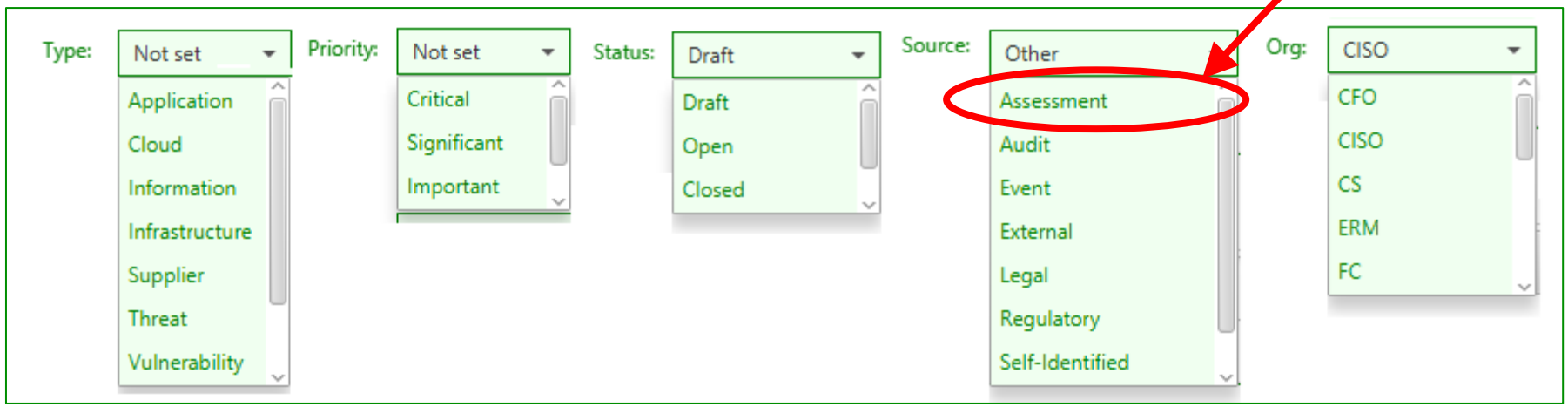
Assessment Workpapers

Response	Requirement	Observations	Evidence	Recommendation
ID.AM-1: Meets	Physical devices and systems within the organization are inventoried	Asset inventory is maintained via enterprise workflow wherein procurement, supplier risk management, and technology operations are tightly integrated. Contact: Physical, Phyllis	*Cited_Controls:* ISP:C.4: Physical Security (Policy, Protect) INFSEC:AM: Asset Management (Standard, Identify)	
ID.AM-2: Meets	Software platforms and applications within the organization are inventoried	Software inventory is maintained via technology workflow starting with procurement and maintained via the life of the software asset. Contact: Cio, The	*Cited_Controls:* INFSEC:AM-SW: Software Inventory (Standard, Identify)	
ID.AM-3: Compensates	Organizational communication and data flows are mapped	Although technology notifications are automated and crisis management notifications cover all staff, data flow documentation is partial and procedudres sometimes must be supplemented with call lists. Contact: Opsman, Sec	*Cited_Controls:* ISP:A.4: Communication (Policy, Identify) IPCM:4.D: Communicate (Procedure, Respond) FCSS-CFG:IV-CO.3: Respond Procedures (Procedure, Respond) Files uploaded: CallLists.xlsx	
ID.AM-4: Planned	External information systems are catalogued	Third Party vendors are cataloged and data exchanges logged, but there is no systematic method to ensure that all Third Parties are in the catalog. Contact: Opsofficer, Chief Issue flagged.	*Cited_Controls:* FCSS-CFG:III.4: Third Party Service Logs (Control, Identify)	Charge accounts payable with creating a Third Party vendor record as a precondition of payment.
ID.AM-5: Not Met	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Although ranks are assigned to resources based on business criticality and information classification, resources for critical controls such as endpoint security are not prioritized accordingly. Contact: Techrisk, Tammy Issue flagged.	*Cited_Controls:* ISP:A.2: Information Classification (Policy, Identify) FCSS-CFG:V.2: Asset Rank (Standard, Identify)	Establish security support tiers by rank and prioritize resources for security services accordingly.
ID.AM-6: Meets	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Security policy assigns responsibility for least privilege. Contact: Ciso, The	*Cited_Controls:* ISP:B.2.1: User Classification (Control, Identify) ISP:B.2.2: Departmental Responsibility (Control, Identify)	

