# Cyber Defense

Best Practices

# Agenda

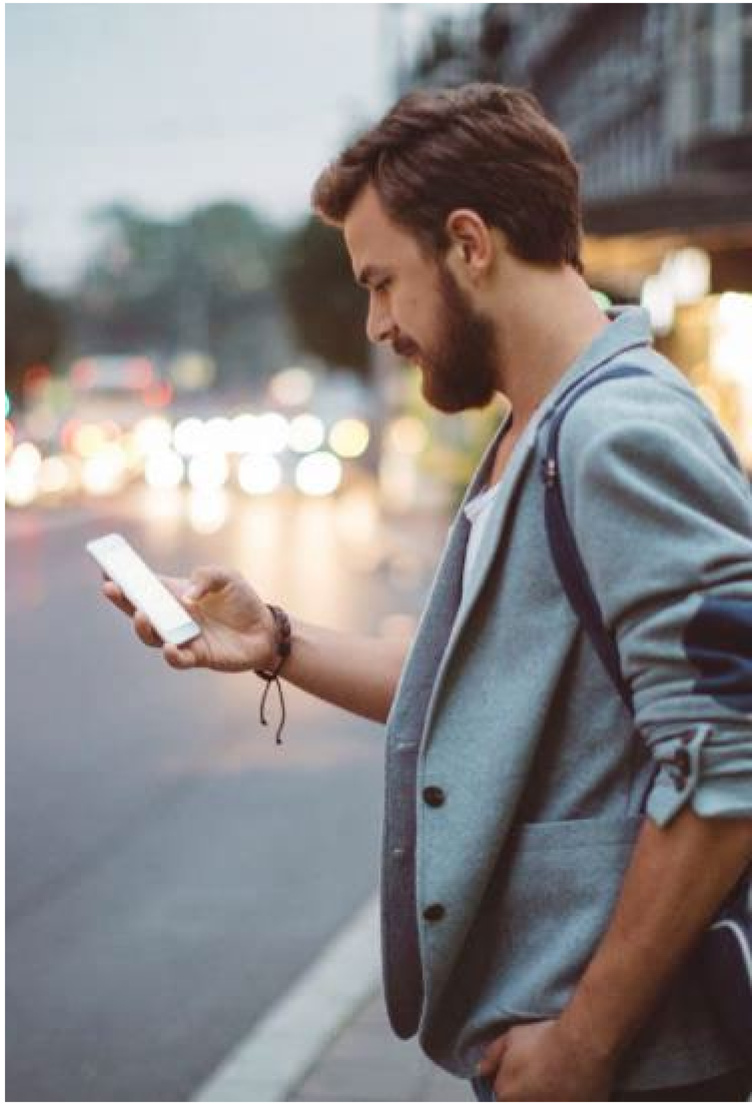
Security is a FEELING

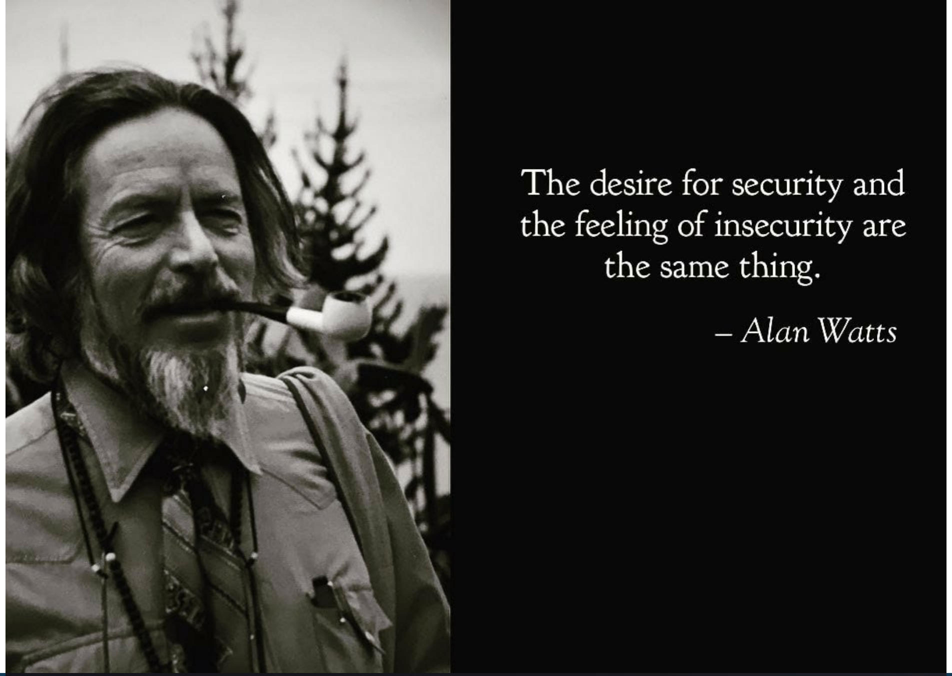
Defense in Depth

Least Privilege / Zero Trust

McCumber Cube (CIA, TPP, and Data); AAA

Example Frameworks (NIST, ISO, and others)

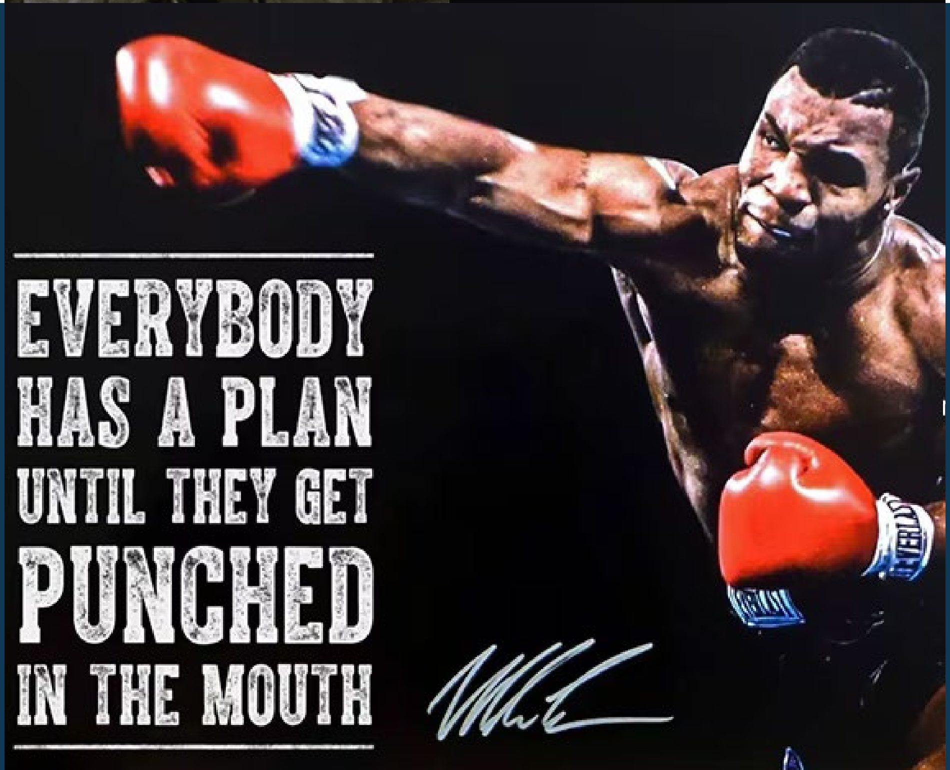




The desire for security and the feeling of insecurity are the same thing.

– *Alan Watts*

# Security is a FEELING



EVERYBODY HAS A PLAN UNTIL THEY GET PUNCHED IN THE MOUTH

*Security is both a feeling and a reality,*
*and they're different.*

*You can feel secure even though you're not.*

*You can be secure even though you don't feel it.*

# DEFENSE IN DEPTH

**Developing a defensive strategy**

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization -NIST

- Defined Organization
- Risk Appetite
- Top-Down Implementation
- Business Continuity Plan (BCP)
- Disaster / Recovery Plan

https://www.youtube.com/watch?v=Rmps-hVxZ5s

# Zero Trust / Least Privilege

**Click to add title here**

- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Phasellus auctor efficitur dui et facilisis.
- Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.
- Etiam molestie in quam ac viverra.
- Cras consequat gravida aliquam. Maecenas cursus eleifend risus, in vulputate velit imperdiet non.Etiam molestie in quam ac viverra.

