

# Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI) Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOM's Existing Assessment Framework

Presented by: **Lori D. Coombs, MBA, MSE**

2025 Human Systems Conference - March 11-12, 2025  
National Defense Industrial Association (NDIA)  
Arlington, VA

Approved for Public Release

## Acknowledgements / Thanks

- Institutional Affiliation: Marymount University
- **Don B. Coombs, MBA:** Chief Strategy Officer, CyberJobs, WWCM, and Director of WWCM Academy for support & contributions
- **Dr. Andrew O. Hall:** Professor, Faculty Advisor, Marymount University, Chair of the editorial board for the Cyber Defense Board of Cyber Defense Review, Former President of Military and Security Applications Society of INFORMS, Former Director of the Army Cyber Institute, the Army's Think Tank for the cyber domain, Retired Army Colonel
- **Dr. Shelton Rhodes:** Mentor, Dean of the College of Business at Delaware State and Founding Dean of the Howard S. Brown School of Business at Stevenson University, Retired Army Infantry Major
- **Dr. Lelyn D. Saner:** USCYBERCOM Mentor (J533)

# Meet Lori D. Coombs



- **United States Senate / Capitol Hill**

- Appointed Female Delegate to the DNC – Former President Al Gore and US Vice Presidential Nominee Joe Lieberman (2000), US Presidential Nominee (2004), US Senator, (CT), Capitol Hill (1989-2013)

- **Marymount University**

- Doctor of Science (D.Sc.) in Cybersecurity | MBA: Mgmt, MS: Sys Engineering, BS: Business Admin

- **IEEE**

- Director of the Northern Virginia Section Executive Committee

- **NIST / NICE**

- Publications: “The Landscape of Performance-Based Assessments in Cybersecurity” and “Help Wanted: Cybersecurity Educators”

- **University of Arizona Global Campus**

- Associate Professor – Master of Info Systems Management (MISM), Drone Aviation Education: Integrating drones in cybersecurity

- **University of Colorado Colorado Springs**

- Sr. Program Advisor: Strategic AI and Distinguished Women in Leadership Programs

- **WWCM, and WWCM Academy (501c3)**

- Cybersecurity, Heliophysics, Adv Air Mobility, Clean/Renewable Energy Sys, Sys & Cloud Integration, DevSecOps, AI, ML, C6ISR

- **CyberJobs**

- Upskilling Cybersecurity Talent, Enterprise Executive Cybersecurity Upskilling and Training, Personal Career Coaching for Cyber Jobs

- **NASA, DoD, Private & Public Industries**

- R&D Test & Eval | Title 51 USC: National and Commercial Space Programs



- INTRODUCTION
- RESEARCH METHODOLOGY
- ANALYSIS
- RESULTS / CONCLUSION

**Today's Goal:** To communicate the importance of illustrating ways for enhancing current approaches that assess USCYBERCOM's measures of excellence (MOEs) that consider human systems integration (HSI) to keep pace with the evolving cybersecurity threats landscape to support warfighters and the systems they use.

## Introduction: Overview Topics

- **MOE's:** Evaluates how well an organization or system is meeting goals
- Supply Chain Management (SCM) Life Cycle & Scaled Agile Framework (SAFe)
- **Evaluation of 5 Frameworks = CYBER DEFENSE READINESS FRAMEWORK:** Risk Management Framework (**RMF**), Cybersecurity Maturity Maturation Certification (**CMMC**), National Institute of Standards Cybersecurity Framework (**NIST CSF**), International Organization for Standardization/International Electrotechnical Commission (**ISO/IEC 27001:2013**) – Information Security Management Systems, and the Center for Internet Security Controls (**CIS**)
- **Upskilling, Retaining & Recruiting Cyber Talent**
- Today's talk highlights USCYBERCOM, however the Cyber Defense Readiness Framework supports the mission of cyberspace defense that includes all DoD

# Discussion: Human Systems Integration (HSI)

**HSI:** Optimizes the relationship between humans and systems to enhance overall performance and safety.

## USCYBERCOM

1. Cybersecurity Tools
2. Incident Response Systems
3. Training and Simulation
4. Human-Machine Teaming
5. User-Centered Design

HSI ensures that military personnel and cyber operators can perform their duties effectively and safely which enhances mission success metrics.

## Military and Armed Forces

1. Ergonomic Equipment Design
2. Cockpit Design
3. Training Simulators
4. Decision Support Systems
5. Communication Systems



SPACE	LINK	USER	GROUND
Command Intrusion	Spoofing	Phishing	Hacking
Payload Control	Denial of Service (DoS)	Out of Date / Unpatched Software	Hijacking
Denial of Service (DoS)	Malware	Ransomware	Malware
Malware		Social Engineering	
		Malware	

**Figure 1.**

*Common Cyber-Attacks to Segments*

# Research Methodology

- **Problem Statement:** Cyber supply chain security involves securing critical infrastructure and assets. Key risks include ransomware attacks, security breaches, malware infections, process disruptions, and intellectual property theft due to unprotected devices throughout the supply chain.
- **Research Approach:** Compares 5 cybersecurity frameworks to USCYBERCOM's method of assessing MOEs that aim to meet command objectives.
- **Research Scope:** Compares MOEs of USCYBERCOM to the KPIs of the private sector.
- **Goal:** To examine the way that the private sector assesses KPIs to see how it can enhance current methods that USCYBERCOM uses for assessing MOEs. Combining frameworks identifies best practices and methods for fortifying the cybersecurity posture of USCYBERCOM operations.

