

# How to Prioritize NIST CSF Controls with FAIR

Richard Barretto  
Manager of Security Operations

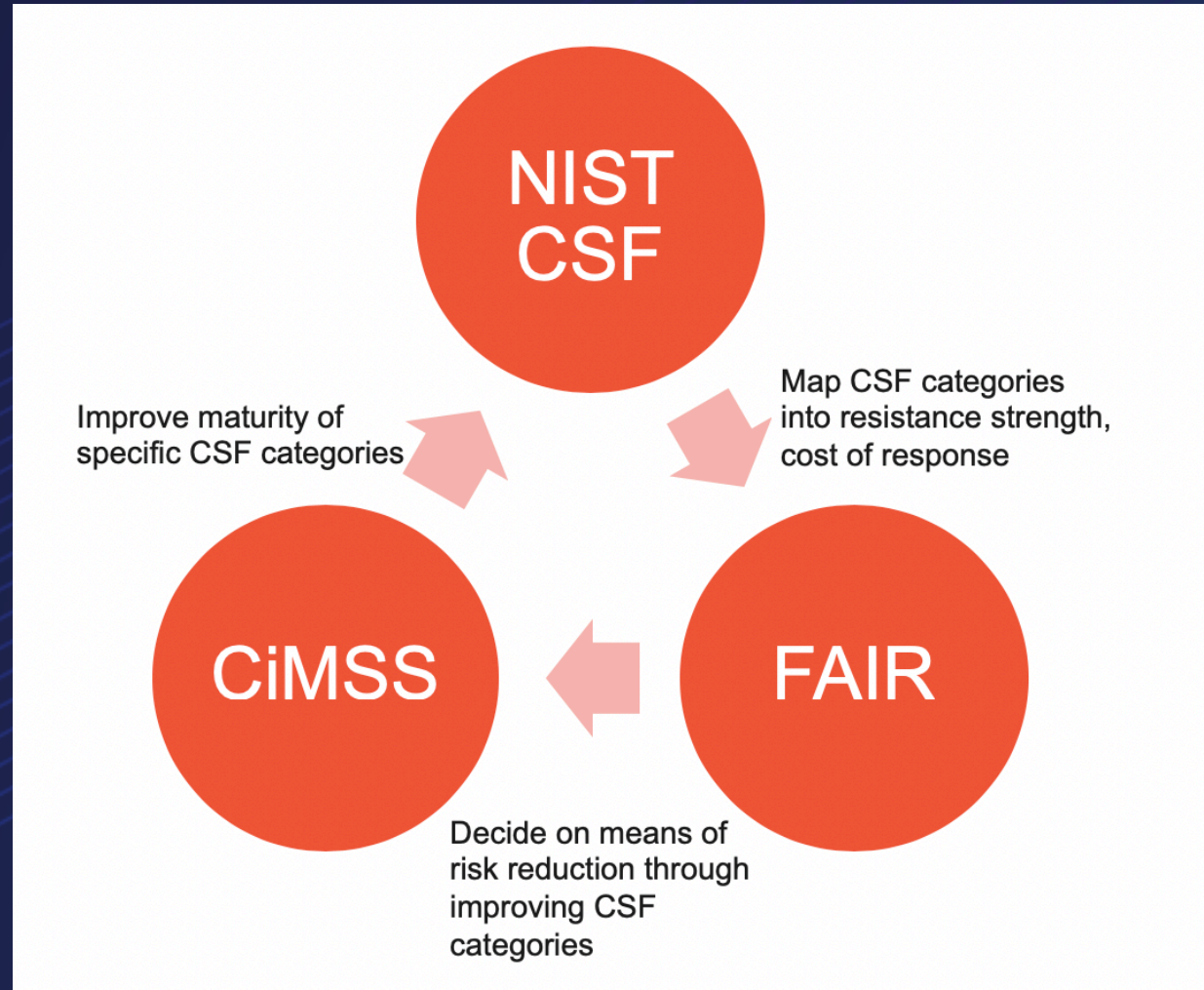


@richardbarretto

# Agenda

- Cimpres's journey with FAIR
- What worked and what didn't ?
- How can FAIR work with NIST CSF?
- Prototype mapping and measurement
- How to prove security value?