# Access Authentication Auditing

# McCumber Cube

Information Assurance

The concept of this model is to devise a robust information assurance program; one must consider not only the security goals of the program but also how these goals relate specifically to the various states in which information can reside in a system and the full range of available security safeguards that must be considered in the design. The McCumber model helps one to remember to consider all important design aspects without becoming too focused on any one in particular

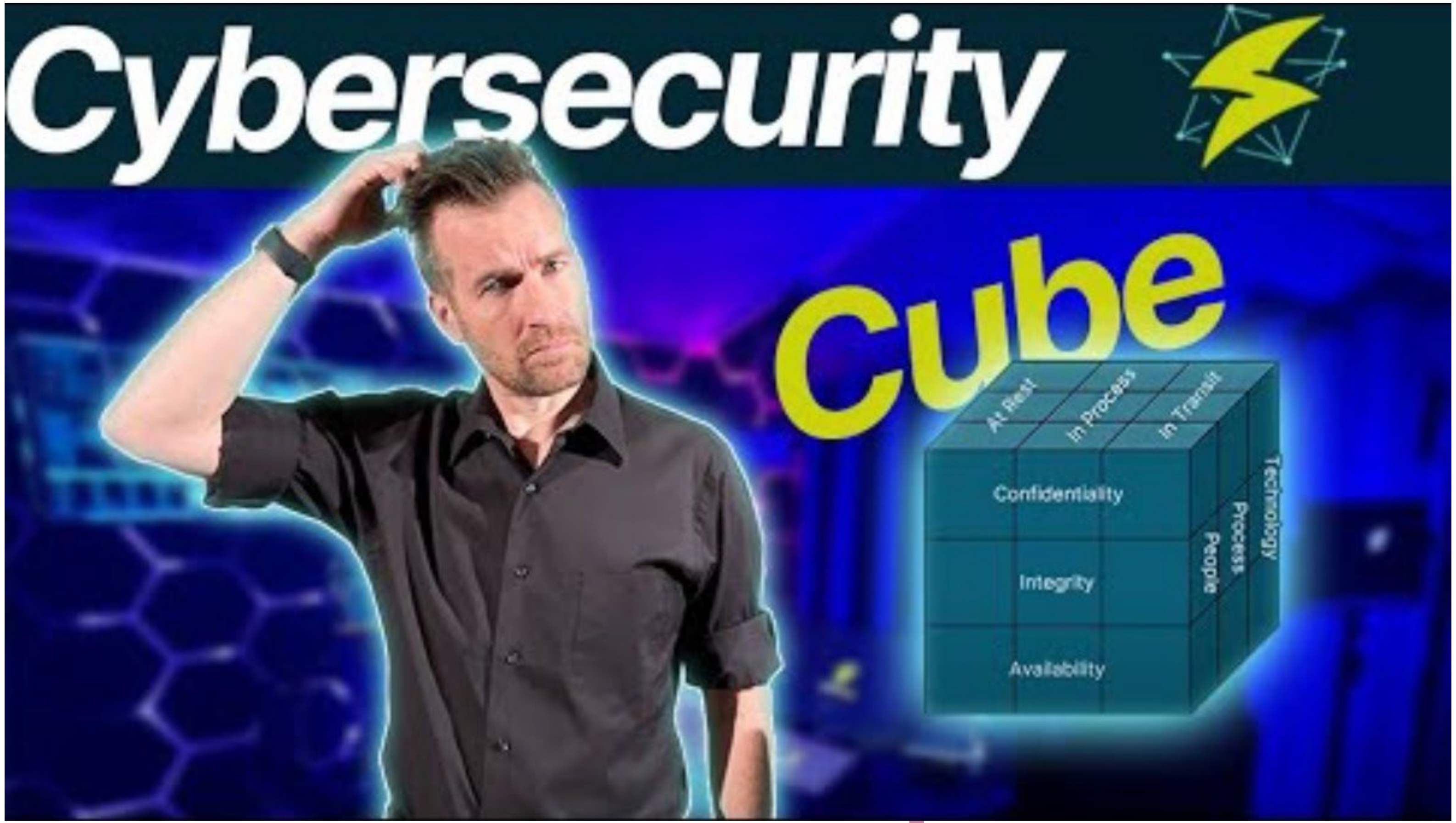
https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad

Confidentiality, Integrity, and Availability (CIA) Triad

People, Processes, and Technology (PPT) Defense

At Rest, In Process, In Transit (Data)

