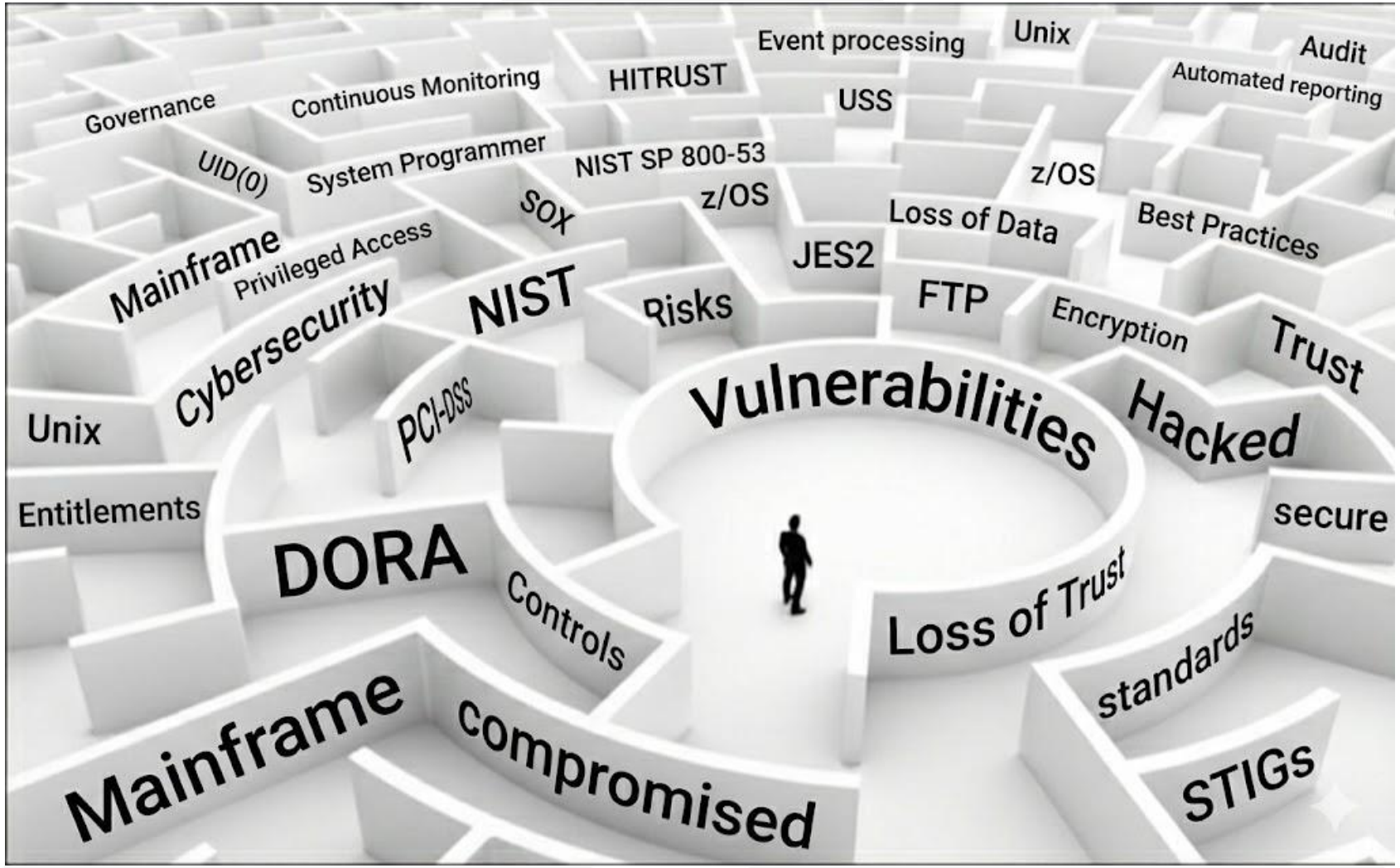
Mainframe Cybersecurity Governance: You Need a Robust Plan for a Typhoon-Free Future

Steve Hosie, CISSP-ISSAP, CISM, CRISC, CISA, CGEIT, CDPSE, PROJECT+
Cybersecurity Executive Advisor & Strategist | Cybersecurity Evangelist

Why, what, how, who, where and when?



