Critical Insight®

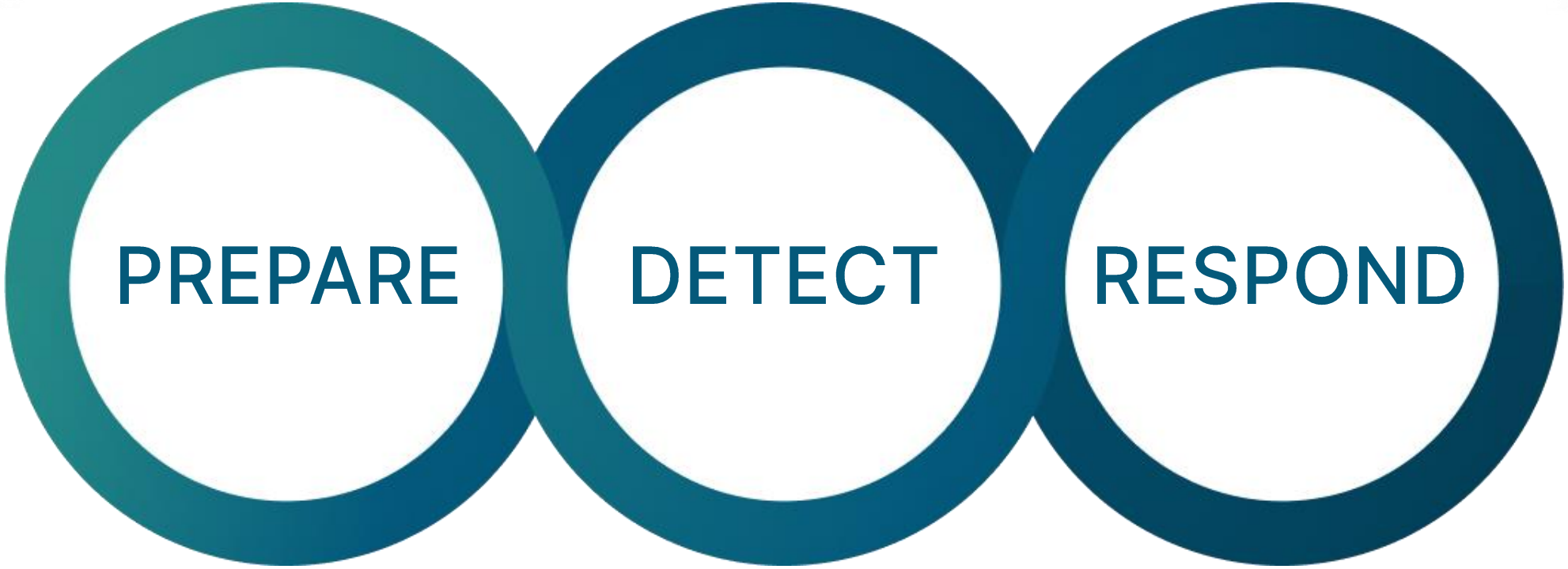
NIST CSF 2.0
What to Expect

Things to Know

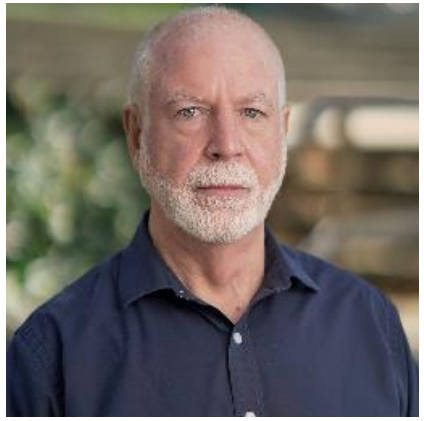
- Chat is on the right
- Mute the chat if you want
- You will get a recording
- You will get the slide deck