Cybersecurity Frameworks

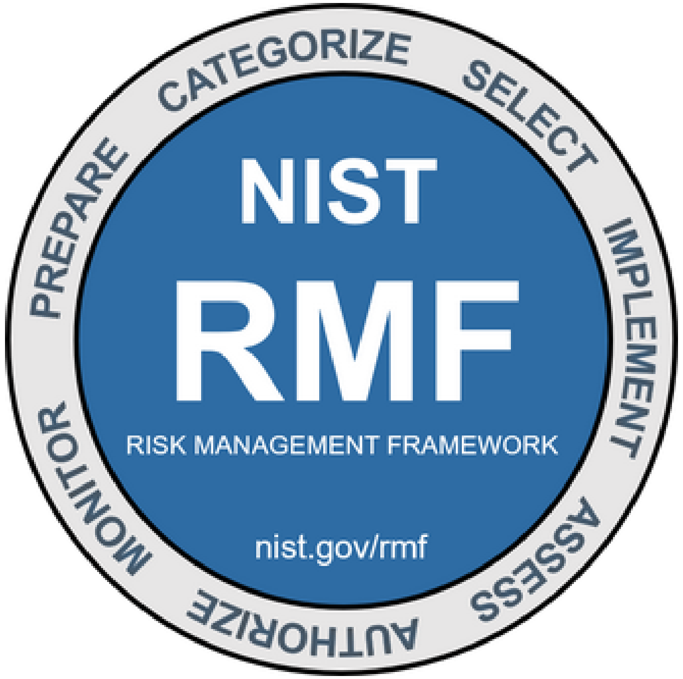


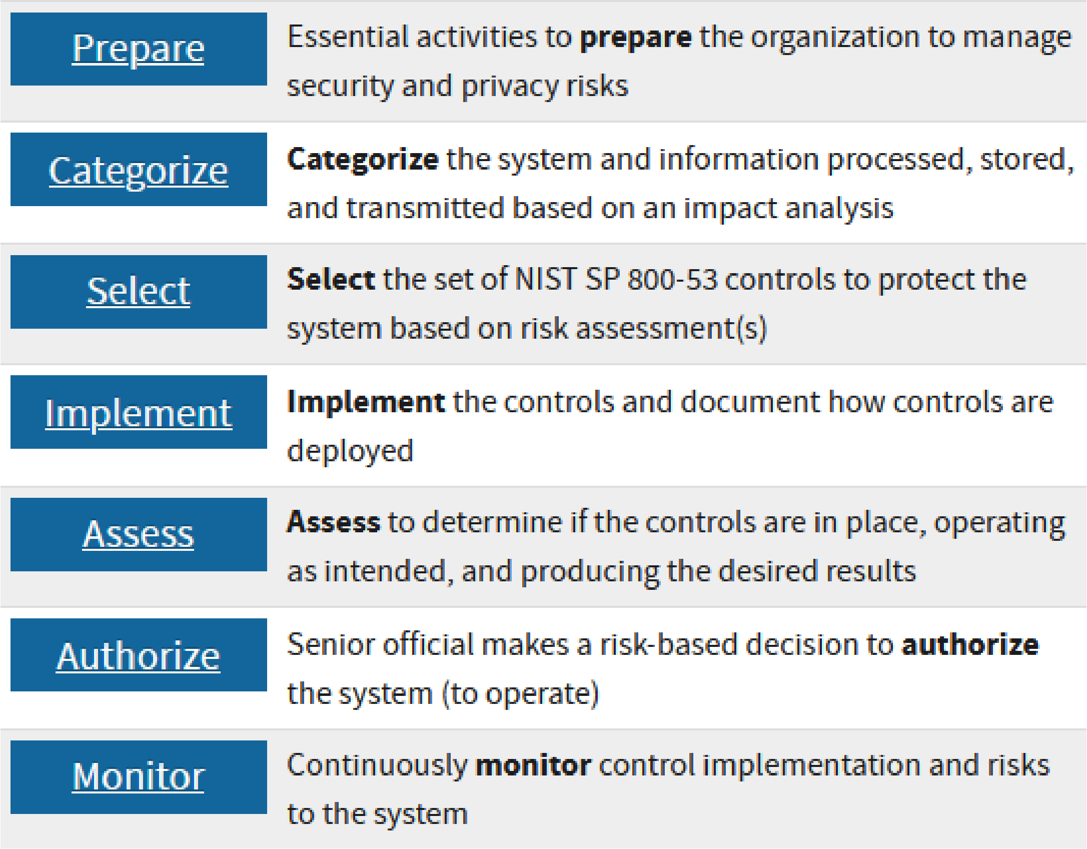
# McCumber Cube overview

# NIST Frameworks

Risk Management Framework (RMF)