# Our Journey

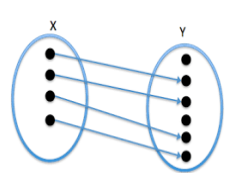


# Challenges

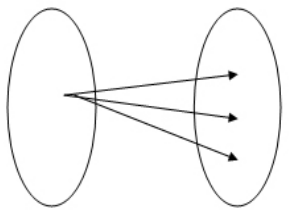


- How could we back up the rationale for Resistance Strength?
- Which controls gave the best value?
- Transparency between Risks and Controls

# FAIR and NIST Mapping Model



**1:1:** Risk Scenario to mitigating controls can map directly to a FAIR element such as Resistance Strength.



**1:Many** – Risk Scenario to mitigating controls can map to more than one NIST Control

# Risk Scenario: Malware

## MITGATIONS:

- Account Use Policies
- Active Directory Configuration
- Antivirus/Antimalware
- Data Backup
- Disable or Remove Feature or Program
- Encrypt Sensitive Information
- Execution Prevention

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.AC-3: Remote access is managed

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate

PR.DS-5: Protections against data leaks are implemented

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)



# NIST Maturity Score 1:1



PR.IP-12: A vulnerability management plan is developed and implemented

Maturity Average	Resistance Strength
<b>0 – None</b>	0-20%
<b>1 - AdHoc</b>	20-50%
<b>2 - Repeatable</b>	50-79%
<b>3 - Managed</b>	80-95%

# NIST Maturity Score 1: Many



Resistance Strength = 50-79%

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for servers and systems is established and managed	2	
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	2	
		DE.AE-5: Incident alert thresholds are optimized	2	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity	DE.CM-1: The network is monitored to detect potential cybersecurity events	2	
		DE.CM-8: Vulnerability scans are	3	
		DE.DP-1: Roles and responsibilities for	3	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of or response to anomalous events.	DE.DP-2: Detection activities comply with all applicable requirements	3	
		DE.DP-3: Detection processes are tested	3	
DE.DP-4: Event detection information is communicated to appropriate parties		3		
DE.DP-5: Detection processes are		2		

Maturity Average	Resistance Strength
0 - None	0-20%
1 - AdHoc	20-50%
2 - Repeatable	50-79%
3 - Managed	80-95%