Issues

NIST CSF Assessment Results





Not Met (5)

ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value

ID.SC-5 Response and recovery planning and testing are conducted with suppliers and third-party providers

PR.PT-2: Removable media is protected and its use restricted according to policy

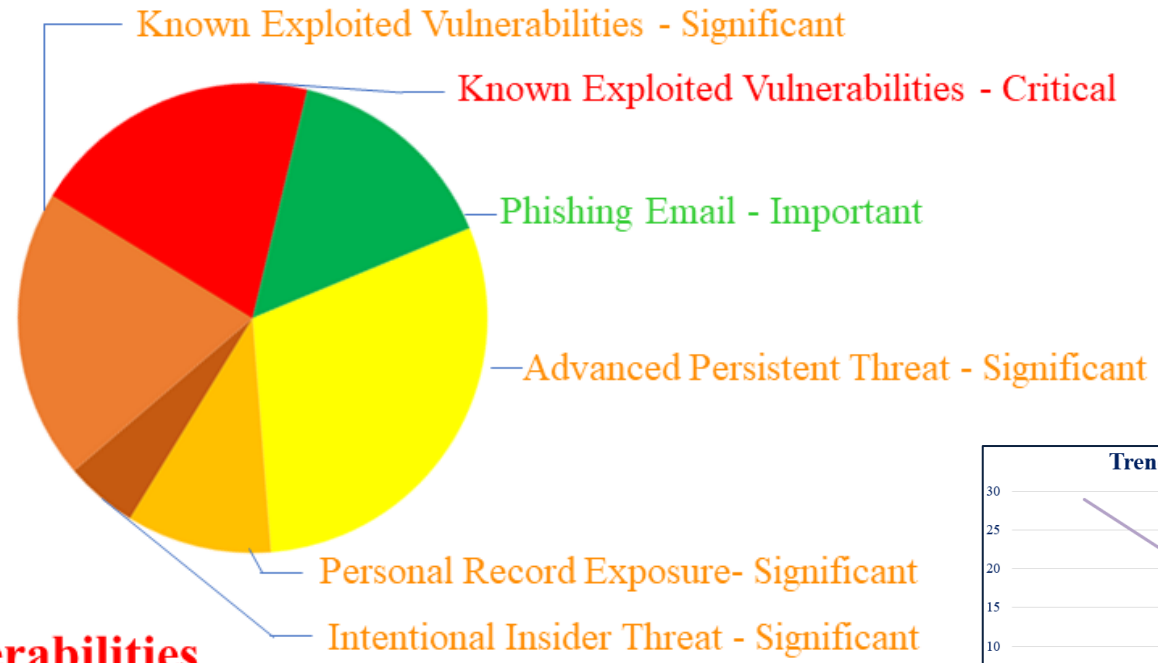
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

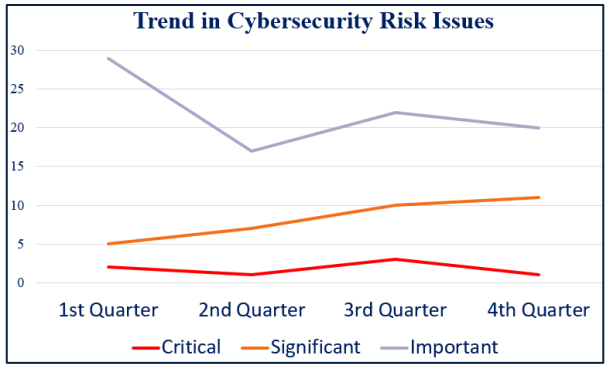
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