Cybersecurity Framework (CSF)





| | |
|---|---|
| Prepare | Essential activities to **prepare** the organization to manage security and privacy risks |
| Categorize | **Categorize** the system and information processed, stored, and transmitted based on an impact analysis |
| Select | **Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s) |
| Implement | **Implement** the controls and document how controls are deployed |
| Assess | **Assess** to determine if the controls are in place, operating as intended, and producing the desired results |
| Authorize | Senior official makes a risk-based decision to **authorize** the system (to operate) |
| Monitor | Continuously **monitor** control implementation and risks to the system |

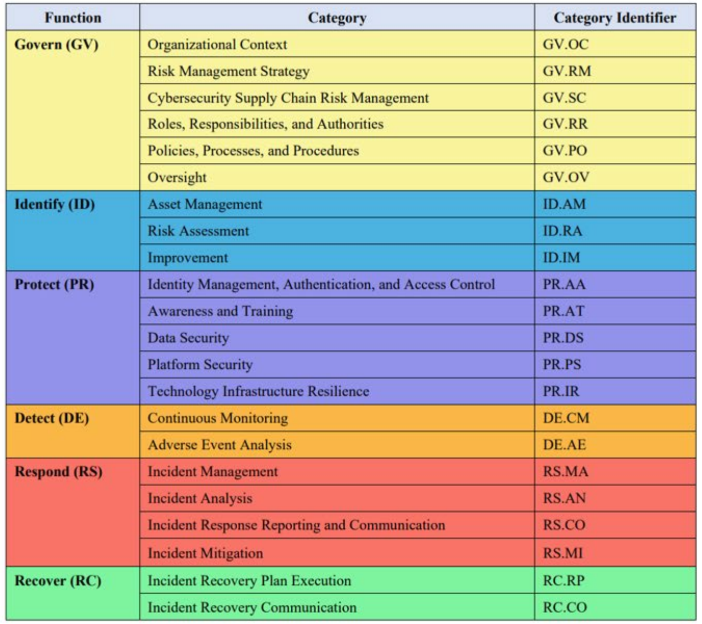
# NIST Risk Management Framework (RMF)

https://csrc.nist.gov/projects/risk-management

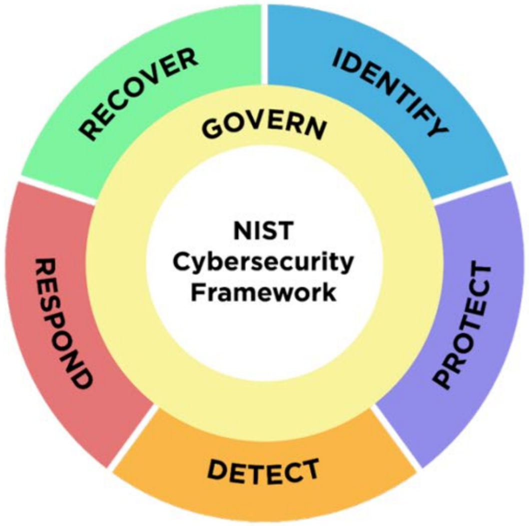
# NIST Risk Management Framework

https://www.youtube.com/watch?v=d8Z1RyhmRXg

# NIST Cybersecurity Framework (CSF)



| Function | Category | Category Identifier |
|---|---|---|
| Govern (GV) | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policies, Processes, and Procedures | GV.PO |
| | Oversight | GV.OV |
| Identify (ID) | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Improvement | ID.IM |
| Protect (PR) | Identity Management, Authentication, and Access Control | PR.AA |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Platform Security | PR.PS |
| | Technology Infrastructure Resilience | PR.IR |
| Detect (DE) | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| Respond (RS) | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| Recover (RC) | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |



https://www.nist.gov/cyberframework

# NIST Cybersecurity Framework (CSF)

https://www.youtube.com/watch?v=Ula3TG8QS7g

# Thank You !