# Comparing Assessment Frameworks and Cybersecurity Standards

Framework(s)	Action/Method	Objective	Input	MOEs
RMF & CMMC	Cybersecurity Risk Management	Establish risk management capabilities that ensure the defense of national interests in cyberspace.	Risk assessments	Measure the risk reduction efficiency. Notable Metrics: number of threats mitigated and incident response times.
CMMC	Cybersecurity Maturity	Ensure that cybersecurity capabilities grow over time, and systems are progressively hardened.	Maturity level assessments	Measure maturity improvement over time (e.g., Level of compliance with ISO/IEC 27001:2013, improvements in CMMC maturity scores).
NIST CSF	Incident Detection & Response	Ensure early detection of adversarial activities and fast response.	Implement the NIST-5: Detect and Respond actions	Measure Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and post-incident recovery times.
CIS Controls	Cybersecurity Best Practices	Use CIS Controls as a baseline for continuous improvement and address the most frequent vulnerabilities.	Deploy applications (e.g., configuration settings, vulnerability management, etc.)	Determine the compliance rate with highest CIS Controls. Measure the reduction in vulnerabilities.
NIST & RMF	Operational Coordination and Integration	Improve the coordination of cyberspace operations within and between U.S. and international partners.	Implement interoperability assessments and process coordination efforts	Coordination time between USCYBERCOM, partners, and the frequency of joint operations.

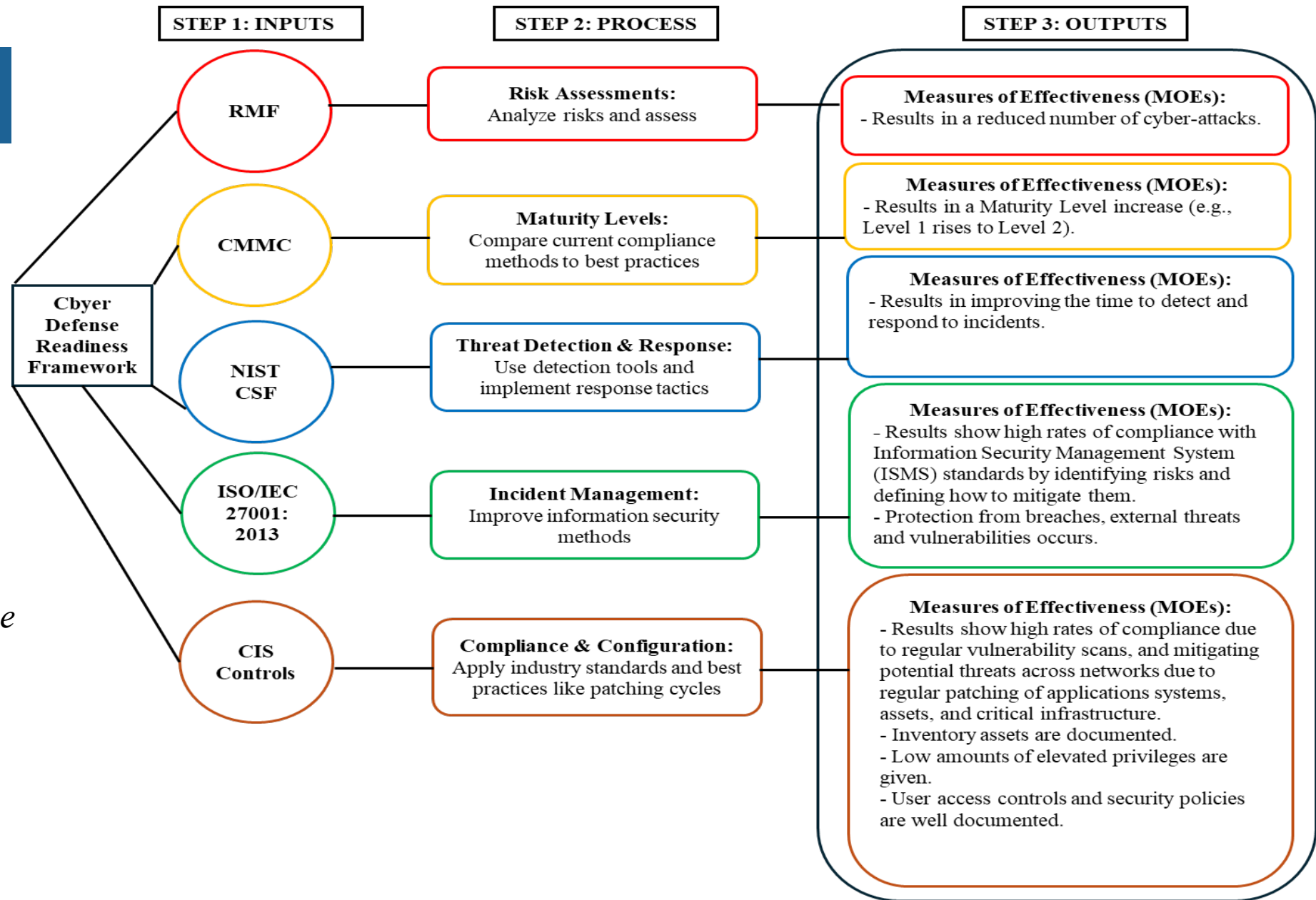
**Table 1.**

*Exploring Frameworks to Collectively Assess Cyber Posture for USCYBERCOM*

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOM's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE