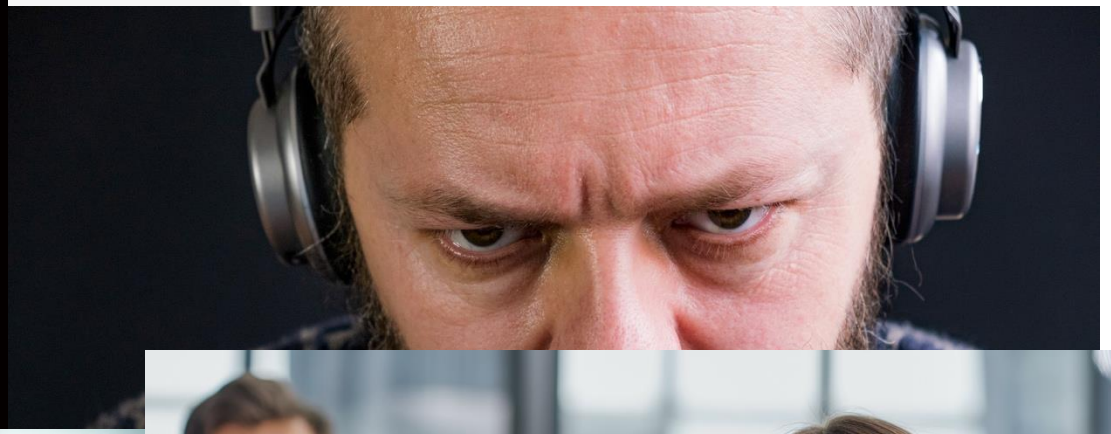
Dreaming

Double-Edge Sword – People, they are vital

Cybersecurity by Inheritance

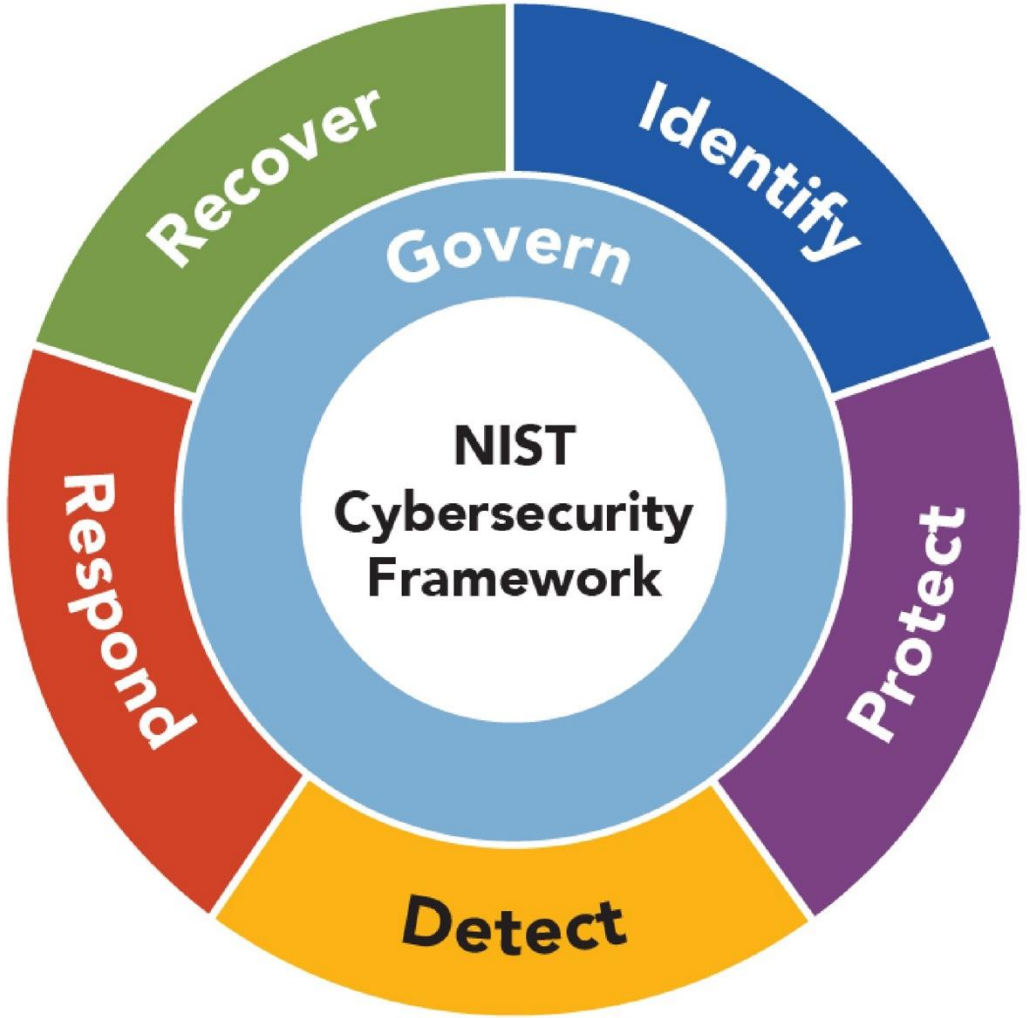
Standards

INSIDER THREATS



- Not an insider threat – yet… Just turned 13…

NIST CSF 2.0



GOVERN

Establishes the organizational structure, policies, and processes to manage cybersecurity risk.

This includes defining roles and responsibilities, ensuring compliance with regulations and aligning cybersecurity strategies with business objectives.

