A NIST Cybersecurity Framework for Everyone: Presenting CSF 2.0

October 2025
San Diego

Techno Security & Digital Forensics Conference

Barry Hudson, CISSP
bhudsoncissp@gmail.com
bhudsoncissp.com
www.linkedin.com/in/barry-hudson-cissp-ab9b2136/

Presentation Outline

Aiken
UNIVERSITY OF SOUTH CAROLINA
Security Servers (Virus, Scanners, SIEM, Updates)
App Server VLAN
VPN
Security Server VLAN
Open Jack
Office PCs Bldg2 Subnet

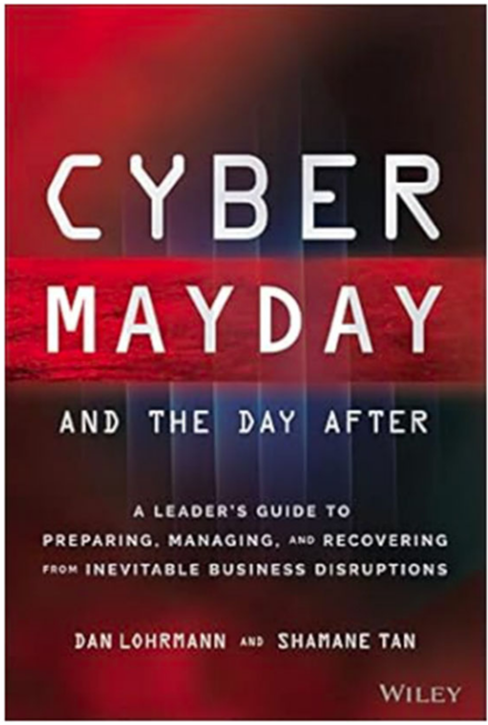
Barry Hudson, CISSP
Most Joyous and Passionate Cybersecurity Preacher
barry.hudson@usca.edu

- Some Questions to **Evaluate** Your Current Readiness
- **Why** You Should Consider a Framework (And Why You Might Not Have One)
- **Overview** of NIST Cybersecurity Framework (CSF 2.0)
- The **Six Functions** in CSF: Govern, Identify, Protect, Detect, Respond, Recover
  - A **Tour** of the Profile Spreadsheet
  - See one **Example** of Each Function
- **More resources**
  - **Navigating** The Framework Website and Beyond
  - Your **Next Steps**: Quick Start Guides and Profiles
- Summary and **Conclusions**
- **Questions**

Say Yes Sooner – Dan Lohrmann

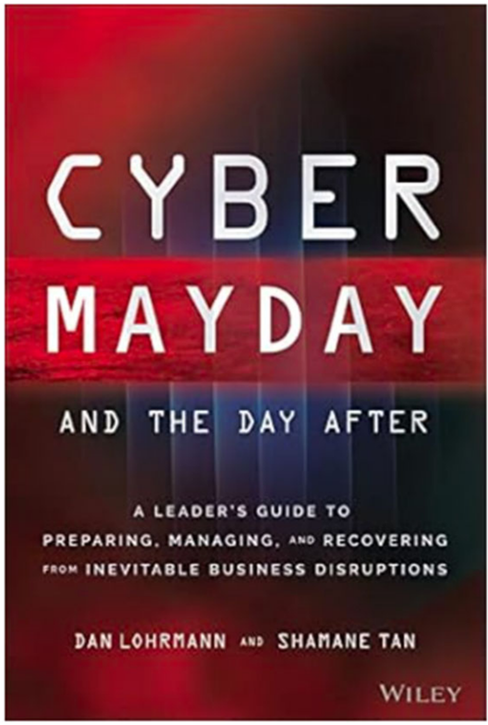
Cyber Shall Not Be An Obstacle
It is never too late to start

- I attended a talk by the Author and bought the book to read more of his and other's real-life experiences. There are numerous stories from the past 5 years about how the lax and complacent attitudes in upper management and even technical people result in successful cyber attacks. The book emphasizes the need for sharing (rather than hiding) what happened to help others respond to or prevent incidents.
- He remains perplexed why companies and individuals do not follow even the five simplest security measures, (covered later) and that very few have written or practiced the incident response playbooks.