Risk Issues

Cybersecurity Risk

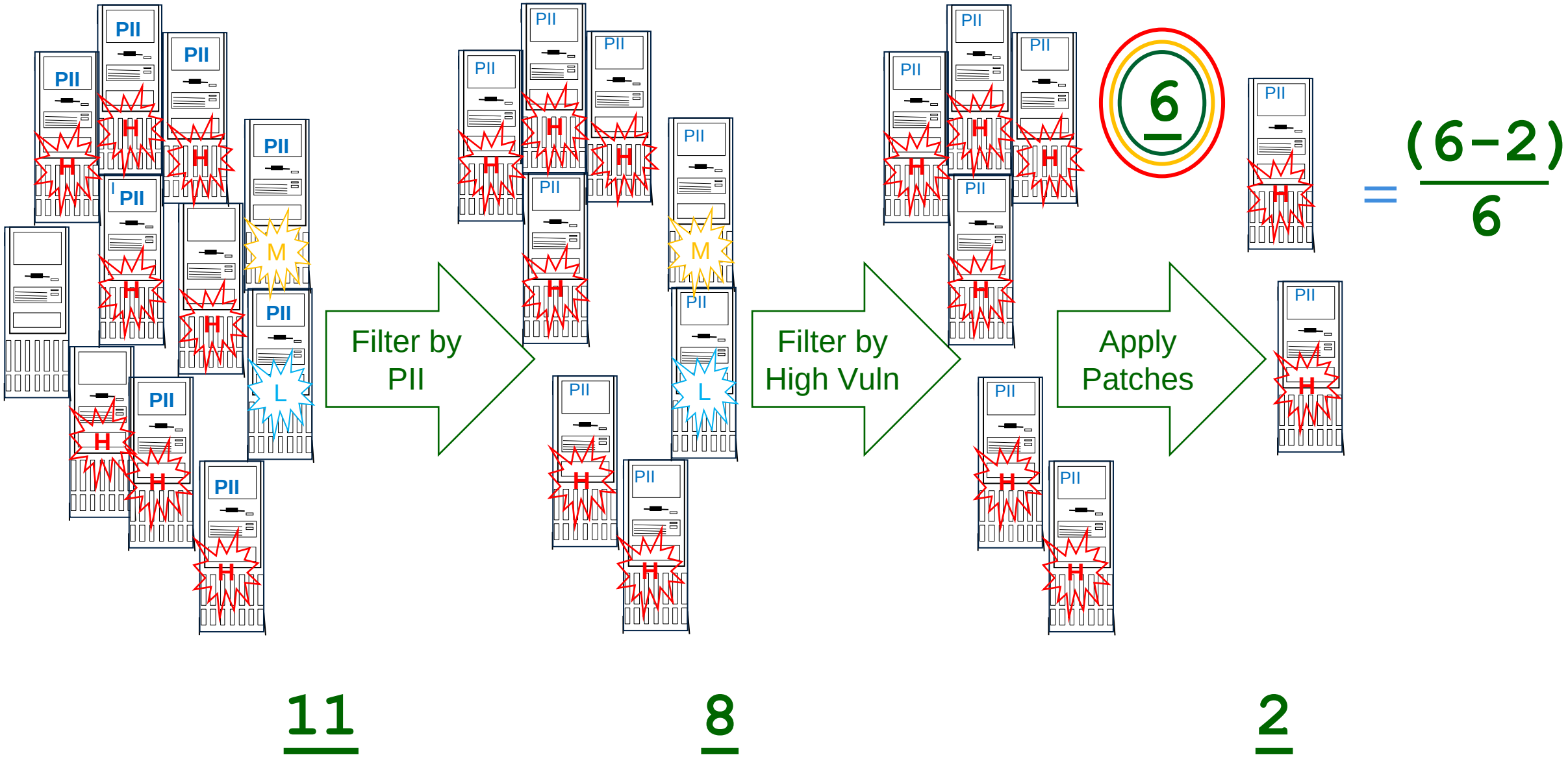
|---APT Advanced Persistent Threat
|---CFG Misconfigurations
|---DL Data Breach
| |---DL.C Lost or Stolen Credentials
| |---DL.P Personal Record Exposure
|---IT Insider Threat
| |---IT.A Accidental Insider Threat
| |---IT.I Intentional Insider Threat
| |---IT.P Phishing Email
|---MW Malware Infection
| |--- MW.KEV Known Exploited Vulnerabilities
| |--- MW.ZD Zero Day Attacks
|---SI Service Interruption
| |---SI.N Distributed Denial of Service
| |---SI.O Technology Outages