Control Average = 2.44



# Cimpress Journey

NIST CSF

FAIR

Red Team  
Test

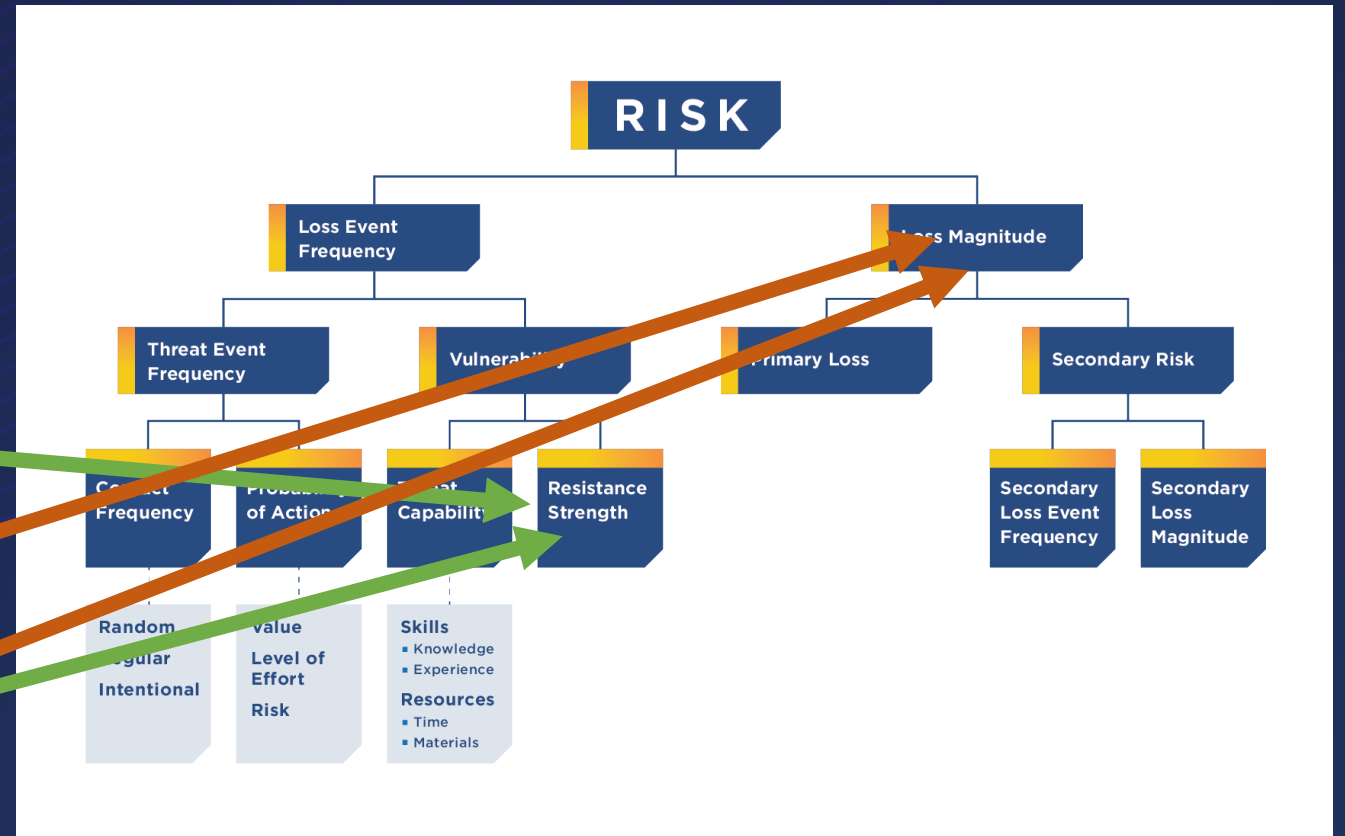
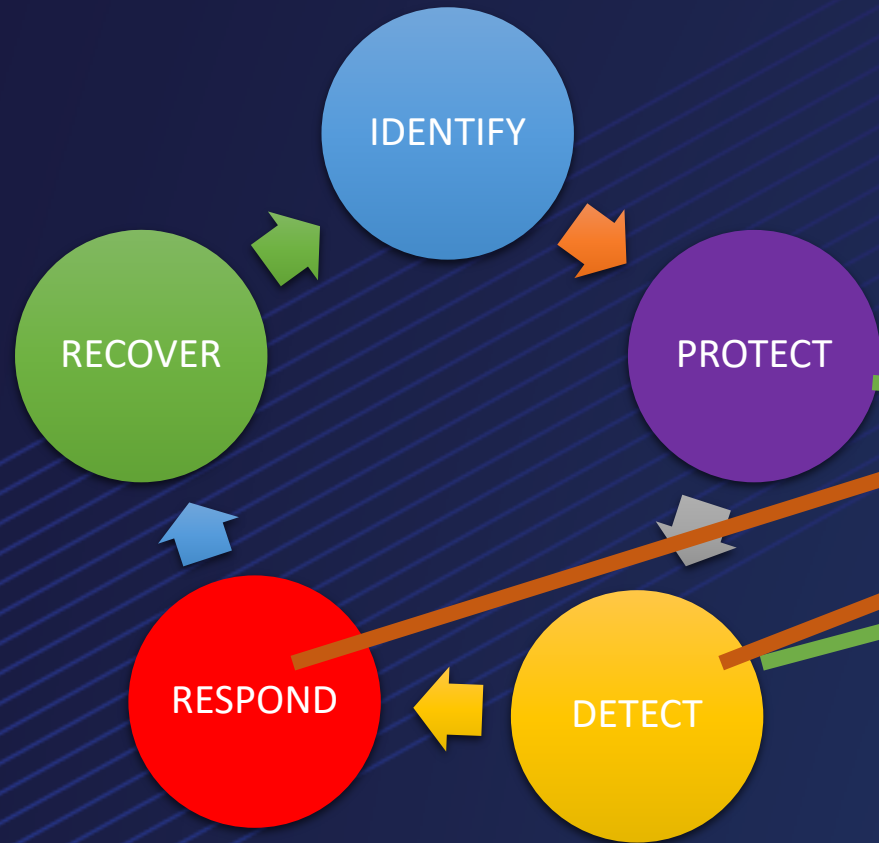


