SecureIdeas
professionally evil®

Hands-on with the NIST Cybersecurity Framework 2.0

Nathan Sweaney

Nathan Sweaney

- Principal Consultant – Secure Ideas
- Renaissance Hacker
- BSidesOK Organizer/Founder
- General Nuisance

- Other Interests
  - American Politics
  - History & Culture of the Middle East
  - Movies that begin with "Top Gun"
  - AI Overlords that you don't know by name yet

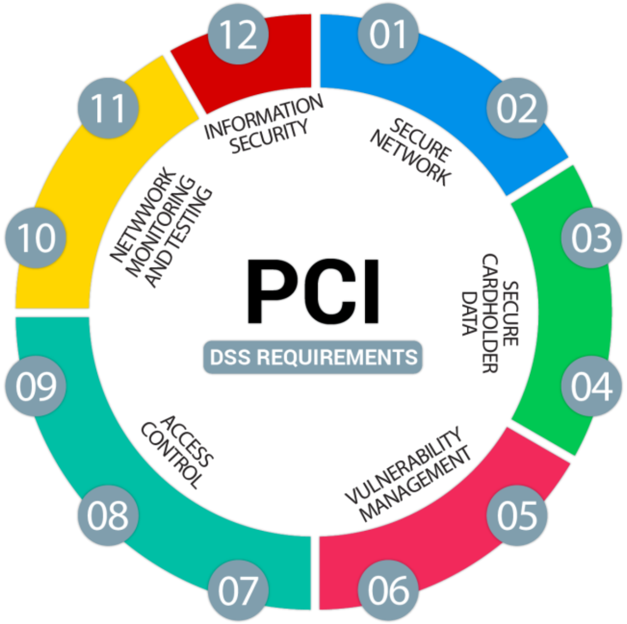
- nathan@secureideas.com
- @sweaney

Copyright © 2023 Secure Ideas LLC

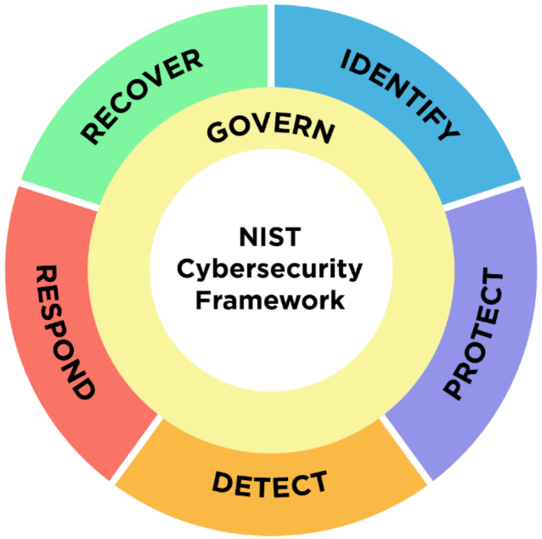
Why use a Security Framework?

- Improve Cybersecurity Maturity
- Objective & Unbiased Measurements
- Better Communication with ~~Muggles~~ Business Stakeholders
- Demonstrate Intentionality
- Have a Plan
  - Fail to plan == plan to fail

Other Common Frameworks



CIS Controls



ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

Copyright © 2023 Secure Ideas LLC

NIST CSF History

- Commissioned by President Obama in 2013 by Executive Order
  - ”Develop a voluntary framework to help protect critical infrastructure.”