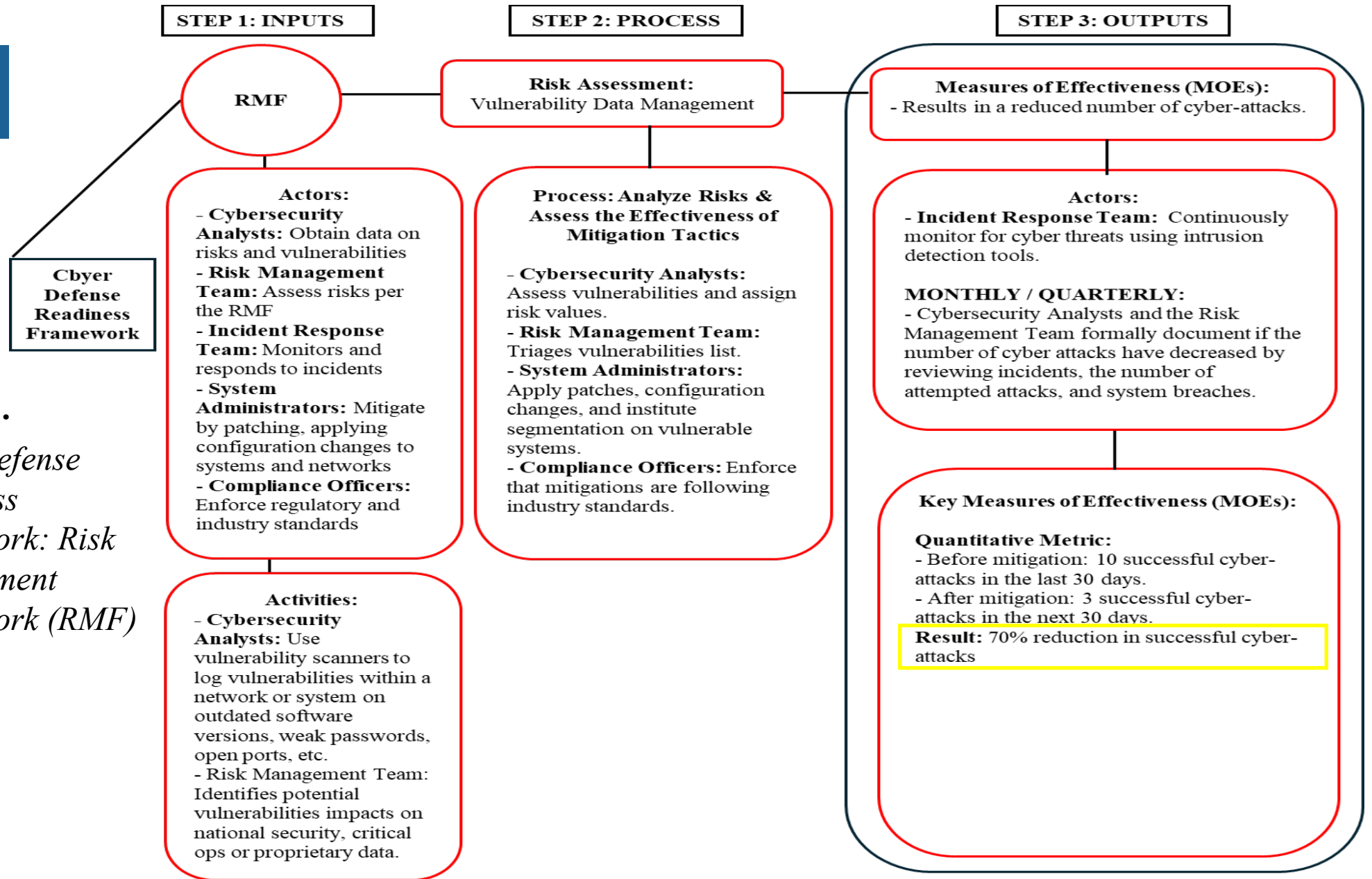
# Analysis



**Figure 2.**  
*A High-Level Taxonomy of the Cyber Defense Readiness Framework*

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