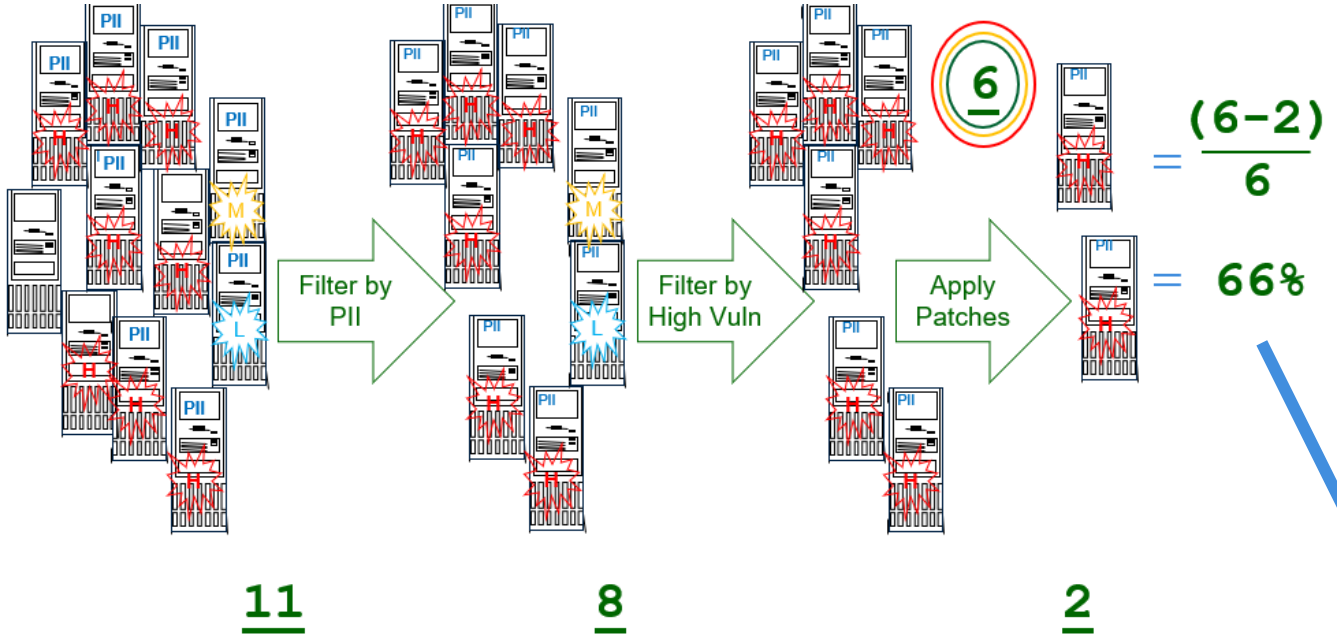
Issue	Summary	Source/Criteria	Remediation
I5 Open Significant 2024-02-06	NIST-CSF requirement: ID.AM-3 Type: Infrastructure	Assessment (A000002-ID.AM-3) Criteria: Does not Meet NIST-CSF assessment requirement: Organizational communication and data flows are mapped Linked Risks: CS.APT: Advanced Persistent Threat - Activities of well-organized and funded adversaries with long-term plans to achive goals that negatively impact the firm.	Enginir, Simrin FC 2024-10-31
I2 Open Important 2024-04-12	Malware event, impact Moderate: End Point Security Desktop apt malware scanning files on all shares for PII Type: Infrastructure	Event (Event-SIRT4753) Criteria: Known exploited vulnerability to threat vector: Phishing -- breach of risk appetite for PII Linked Risks: CS.MW: Malware Infection - Execution of malicious software on a firm systems.	Opsman, Sec CISO No Target