**MITRE**  
**ATT&CK™**

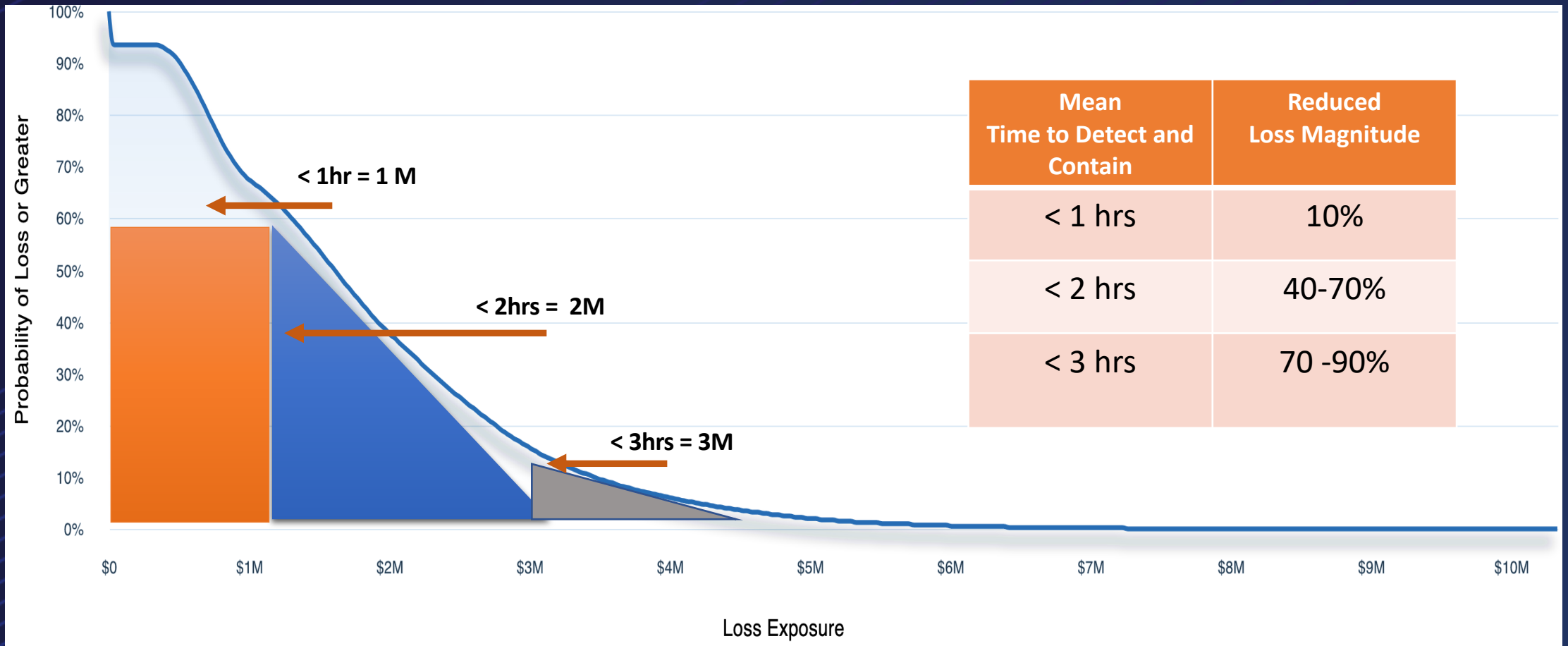
# MITRE ATT&CK Coverage Heat Map

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Deobfuscate/Decode Files or Information	Credentials from Password Stores	Browser Bookmark Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Show apps /e API	Browser Extensions	Create or Modify System Process	Execution Guardrails	Exploitation for Credential Access	Cloud Service Dashboard	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Scheduled Task/Job	Compromise Client Software Binary	Event Triggered Execution	Exploitation for Defense Evasion	Input Capture	Cloud Service Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Man-in-the-Middle	File and Directory Discovery	Remote Services	Data Staged	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Supply Chain Compromise	User Execution	Create or Modify System Process	Hijack Execution Flow	Hide Artifacts	Modify Authentication Process	Network Service Scanning	Software Deployment Tools	Data from Information Repositories	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Trusted Relationship		Event Triggered Execution	Process Injection	Hijack Execution Flow	Network Sniffing	Network Share Discovery		Data from Local System	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Valid Accounts		External Remote Services	Scheduled Task/Job	Impair Defenses	OS Credential Dumping	Network Sniffing		Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
		Hijack Execution Flow	Valid Accounts	Indicator Removal on Host	Steal Application Access Token	Password Policy Discovery		Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
		Pre-OS Boot		Masquerading	Steal Web Session Cookie	Permission Groups Discovery		Input Capture	Non-Application Layer Protocol		Network Denial of Service
		Scheduled Task/Job		Modify Authentication Process	Two-Factor Authentication Interception	Process Discovery		Screen Capture	Non-Standard Port		Resource Hijacking