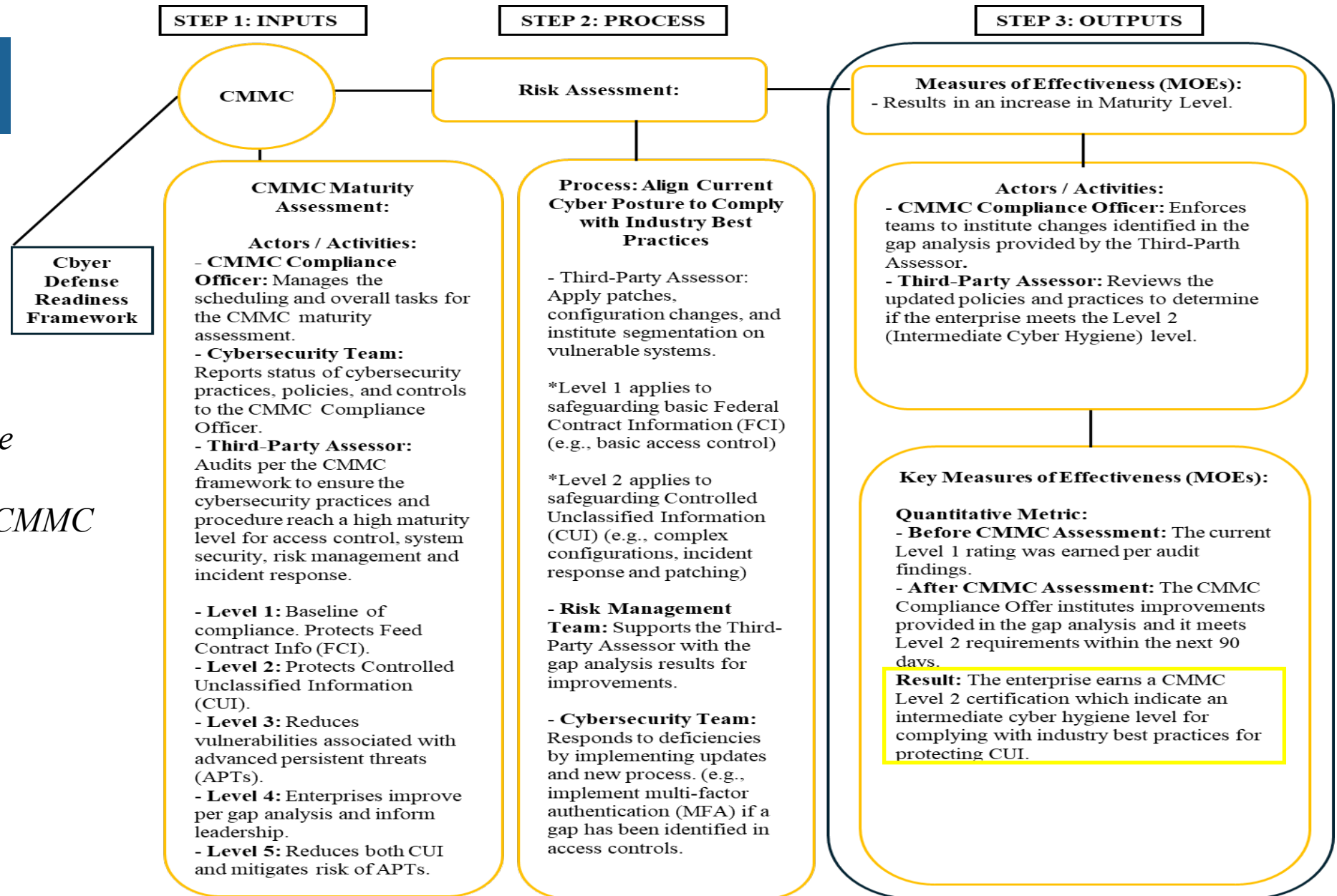
# Analysis



**Figure 3.**  
*Cyber Defense Readiness Framework: Risk Management Framework (RMF)*

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