Critical Insight

CRITICAL INSIGHT DEFENDS CRITICAL INFRASTRUCURE



Panelists



Michael Hamilton

Founder, CISO, and
Former CISO of Seattle

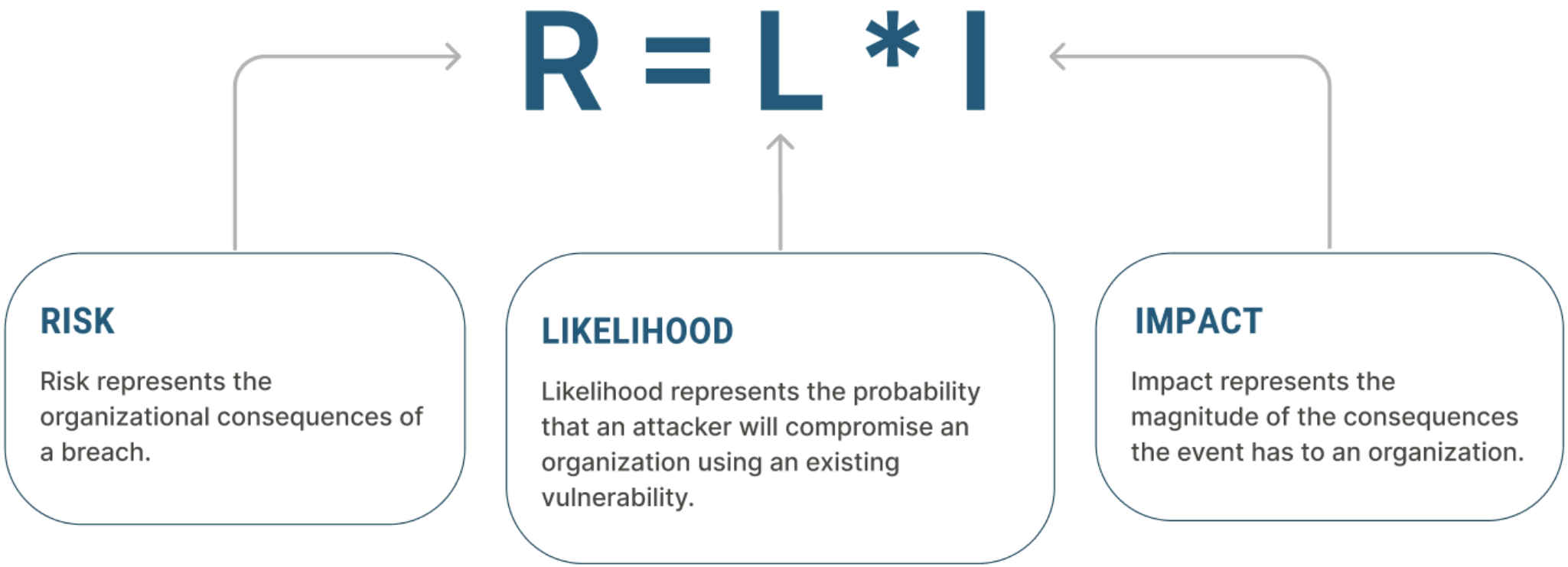
Fred Langston

Founder and Chief
Product Officer

Jake Milstein

CMO and Event Host

There is no 100% Effective Cybersecurity



What is the CSF?

- National Institute of Standards and Testing (NIST) CyberSecurity Framework (CSF)
- Developed by Obama administration for use by any organization
- Outcome-based
  - One size truly does fit all
  - You design the controls solutions based on your organization and capabilities
  - Results in Gap Analysis and Roadmap
- Being strongly advocated for critical sectors
  - Pipelines, health, aviation, rail, water, SmartCities
- The most universal standard available and applicable to ANY organization
- Very widely used standard of practice
- We have added a risk assessment format that builds on the Gap Analysis