- Extensive public-private collaboration process

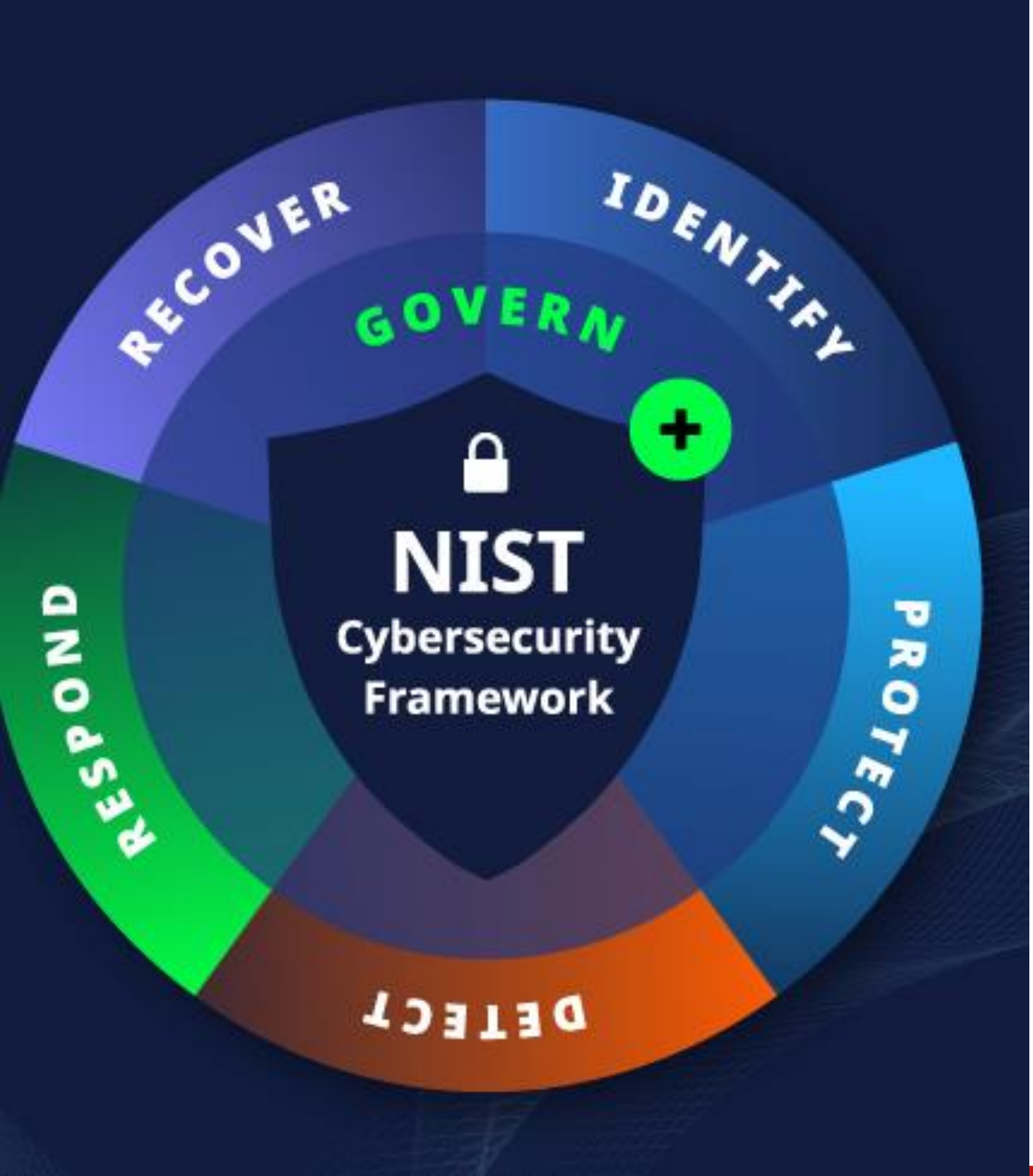
- v1.0 released in 2014
- V1.1 released in 2018
- v2.0 released in 2024

- More in-depth than CIS Controls
- More flexible than PCI DSS
- More thorough than Miter ATT&CK
- More focused than ISO 27001