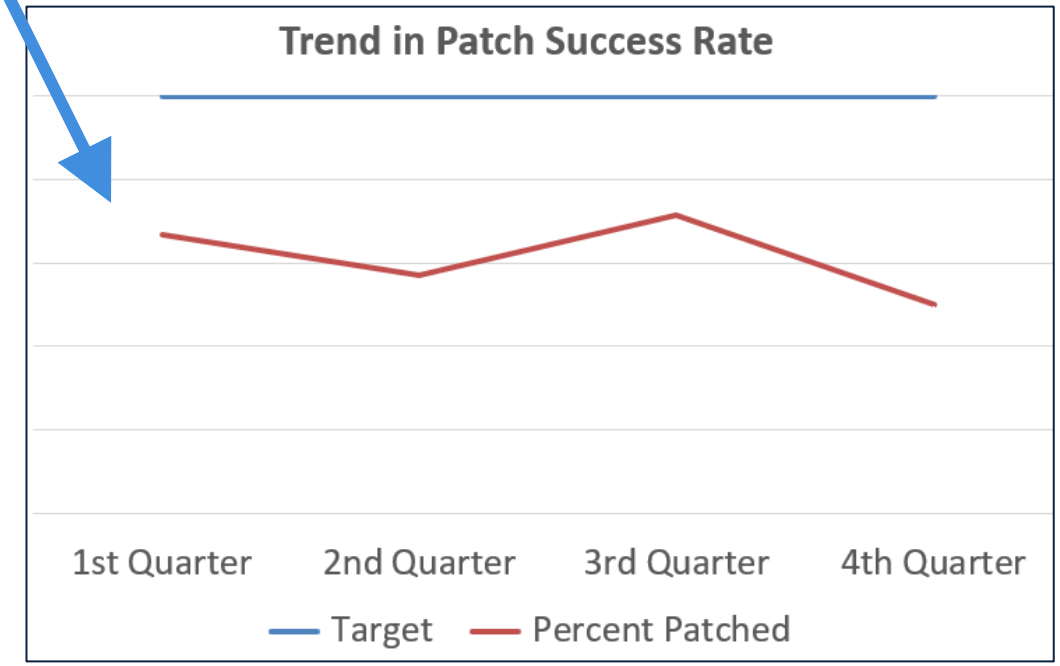
From Measures to Metrics



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Wiley 2024

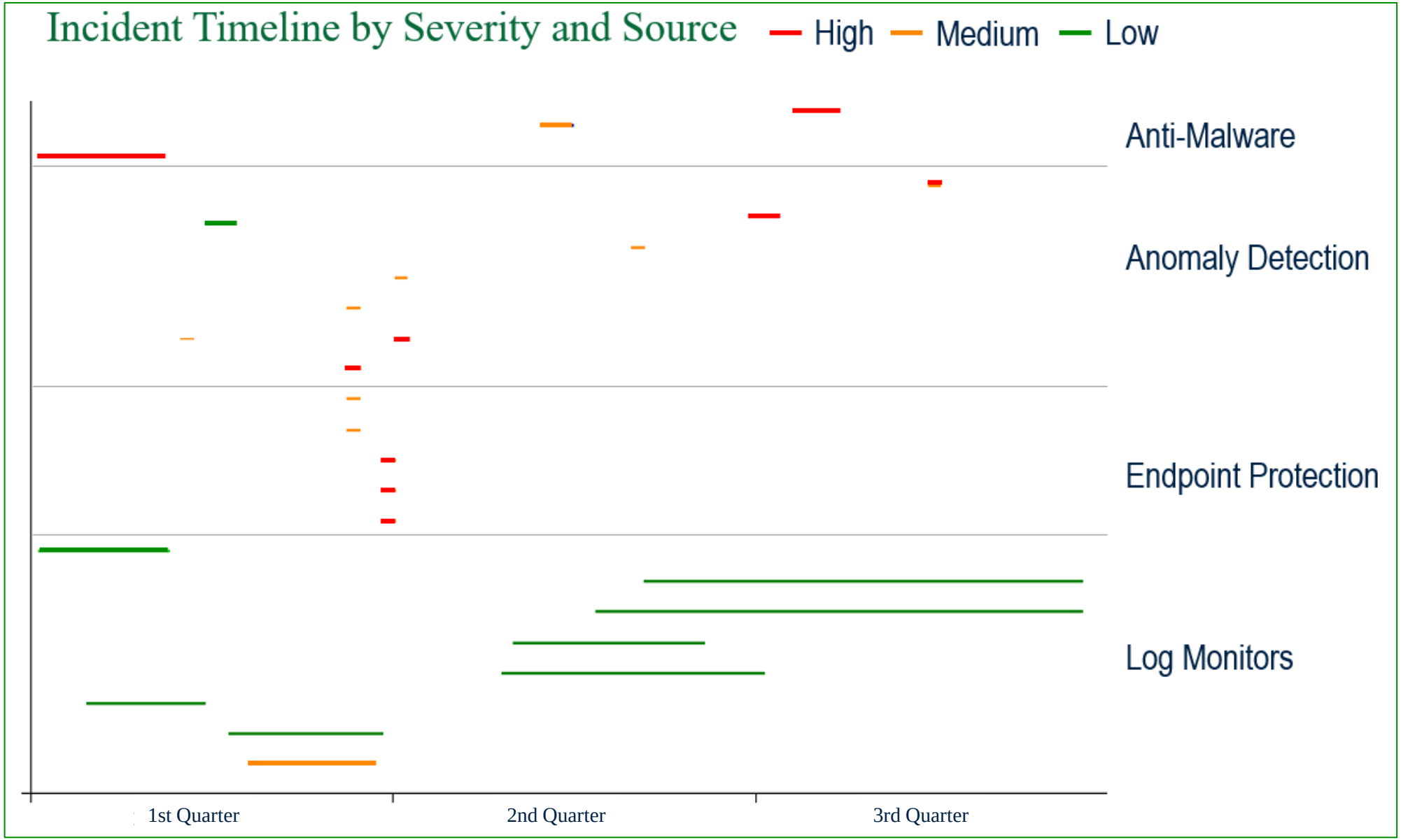
Key Risk Indicators: Trends in Patching Effectiveness