Vocabulary

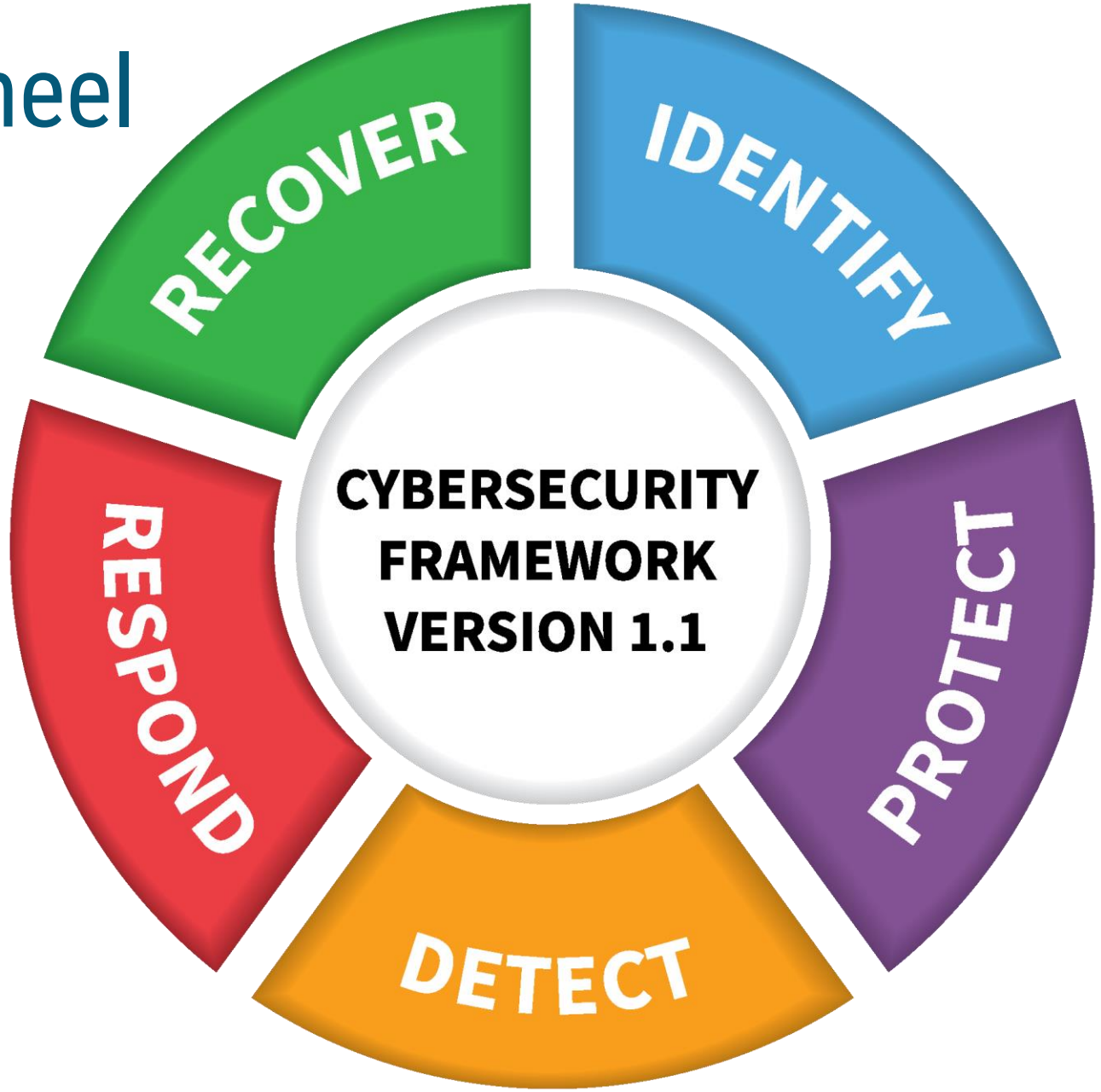

FRAMEWORK FUNCTIONS
IDENTIFY ID
PROTECT PR
DETECT DE
RESPOND RS
RECOVER RC
CATEGORIES
SUBCATEGORIES
INFORMATIVE REFERENCES

NIST 2.0

Comment period ended

New version out after 5/31 (today)

The Old Wheel




Govern
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

What's IN and what's OUT in the new NIST CSF?