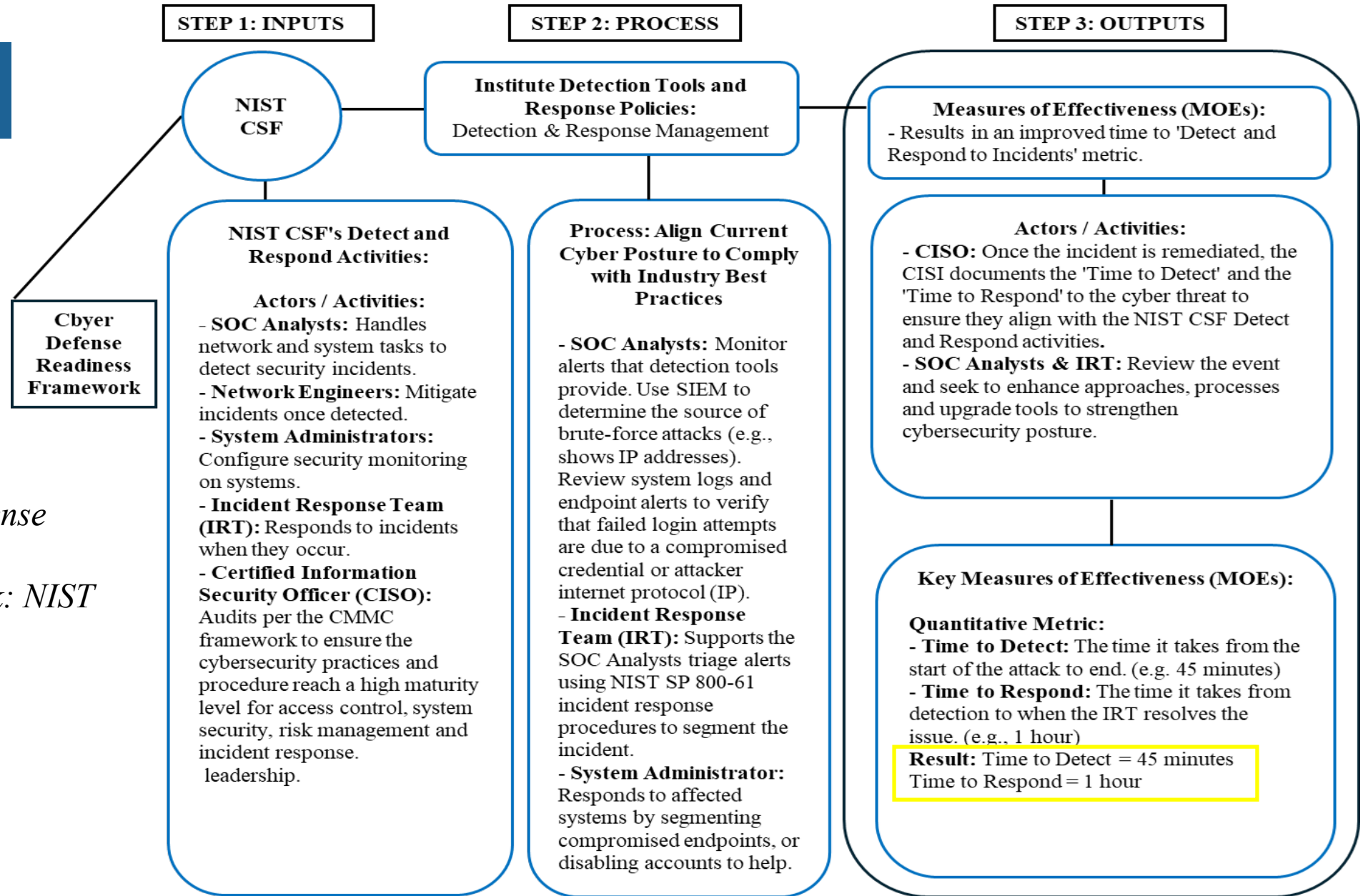
# Analysis



**Figure 4.**  
*Cyber Defense Readiness Framework: CMMC*

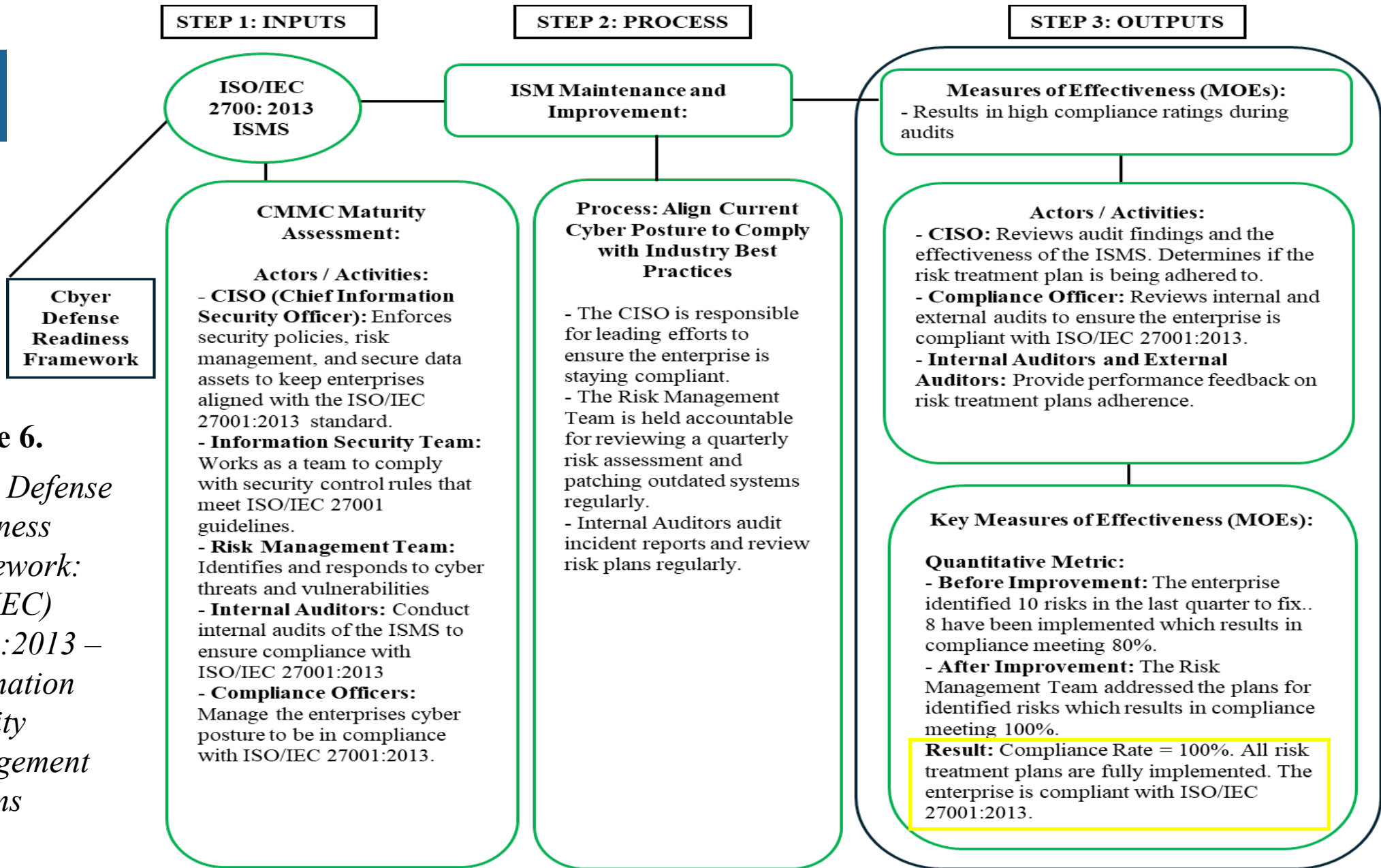
Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# Analysis