Mainframe Cybersecurity Governance Plan

Mainframe Cybersecurity Governance Plan

SHARE
EDUCATE • NETWORK • INFLUENCE

1. Mainframe Cybersecurity Standards
2. Security Continuous Monitoring
3. Mainframe Cybersecurity Database Protection
4. External Security Manager Exits
5. Infrastructure Role Access
6. Privileged Access Management
7. Hygiene of mainframe security database
8. Advanced Authentication on z/OS Mainframes
9. Cybersecurity Event Processing

Mainframe Cybersecurity Governance Plan

SHARE
EDUCATE • NETWORK • INFLUENCE

10. Automated Audit and Compliance Reporting
11. Organizational self-audit and validation
12. Mainframe Cybersecurity solution Maint.
13. Mainframe Cybersecurity database recovery
14. Encryption of Data at Rest/Data in Motion
15. Cybersecurity Incident Management on MF
16. Identity and Access Management (IAM) on MF
17. Disaster Recovery, Business Resumption
18. Knowledge Sharing (Training and Education)

Mainframe Cybersecurity Governance Plan

- Cybersecurity standards and best practices
- Infrastructure Roles
- Security Continuous Monitoring
- Privileged Access Management
- Hygiene of Security and Revalidation
- Security Event Processing
- Automated Audit and Compliance Reporting
- Knowledge Sharing (Training and Education)

Where can I obtain a copy?

- To obtain a copy of the draft Mainframe Cybersecurity Governance Plan, please contact Steve Hosie via email: Steven.Hosie@Broadcom.com

Join a Mainframe Technical Exchange

SHARE
EDUCATE • NETWORK • INFLUENCE

Apr. 21-23, 2026	June 23-25, 2026	Oct. 20-22, 2026
European MTE Prague, Czech Republic	Virtual MTE Held Virtually	North American MTE Plano, TX

- Network with peers and Mainframe technical experts
- Participate in technical how-to sessions and hands-on workshops
- No registration fee!

Important Cybersecurity Standard References

- NIST Cybersecurity 2.0 Framework – https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf and https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- NIST Special Publication 800-53 - https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- What is new in PCI DSS v4.0 - https://securityboulevard.com/2023/07/what-is-new-in-pci-dss-version-4-0-a-complete-guide-to-it/
- PCI DSS document library: https://www.pcisecuritystandards.org/document_library/?category=pcidss
- Summary of Changes from v3.2.1 to v4.0 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf
- PCI DSS Version 4.0 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- Broadcom Top Secret (TSS) STIG articles - https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-top-secret-for-z-os/16-0.html
- Broadcom ACF2 STIG articles - https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-top-secret-for-z-os/16-0.html
- CIS Benchmarks for RACF - https://www.cisecurity.org/benchmark/ibm_z

DORA Links

- Article 5, Governance and organisation, Digital Operational Resilience Act (DORA)
- Article 6, ICT risk management framework, Digital Operational Resilience Act (DORA)
- Article 7, ICT systems, protocols and tools, Digital Operational Resilience Act (DORA)
- Article 8, Identification, Digital Operational Resilience Act (DORA)
- Article 9, Protection and prevention, Digital Operational Resilience Act (DORA)
- Article 10, Detection, Digital Operational Resilience Act (DORA)
- Article 11, Response and recovery, Digital Operational Resilience Act (DORA)
- Article 12, Backup policies and procedures, restoration and recovery procedures and methods, Digital Operational Resilience Act (DORA)
- Article 13, Learning and evolving, Digital Operational Resilience Act (DORA)
- Article 14, Communication, Digital Operational Resilience Act (DORA)
- Article 15, Further harmonisation of ICT risk management tools, methods, processes and policies, Digital Operational Resilience Act (DORA)
- Article 16, Simplified ICT risk management framework, Digital Operational Resilience Act (DORA)

Speaker Info

Steve Hosie
Cybersecurity Strategist
Indian Hills, Colorado USA
Direct: +1 303 517 8645
Steven.Hosie@Broadcom.com
https://www.linkedin.com/in/stevehosie/

Who is Steve?

- Dad to two amazing individuals, Husband, Friend and Mentor to many, and a US Marine Corps Veteran.
- Credentials: CISSP-ISSAP, CISM, CISA, CGEIT, CRISC, CDPSE
- 39+ years as an active security practitioner in mainframe cybersecurity and compliance.
- Provides Mainframe cybersecurity advisement to Broadcom clients worldwide
- https://www.facebook.com/groups/ProfessionalMainframers/ FB group with over 36,000 members and growing.
- Mainframe Cybersecurity and Compliance Professionals - https://www.linkedin.com/groups/36083/
- Organizer of "Veterans in IT" group on Linkedin
- Founder of the world's largest social media group of USMC Veterans with over 147,000 members and growing.

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation

THANK YOU