IN	• Cybersecurity outcomes applicable to all organizations
OUT	• Language specific to critical infrastructure
IN	• Prevention of cybersecurity incidents through outcomes focused in Govern, Identify, and Protect functions
IN	• Detection and response of incidents through the Detect, Respond, and Recover functions
OUT	• Governance under Identify
IN	• New Govern function covering organizational context, risk management strategy, policies and procedures, and roles and responsibilities

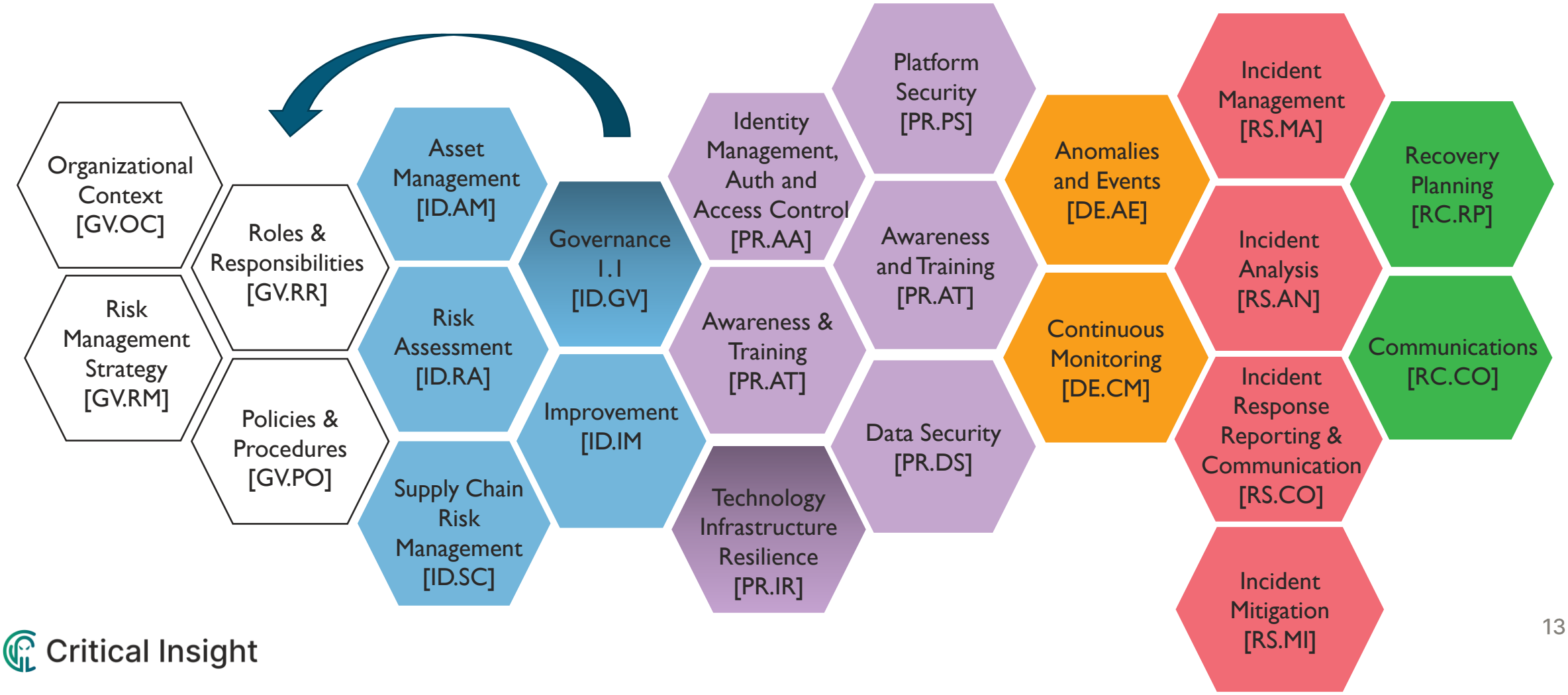
What's NEW in the NIST CSF?

IN	• Cybersecurity supply chain risk management outcomes
IN	• Continuous improvement through a new Improvement category in the Identify function
IN	• Leveraging the combination of people, process, and technology to secure assets across all categories in the Protect function
IN	• Resilience of technology infrastructure through a new Protect category
IN	• Cybersecurity incident response management, including the importance of incident forensics, through new categories in the Respond and Recover functions

NIST CyberSecurity 2.0 Framework

Govern | **Identify** | **Protect** | **Detect** | **Respond** | **Recover**

What does the NIST CSF 2.0 Include?