**Figure 5.**  
*Cyber Defense Readiness Framework: NIST CSF*

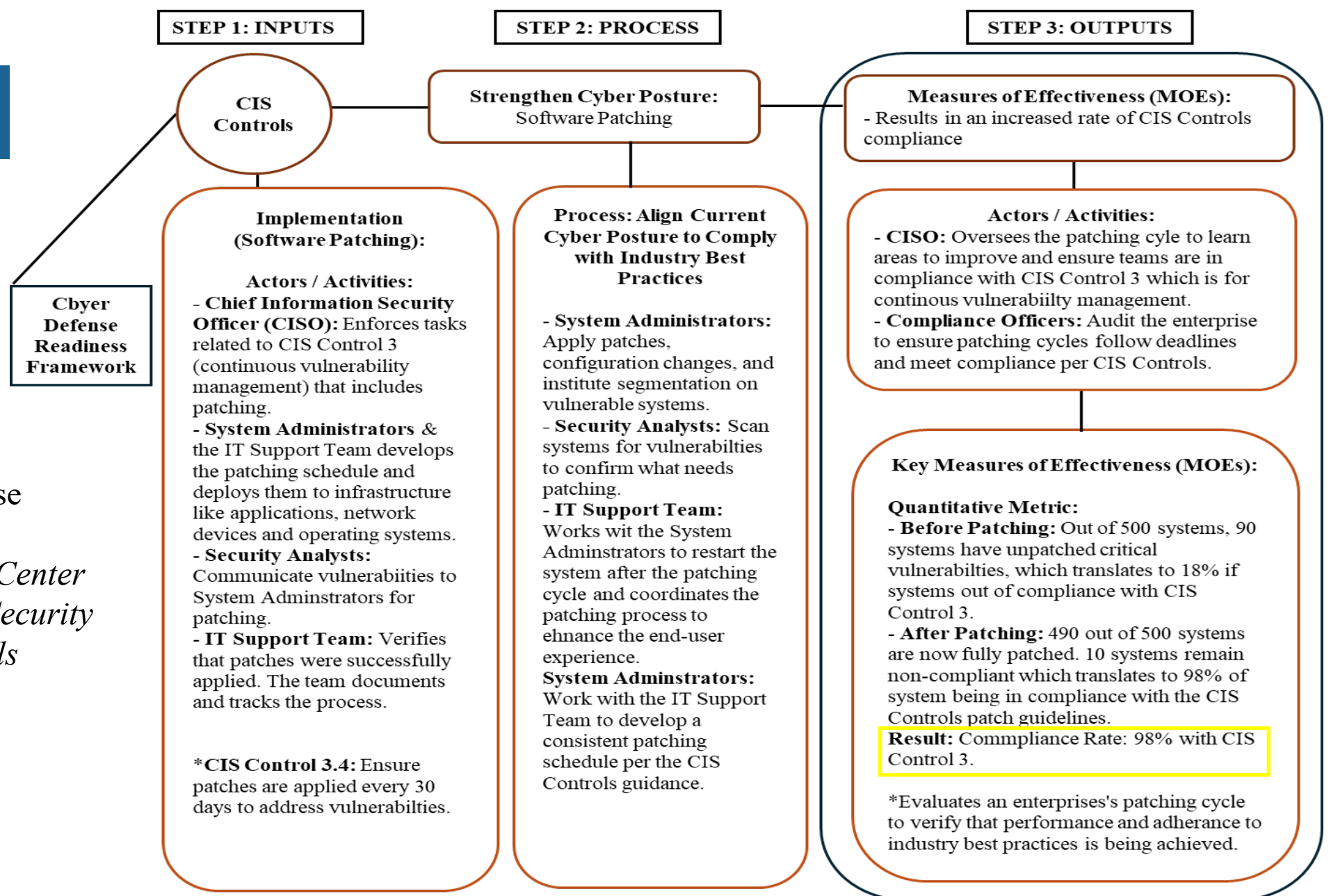
# Analysis



**Figure 6.**  
*Cyber Defense Readiness Framework: (ISO/IEC) 27001:2013 – Information Security Management Systems*

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS’s Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# Analysis



**Figure 7.**  
Cyber Defense Readiness Framework: *Center for Internet Security (CIS) Controls*

# Results / Conclusion

**Today's Goal:** To examine the way that the private sector assesses KPIs to see how it can enhance current methods that USCYBERCOM uses for assessing MOEs. Combining frameworks identifies best practices and methods for fortifying the cybersecurity posture of USCYBERCOM operations.

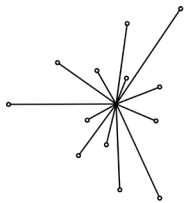
**Results:** Success! Research supports that the methods which the private sector uses can be integrated as an assessment approach for USCYBERCOM to enhance cyber operational effectiveness.

**Future research supports:** Upskilling / Retaining / Recruiting Cyber Talent, National Security and Defense, as well as fortifying US cybersecurity posture as the cyberthreat landscape evolves.



# Thank You! | Questions?

## LORI D. COOMBS, MBA, MSE



**WWCM**

Science.Technology.Engineering.Art.Math

<https://wwcapmgmt.com>

[contact@wwcapmgmt.com](mailto:contact@wwcapmgmt.com)



**WWCM ACADEMY**

Science.Technology. Engineering. Art. Math

<https://wwcmacademy.org>

[contact@wwcmacademy.org](mailto:contact@wwcmacademy.org)



**CyberJobs**

<https://cyberjobs.world>

[contact@cyberjobs.world](mailto:contact@cyberjobs.world)

LinkedIn: <https://www.linkedin.com/in/lori-d-coombs/>  
MARYMOUNT UNIVERSITY: [LDC72459@marymount.edu](mailto:LDC72459@marymount.edu)  
UNIVERSITY of ARIZONA Global Campus: [Lori.Coombs@faculty.uagc.edu](mailto:Lori.Coombs@faculty.uagc.edu)



# BACK-UP SLIDES



Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOM's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# Key Terms

<b>Acronym / Term</b>	<b>Definition / Meaning</b>
AI	Artificial Intelligence
ART	Agile Release Train
C6ISR	Command, Control, Comms, Computers, Cyber-Defense, Combat Systems, Intelligence, Surveillance and Reconnaissance
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
CO	Command Operations
CSF	Cybersecurity Framework
DoDIN	Department of Defense Information Network
EDR	Endpoint Detection and Response
GPS	Global Positioning System
IDS/IPS	Intrusion Detection/Prevention Systems
IRT	Incident Response Team
ISMS	Information Security Management System
IP	Internet Protocol
JCIDS	Joint Capabilities Integration and Development System