Copyright © 2023 Secure Ideas LLC

Voluntary

Copyright © 2023 Secure Ideas LLC

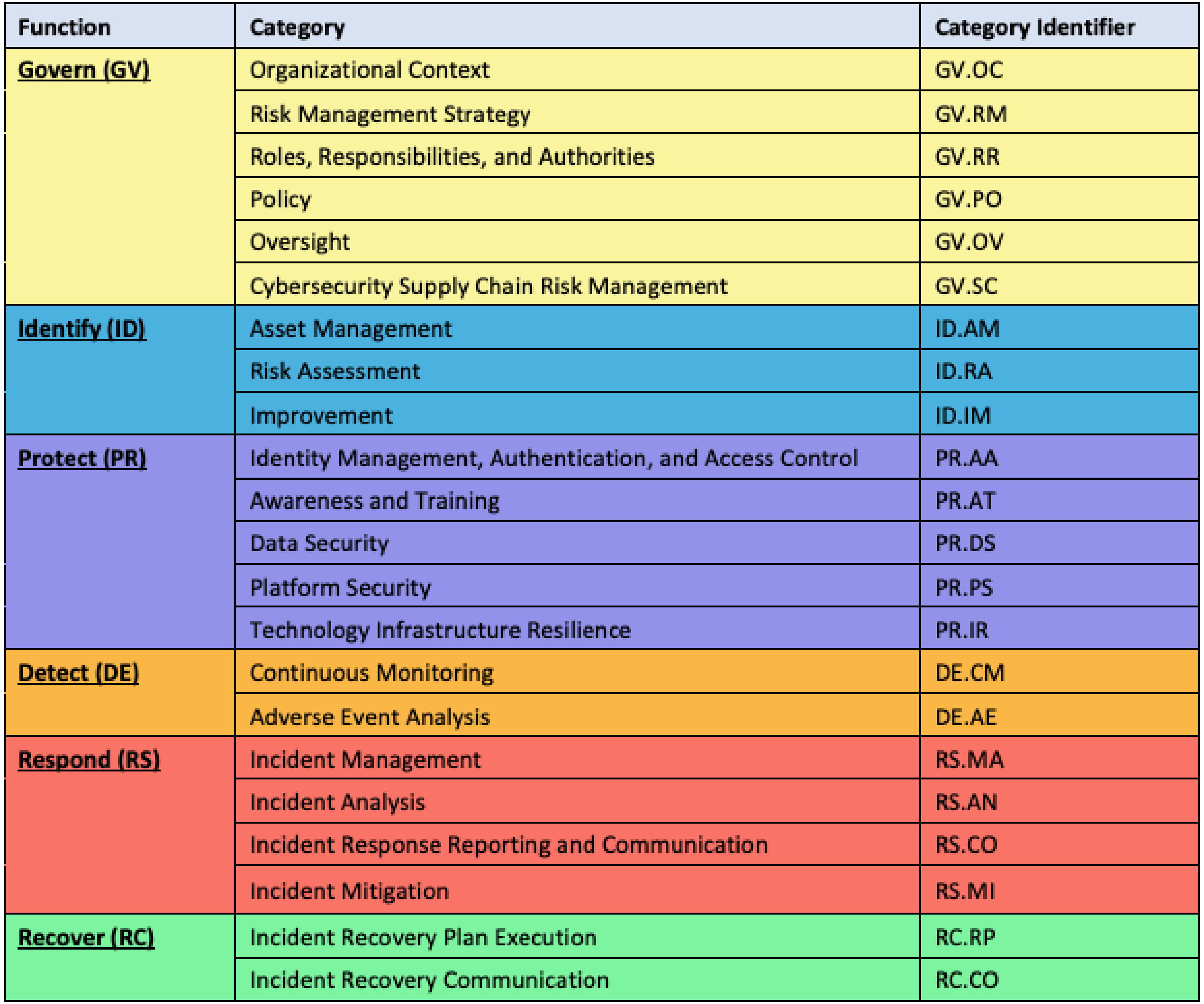


Core Functions

- **Govern (GV)**
  - Risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID)**
  - Current cybersecurity risks are understood.
- **Protect (PR)**
  - Safeguards to manage cybersecurity risks are used.
- **Detect (DE)**
  - Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS)**
  - Actions taken to address detected cybersecurity incidents
- **Recover (RC)**
  - Assets and operations affected by a cybersecurity incident are restored.

Hands-on

- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Short URL: https://doi.org/10.6028/NIST.CSWP.29
- https://www.nist.gov/cyberframework
- Or just search for NIST CSF 2.0