Critical Insight

What it's NOT

- 800 series which reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security
- NIST 800-53 though it's derived from it
- NIST 800-171/172, also derived from NIST 800-53
- Prescriptive like the Payment Card Industry Data Security Standard (PCI-DSS)
- A risk management framework although we've modified it to include impacts which is key to applying this to Risk Assessment is required such as HIPAA
- A regulatory requirement – although it is required by critical infrastructure providers under the purview of sector-specific agencies

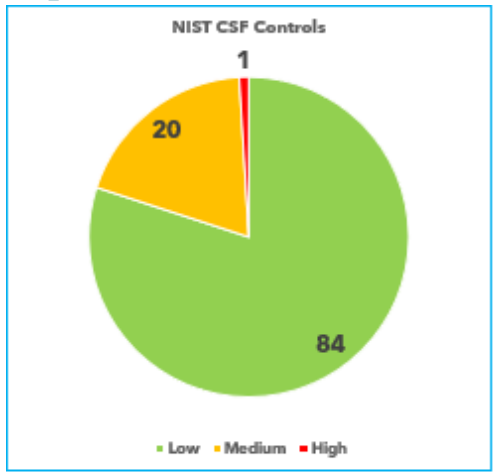
Usage Example

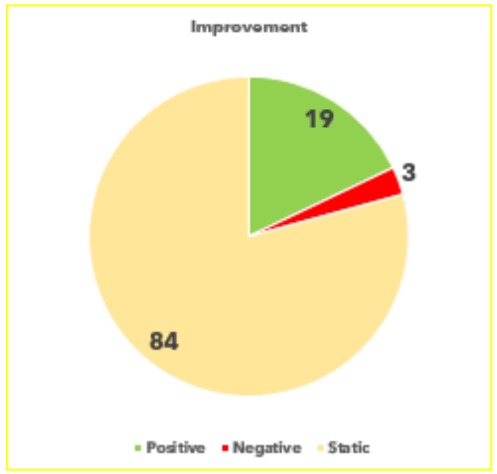
- Healthcare
  - Looks beyond ePHI/PHI to all assets in your environment
    - Bad Actors can use non-HIPAA systems to eventually compromise ePHI
    - Non-HIPAA systems can still impact delivery of healthcare
    - Non-HIPAA systems can still lead to catastrophic loss
- Add Impacts and likelihood of a missing control leading to an adverse event to the assessment to achieve true Risk Assessment as prescribed by the HHS Office of Civil Rights
- Not limited to the data a particular regulation is designed to protect
- True enterprise approach
- NIST Crosswalk for CSF to HIPAA - https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

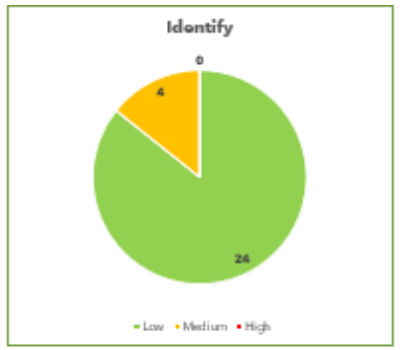
What is Compliance Crosswalking?

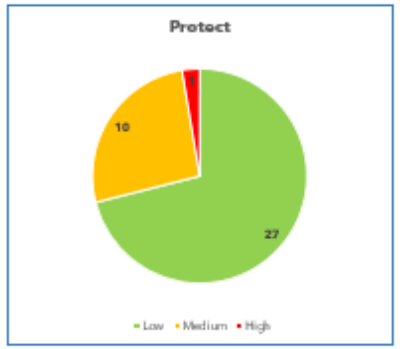
- A Unified Approach to Compliance ("*The Unified Approach to Compliance*", Risk Management Alliance, 2001)
- Compile all regulations and standards that apply to your organization and place them on a matrix, selecting the most important compliance regime as the primary key
  - Healthcare – HIPAA
  - Lenders – GLBA
  - Banking – FFIEC
  - DoD Manufacturing – NIST 800-171
- Align controls based on their function so complying with the primary key covers compliance with all other standards and regulations
- Ensure you understand the scope of each standard
- Assess once for all compliance regimes
- Secure Controls Framework - https://www.securecontrolsframework.com/