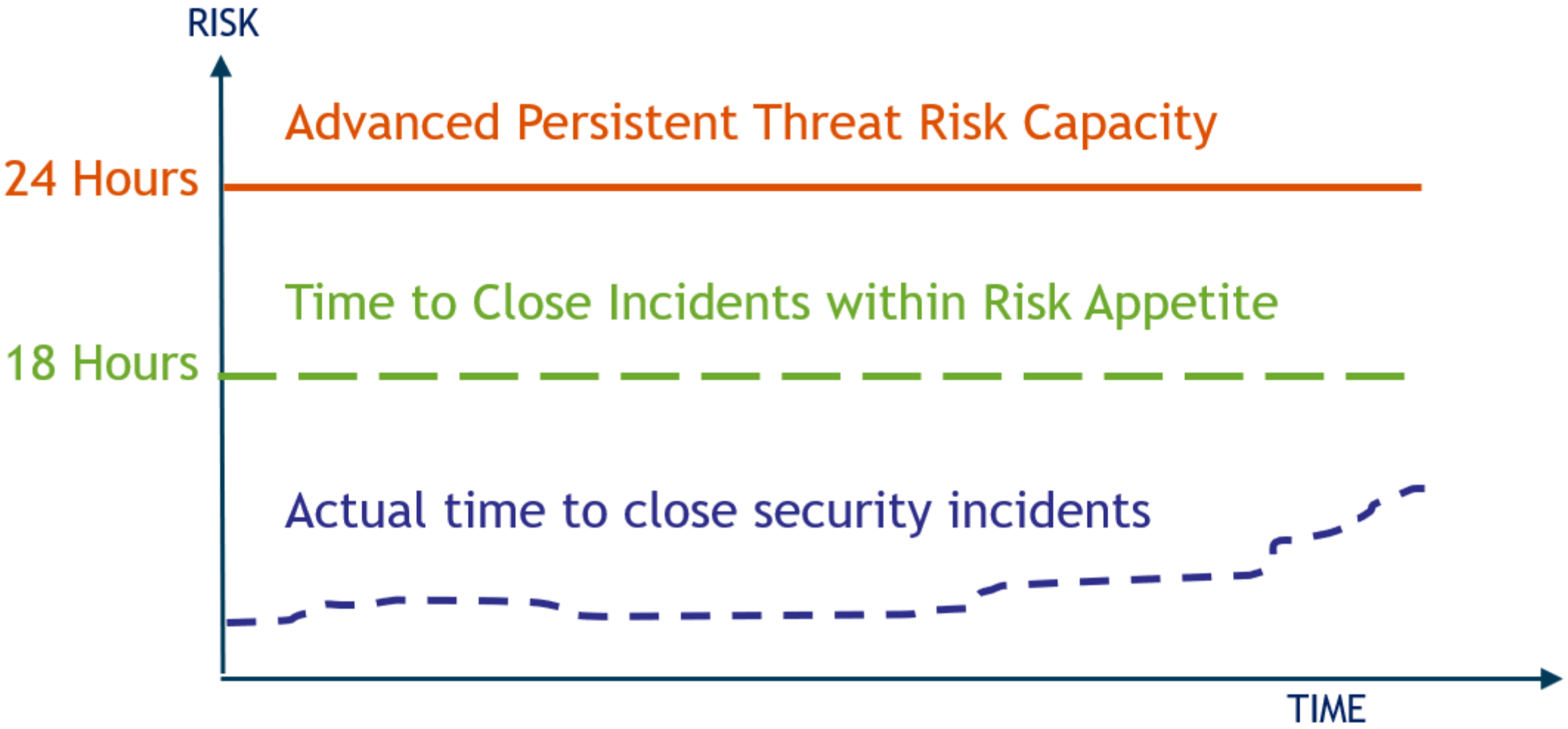


Source: Bayuk, Stepping Through Cybersecurity Risk Management, Wiley 2024

Key Risk Indicators: Trends in Incident Time to Close



Risk Tolerance



Risk Measurement

Cyber:CS Cybersecurity 100%

|---Cyber:CS.IT Insider Threat (90%)

| |---Cyber:CS.IT-A Accidental Insider Threat (20%)

| |---Cyber:CS.IT-I Intentional Insider Threat (20%)

| |---Cyber:CS.IT-P Phishing Email (90%)

|---Cyber:CS.SI Service Interruption (20%)