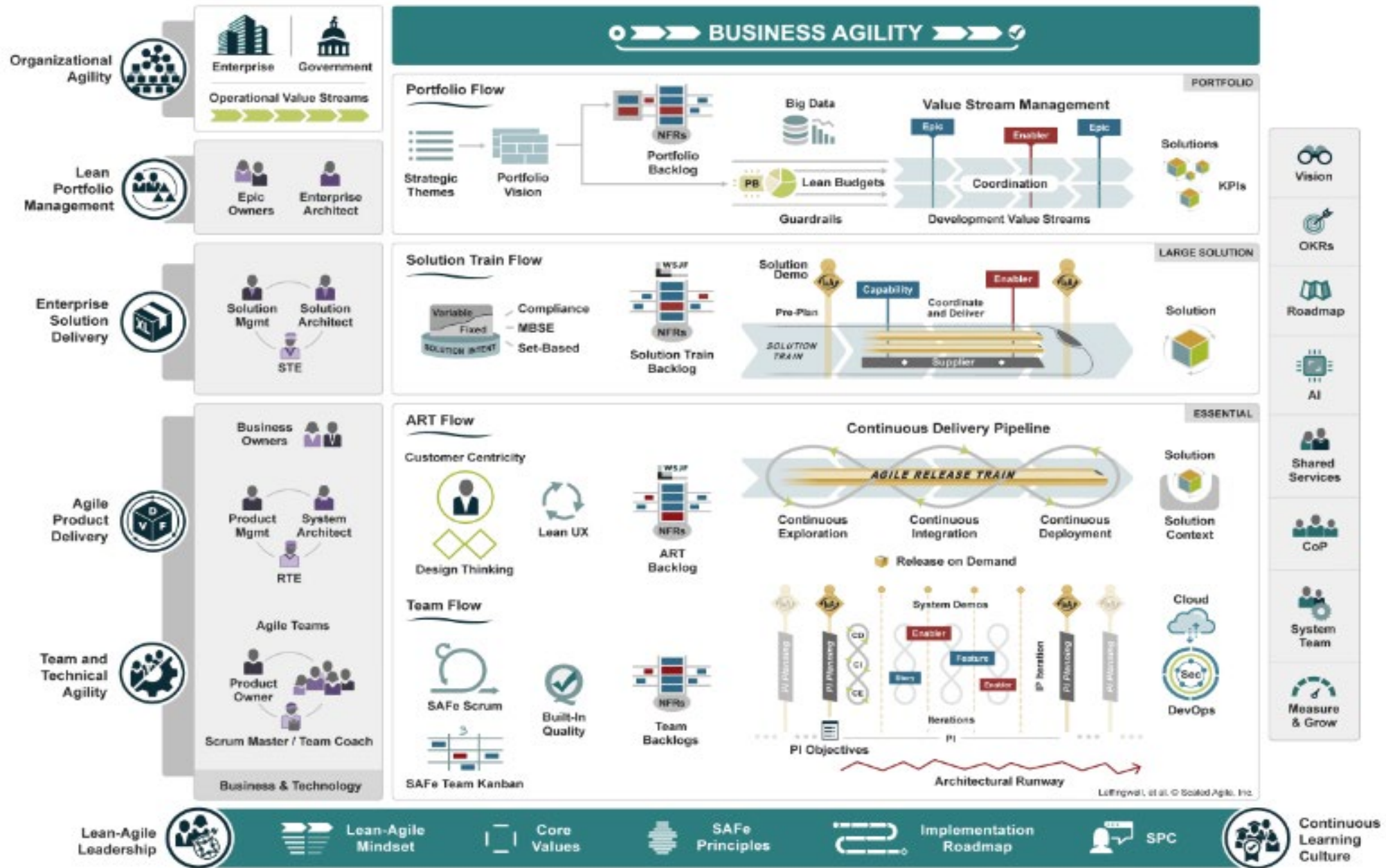
Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# Key Terms

<b>Acronym / Term</b>	<b>Definition / Meaning</b>
JCIDS	Joint Capabilities Integration and Development System (JCIDS)
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
MIL-STD	Military Standard
ML	Machine Learning
MOE	Measure of Effectiveness
MTBF	Mean Time Between Failures
MTTD	Mean Time to Detect
MTTR	Mean Time To Respond
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
ROI	Return on Investment
SAFe	Scaled Agile Framework
SIEM	Security Information and Event Management
SOC	Security Operations Center
USCYBERCOM	United States Cyber Command
WSUS	Windows Server Update Services

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOM's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# SAFe 6.0



Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOM's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# References

AcqNotes. MOEs. AI generated definitions based on acqnotes career fields. [https://acqnotes.com/acqnote/careerfields/se-measures-of-effectiveness#:~:text=Measures%20of%20Effectiveness%20\(MOE\)%20are,system%20will%20perform%20as%20required](https://acqnotes.com/acqnote/careerfields/se-measures-of-effectiveness#:~:text=Measures%20of%20Effectiveness%20(MOE)%20are,system%20will%20perform%20as%20required).

Andress, J. Winterfeld, S. (2014). Measures of Effectiveness. ScienceDirect. Cyber Doctrine. AI generated definitions based on Cyber Warfare (Second Edition), 2014. <https://www.sciencedirect.com/topics/computer-science/measures-of-effectiveness>

Al-Rodhan, N., (2020). The Space Review. Cyber Security and Space Security.

Alruwaili, A. (2019). A Review of the Impact of Training on Cybersecurity Awareness. International Journal of Advanced Research in Computer Science; Udaipur Vol. 10, Iss. 5, (Sep 2019): 01-03. DOI:10.26483/ijarcs.v10i5.6476

Bailey, B., Speelman, R. Doshi, P., Cohen, N., Wheeler, W. (2019). Center for Space Policy and Strategy. Aerospace Corporation. Defending Spacecraft in the Cyber Domain.

Bonnie, E., Gutierrez, R. (2024). The Ultimate Guide to Managing Multi-Framework Compliance: Best Practices & Strategies.

<https://secureframe.com/blog/multi-framework-compliance>

Bowen, B., Stolfo, S., Devarajan, R. (2012). Measuring the Human Factor of Cyber Security. Homeland Security Affairs. Monterey Vol 8.

Burns, L. (2019). Defense Budget Coverage – Air Warfare, Networks/Cyber, Space. US Must Improve Cyber Protection for SAT: Aerospace Corp.

Conca, J. (2023). China Has 'First-Strike' Capability To Melt U.S. Power Grid With Electromagnetic Pulse Weapon. Forbes. <https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse/?sh=25925c2ee190>

CyberSeek. National Initiative for Cybersecurity Education (NICE).