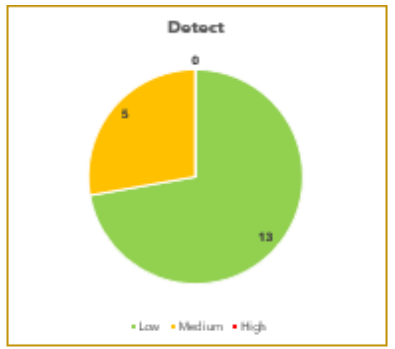
NIST Spreadsheet Tool

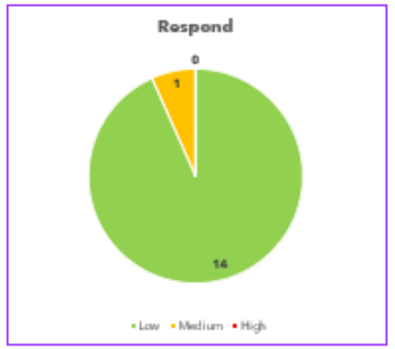












Mitigation Opportunities

Domain	Mitigate Count
Identify	10
Protect	19
Detect	5
Respond	1
Recover	3
Total:	38

Risk Level	NIST CSF Controls
Low	84
Medium	20
High	1
N/A	3
Improvement	
Positive	19
Negative	3
Static	84

Risk Level	Identify
Low	24
Medium	4
High	0
N/A	1
Improvement	
Positive	5
Negative	0
Static	23

Risk Level	Protect
Low	27
Medium	10
High	1
N/A	1
Improvement	
Positive	5
Negative	3
Static	30

Risk Level	Detect
Low	13
Medium	5
High	0
N/A	0
Improvement	
Positive	6
Negative	0
Static	12

Risk Level	Respond
Low	14
Medium	1
High	0
N/A	1
Improvement	
Positive	3
Negative	0
Static	13

Risk Level	Recover
Low	6
Medium	0
High	0
N/A	0
Improvement	
Positive	0
Negative	0
Static	6

SAMPLE ACTION ITEMS AFTER NIST-CSF BASED ASSESSMENT

Issue	Service Mapping
• Asset Management	• vCISO, Policies + Procedures, Hardware/Software Inventory
• Governance	• vCISO + Policy + Change Control
• Risk Management Strategy	• vCISO + Annual Risk Assessment + Compliance + Policy
• Identity Management & Access Control	• Access Control Policy, User Provisioning/De-Provisioning, Identity Management Systems
• Awareness & Training	• SAT + Social Engineering + Phishing Verification Service
• Monitoring & Response	• MDR + EDR + Rapid Quarantine + IR

CYBERSECURITY-AS-A-SERVICE

Most MDR products are just threat detection and investigation. Ours includes Incident Preparedness and Response and is supplemented by a suite of services to bolster your strategic program.

INCIDENT PREPAREDNESS

- Tabletop Exercises
- Incident Response Plan Development
- Rapid Quarantine Playbook Development
- Incident Response Plan Review

24X7 THREAT DETECTION & INVESTIGATION

- On-Prem Network
- Cloud Environments
- Office365
- Third-Party Saas Applications
- Endpoint Detection and Response
- IoT & OT

ACTIVE INCIDENT RESPONSE

- Incident Response onDemand
- Incident Response Retainer
- Rapid Quarantine

REGULATORY COMPLIANCE

- Policy Creation & Review
- vCISO / oCISO
- Security Awareness Training
- Log Retention and Compliance Review

APPLICATION AND PENETRATION TESTING

- Penetration Testing (Internal / External)
- Web Application Security
- Social Engineering

VULNERABILITY SCANNING

- Continuous Vulnerability Identification
- CVI Pro

GAP ANALYSIS AND RISK ASSESSMENTS

- Security Risk Assessment
- Focused Security Assessment

Sign Up!

Daily IT Security News Blast – curated by myself for the last 15 years

Free bi-weekly security awareness training online.

Regular online urgent panels and podcasts

Critical Insight®

Schedule Time With Mike

Jake@criticalinsight.com

Michael.Hamilton@criticalinsight.com