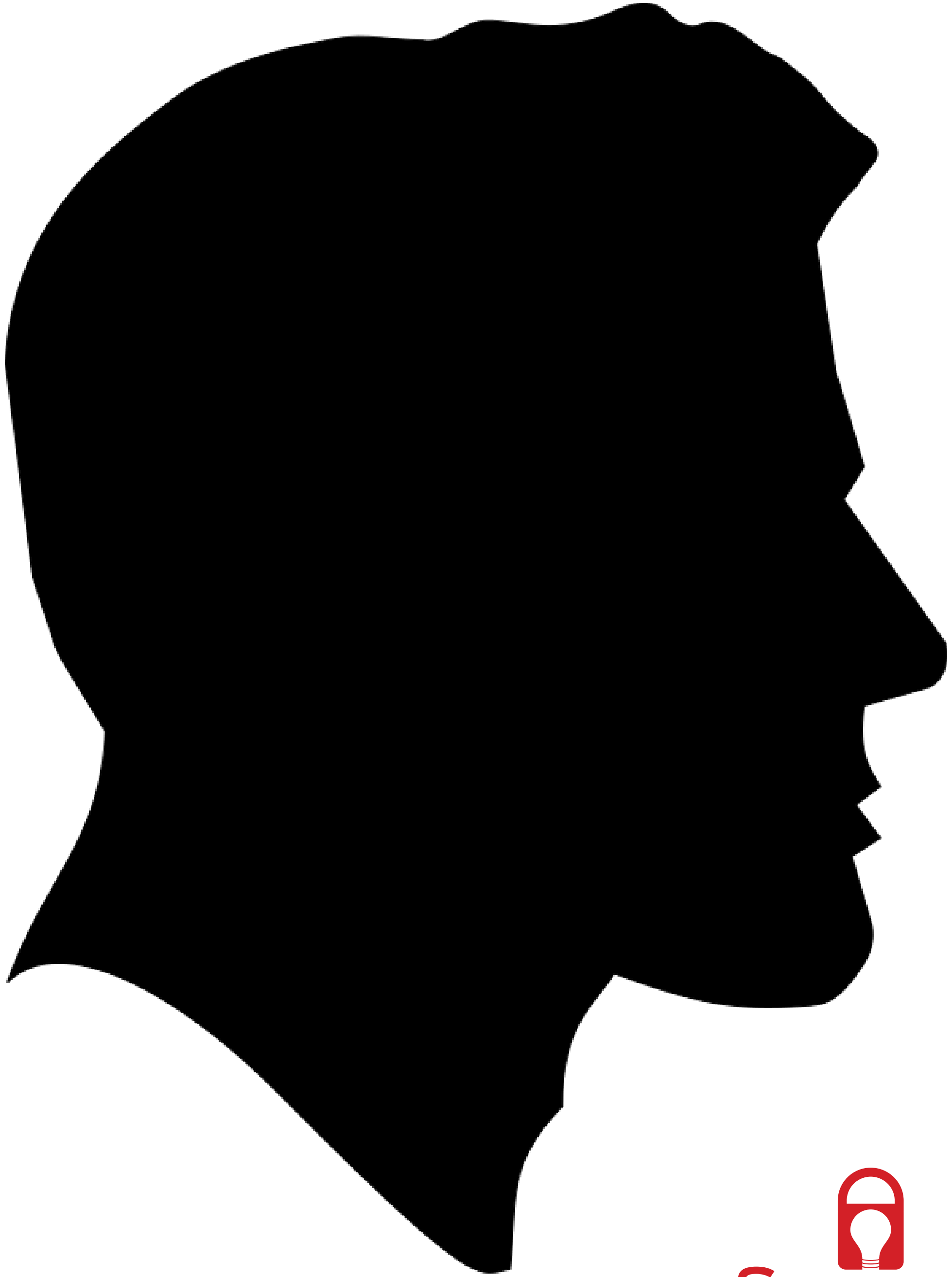
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	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

Objectives outlined in Appendix A (page 15).

Copyright © 2023 Secure Ideas LLC

Profiles

- Custom Tailoring
- Current Profile vs Target Profile
- Considerations:
  - Mission Objectives
  - Stakeholder Expectations
  - Organizational Priorities
  - Threat Landscape
  - Other Requirements
- Organizational Profile Template
- Quick-Start Guide for Creating and Using Organizational Profiles
- Examples of Community Profiles



Copyright © 2023 Secure Ideas LLC

Implementation Tiers (Appendix B)

Tier 1: Partial

- Ad hoc management
- Informal implementation
- Limited awareness

Tier 2: Risk Informed

- Management-approved, but not consistently established
- Prioritization based on objectives & threats
- Controls may not be repeatable or reoccurring

Tier 3: Repeatable

- Formally approved and expressed in policy
- Policies and processes are defined, implemented, and reviewed
- Regularly updated based on changing threats

Tier 4: Adapative

- Wide-scale acceptance and implementation
- Close bond with organizational objectives
- Risk management is accepted part of organizational culture

Copyright © 2023 Secure Ideas LLC

Additional Resources

- CSF 2.0 Reference Tool
  - Online searches or JSON/CSV export
  - https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters
- Cybersecurity and Privacy Reference Tool
  - In-depth searches of control terms & other NIST documents
  - https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home
- Cross-Reference Comparison Reports
  - https://csrc.nist.gov/Projects/olir/Coverage-Report#/olir/coverage-report

Next Steps

- Read the Framework
  - ~30 pages
  - Skim the objectives the first time through
- Quick Start Guides
  - https://www.nist.gov/quick-start-guides
- Start simple and build

Copyright © 2023 Secure Ideas LLC

Secure Ideas
professionally evil®

Questions