Defending Spacecraft in the Cyber Domain. The Aerospace Corporation, 2019.

Fort Moore. (2014). [https://www.moore.army.mil/armor/earmor/content/issues/2014/oct\\_dec/Westphal.html](https://www.moore.army.mil/armor/earmor/content/issues/2014/oct_dec/Westphal.html)

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# References

Gillette, A. (2021) Wilson Center, Insight & Analysis – CTRL Forward. From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space.

Hatzivasilis, George; Ioannidis, Sotiris; Smyrlis, Michail; Spanoudakis, George; Frati, Fulvio ; et al. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences; Basel Vol. 10, Iss. 16, (2020): 5702. DOI:10.3390/app10165702

Hayhurst, K. and Holloway, C. (2002). Proceeding of the 26th Annual NASA Goddard Software Engineering Workshop (SEW'01). Challenges in Software Aspect of Aerospace Systems

How to Manage Multiple Cybersecurity Compliance Frameworks Without Being Overwhelmed. Hyperproof. <https://hyperproof.io/resource/manage-security-compliance-frameworks/>

IBM Sterling Supply Chain Suite, 2023. Retrieved from: <https://www.ibm.com/topics/supply-chain-management>

Joint Capabilities Integration and Development System. (JCIDS). 2025. <https://www.dau.edu/aquipedia-article/joint-capabilities-integration-and-development-system-jcids>

King, M. and Goguichhili, S. (2020). Wilson Center, CTRL Forward. Cybersecurity Threats in Space: A Roadmap for Future Policy.

Kirova, Denitsa; Baumöl, Ulrike. (2018). Factors that Affect the Success of Security Education, Training, and Awareness

Programs: A Literature Review. JITTA : Journal of Information Technology Theory and Application; Hong

Kong Vol. 19, Iss. 4, (Dec 2018): 56-82.

Kuchler, Hannah. (2017). Trump executive order aims to protect US from 'catastrophic' cyber attack FT.com; London (May 25, 2017).

Lee, M. (2012). Securing the human to protect the system: human factors in cyber security. IET Conference Proceedings; Stevenage : The Institution of Engineering & Technology. (Oct 15, 2012) DOI:10.1049/cp.2012.1519

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# References

Machi, L. and McEvoy, B. (2022). The Literature Review – Fourth Edition.

Michael, T. (2024). Cybersecurity Frameworks Comparison: 10 Common Frameworks.

Morgan, S. (2021). Cybersecurity Jobs. Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025. <https://cybersecurityventures.com/jobs-report-2021/>

National Cyber Strategy. (2023).

National Institute of Standards & Technology in the U.S. Dept of Commerce. <https://tolumichael.com/cybersecurity-frameworks-comparison/>

NIST Framework - NIST Risk Assessment: <https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions>

NIST Risk Management Framework at <https://csrc.nist.gov/projects/risk-management/about-rmf>

NQA. information security implementation guide. (2013). [https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27001-Implementation-Guide\\_NON-UK.pdf](https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27001-Implementation-Guide_NON-UK.pdf).

Parker, J. (2025). Can organisations combine multiple cybersecurity frameworks? <https://www.jamesparker.dev/can-organisations-combine-multiple-cybersecurity-frameworks/>

Proctor, Wesley R. (2016). Investigating the efficacy of cybersecurity awareness training programs. Utica College ProQuest Dissertations & Theses, 2016. 10103886.

Rothke, B. (2023). Is there really an information security jobs crisis? Medium. <https://brothke.medium.com/is-there-really-an-information-security-jobs-crisis-a492665f6823>

SAFe 6.0 Provided by Scaled Agile. (2025). <https://www.scaledagileframework.com/posters/>

Tehila, S. (2023). Cybersecurity As A Strategic Investment: How ROI Optimization Can Lead To A More Secure Future. Forbes

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE

# References

- Technology Council. Forbes. <https://www.forbes.com/councils/forbestechcouncil/2023/08/16/cybersecurity-as-a-strategic-investment-how-roi-optimization-can-lead-to-a-more-secure-future/>
- The 7 Biggest Cybersecurity Threats to Your Clients & Customers, Milosh, A., 2019.
- Urooj, B., Shah, M, Maple, C., Abbasi, M., and Riasat, S. (2022). Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms
- VanDerwerken, J., Ubell, R. (2011). Training on the Cyber Security Frontlines. Alexandria. Vol 65, Iss. 6 (Jun 2011): 46-50,6.
- Wang, S., Wan, J., Chen, H., Xiao, J. (2021). 2021 International Conference on Computer Information Science and Artificial Intelligence (CISAI). Analysis and Design of Aerospace Equipment Software Quality Construction.

# Appendix

## TABLES:

Table 1. Exploring Frameworks to Collectively Assess Cyber Poster for USCYBERCOM

## FIGURES:

Figure 1. Common Cyber-Attacks to Segments

Figure 2. A High-Level Taxonomy of the Cyber Defense Readiness Framework

Figure 3. Cyber Defense Readiness Framework: Risk Management Framework (RMF)

Figure 4. Cyber Defense Readiness Framework: Cybersecurity Maturity Maturation Certification (CMMC)

Figure 5. Cyber Defense Readiness Framework: NIST Cybersecurity Framework (CSF)

Figure 6. Cyber Defense Readiness Framework: (ISO/IEC) 27001:2013 – Information Security Management Systems

Figure 7. Cyber Defense Readiness Framework: Center for Internet Security Controls (CIS)

Evaluating the Measures of Effectiveness (MOEs) Associated with Human Systems Integration (HSI), Personalized Assessment, Education, and Training (PAE&T) of USCYBERCOMS's Existing Assessment Framework | PRESENTER: ASSOCIATE PROFESSOR LORI D. COOMBS, MBA, MSE