| |---Cyber:CS.SI-N Distributed Denial of Service (10%)

| |---Cyber:CS.SI-O Technology Outages (20%)

|---Cyber:CS.MW Malware Infection 100%

| |---Cyber:CS.MW.ZD Zero Day Attacks (70%)

| |---Cyber:CS.MW-KEV Known Exploited Vulnerabilities (100%)

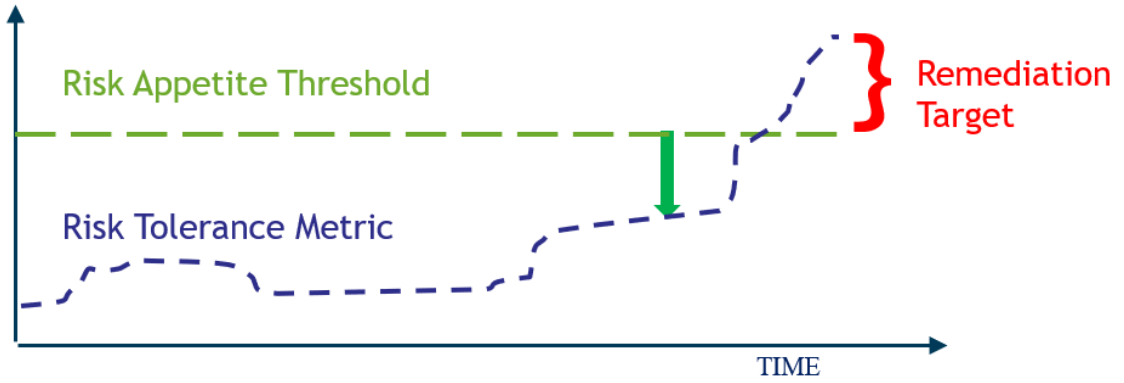
|---Cyber:CS.APT Advanced Persistent Threat (70%)

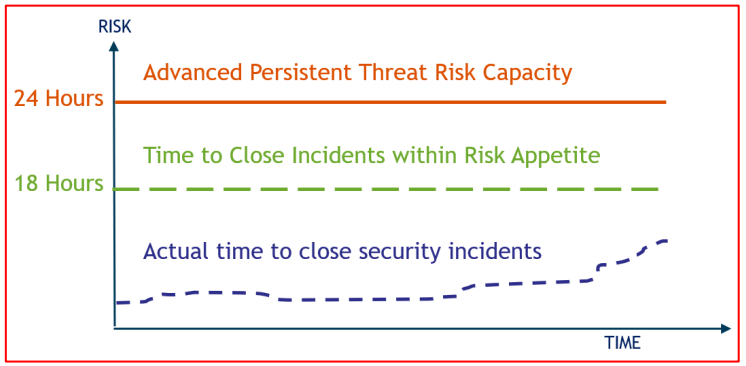
|---Cyber:CS.CFG Misconfigurations (20%)

|---Cyber:CS.DL Data Leaks (80%)