		Server Software Component		Obfuscated Files or Information	Unsecured Credentials	Remote System Discovery			Protocol Tunneling		System Shutdown/Reboot
		Traffic Signaling		Pre-OS Boot		Software Discovery			Proxy		
		Valid Accounts		Process Injection		System Information Discovery			Remote Access Software		
				Rootkit		System Network Configuration Discovery			Traffic Signaling		
				Subvert Trust Controls		System Network Connections Discovery			Web Service		
				Traffic Signaling		System Owner/User Discovery					
				Valid Accounts		Virtualization/Sandbox Evasion					
				Virtualization/Sandbox							

# Two Sides to Every Story



# Impact Reduction



# Metrics to consider

Measuring	Insights
<ul style="list-style-type: none"><li>• <b>Mean time to retrieve logs for investigation</b></li></ul>	Point of attack contact to initial log availability
<ul style="list-style-type: none"><li>• <b>Mean time to get logs and produce detections</b></li></ul>	Log entry to initial security alert
<ul style="list-style-type: none"><li>• <b>Mean time to produce alert from point of attack</b></li></ul>	Security alert to SOC notification
<ul style="list-style-type: none"><li>• <b>Mean time to validate true or false positive to point of escalation</b></li></ul>	SOC notification to escalation to relevant business
<ul style="list-style-type: none"><li>• <b>Mean time to response</b></li></ul>	Escalation to initial Incident Response
<ul style="list-style-type: none"><li>• <b>Mean time to containment</b></li></ul>	IR start to establishing containment and impact scope (IOCs, TTPs, root cause)
<ul style="list-style-type: none"><li>• <b>Mean time to eradicate</b></li></ul>	Containment to Eradication and closure

# Different Scopes for Different Folks

FAIR (\$\$) = Top Business Risks = Risk Tolerance

NIST CSF = Security Governance = Maturity

MITRE ATT&CK = Alerts & Detections

Red Team

Blue Team

# Clear as Glass

- Build test plans
- Clear road map of controls
- Prioritization of controls, tests, and, investments



# Thank you