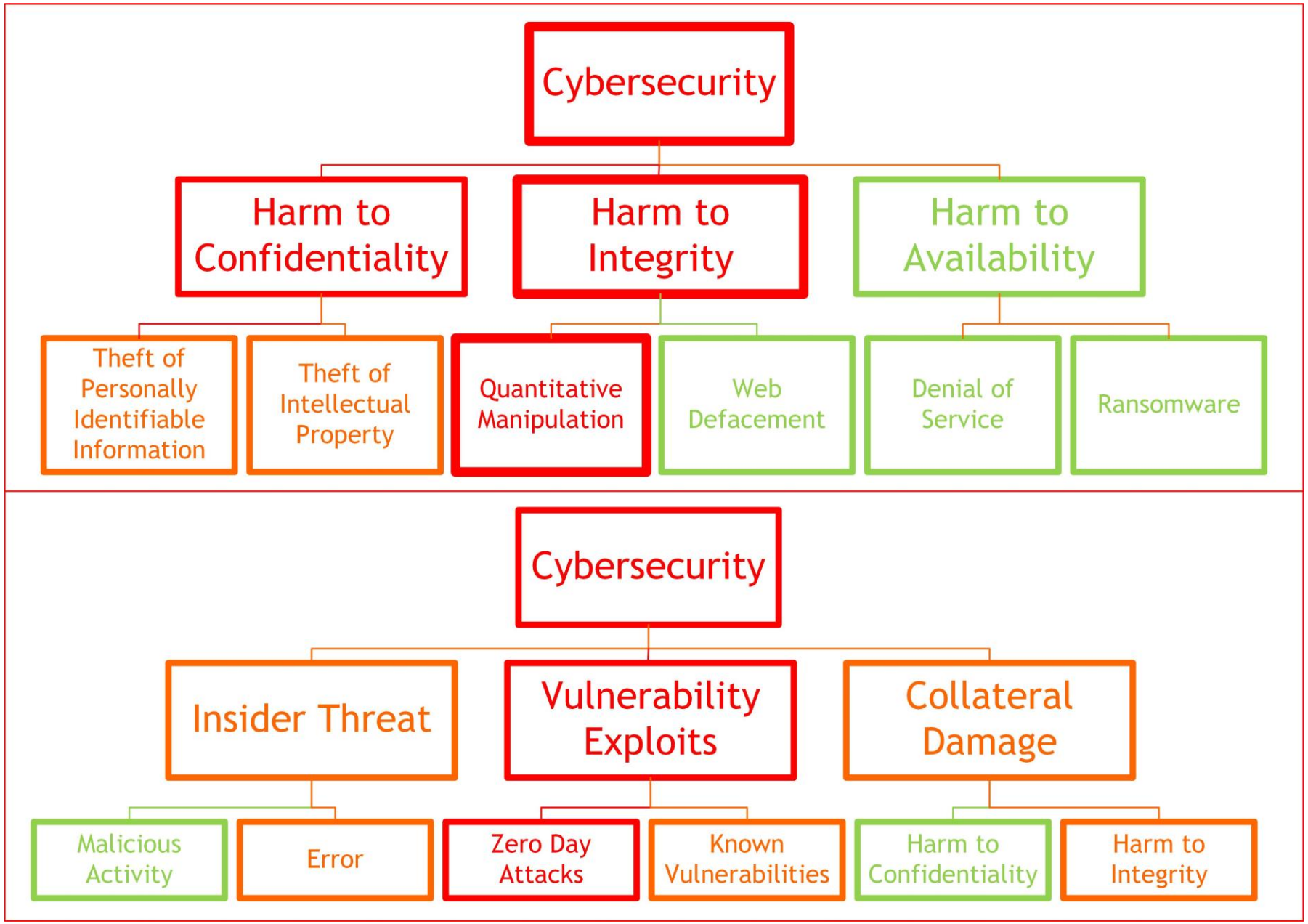
|---Cyber:CS.DL-P Loss of Personal Records (80%)

|---Cyber:CS.DL-C Lost or Stolen Credentials (10%)





Risk Hierarchy



Questions/Discussion?

jennifer@bayuk.com

www.bayuk.com