CYBER MAYDAY
AND THE DAY AFTER
A LEADER'S GUIDE TO PREPARING, MANAGING, AND RECOVERING FROM INEVITABLE BUSINESS DISRUPTIONS
DAN LOHRMANN AND SHAMANE TAN
WILEY

10 excuses for inadequate security includes some real laughers…. (adapted from Dan Lohrmann)

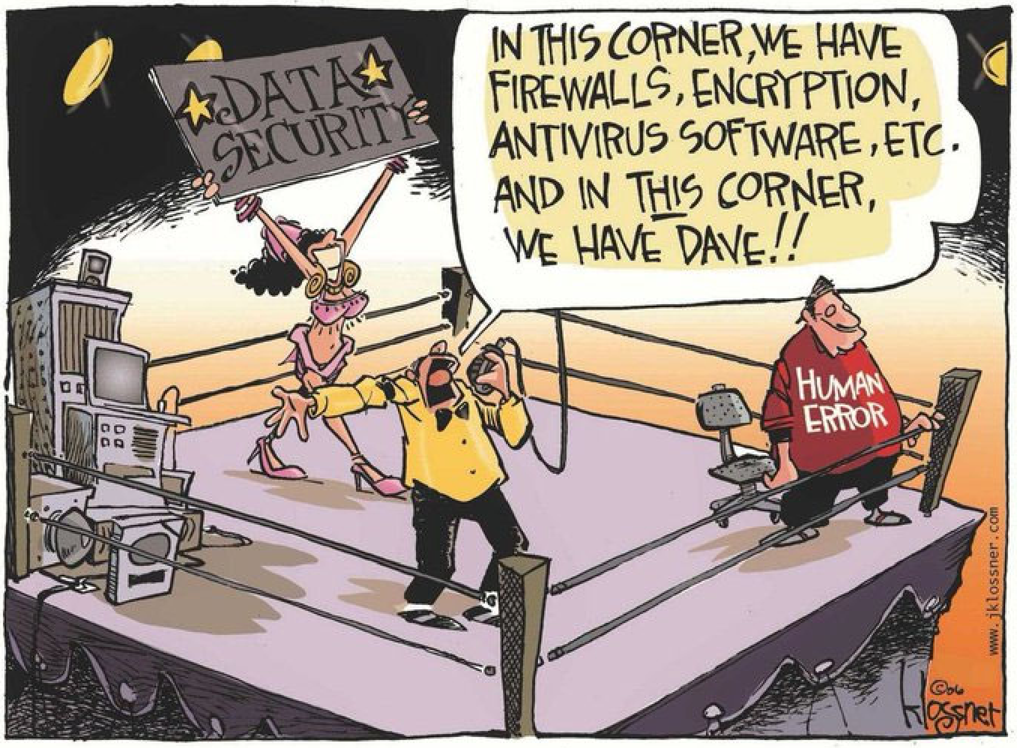
1. We did not have the time
2. We could not afford it, didn’t know where to start
3. Our company is different, not a probable target
4. We trusted our system vendor, said was not necessary
5. Our insurance will cover it
6. We have a firewall, so we're covered
7. It was too complicated and hard
8. We tried it before and it didn’t work
9. We were afraid of what we might discover
10. We thought we had a better way


CYBER MAYDAY
AND THE DAY AFTER
A LEADER'S GUIDE TO PREPARING, MANAGING, AND RECOVERING FROM INEVITABLE BUSINESS DISRUPTIONS
DAN LOHRMANN AND SHAMANE TAN
WILEY

Let's put a few things into perspective

- Companies and individuals do not follow even the five simplest security measures

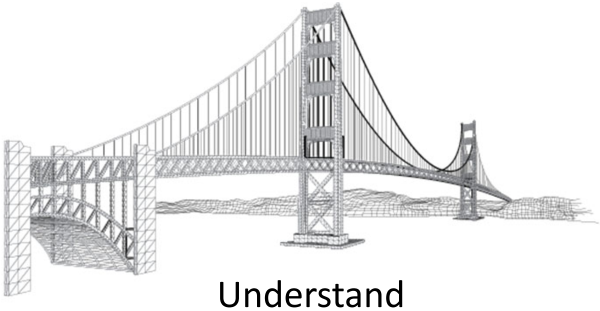
1. MFA (Multi-factor Authentication)
2. Change default passwords (variety of passwords, consider a password manager)
3. Encryption in transit and at rest
4. Testing security controls (make sure controls are effective)
5. Establishing need to know (don't tell everyone everything)
6. And our runner-up…. Train People to NOT BE DUMB (eg Recognize Phishing)


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Why You Should Consider a Framework

(And Why You Might Not Have One)

**If you think technology can solve your security problems…
then you don't understand the problems… and you don't understand the technology.
(Bruce Schneier)**

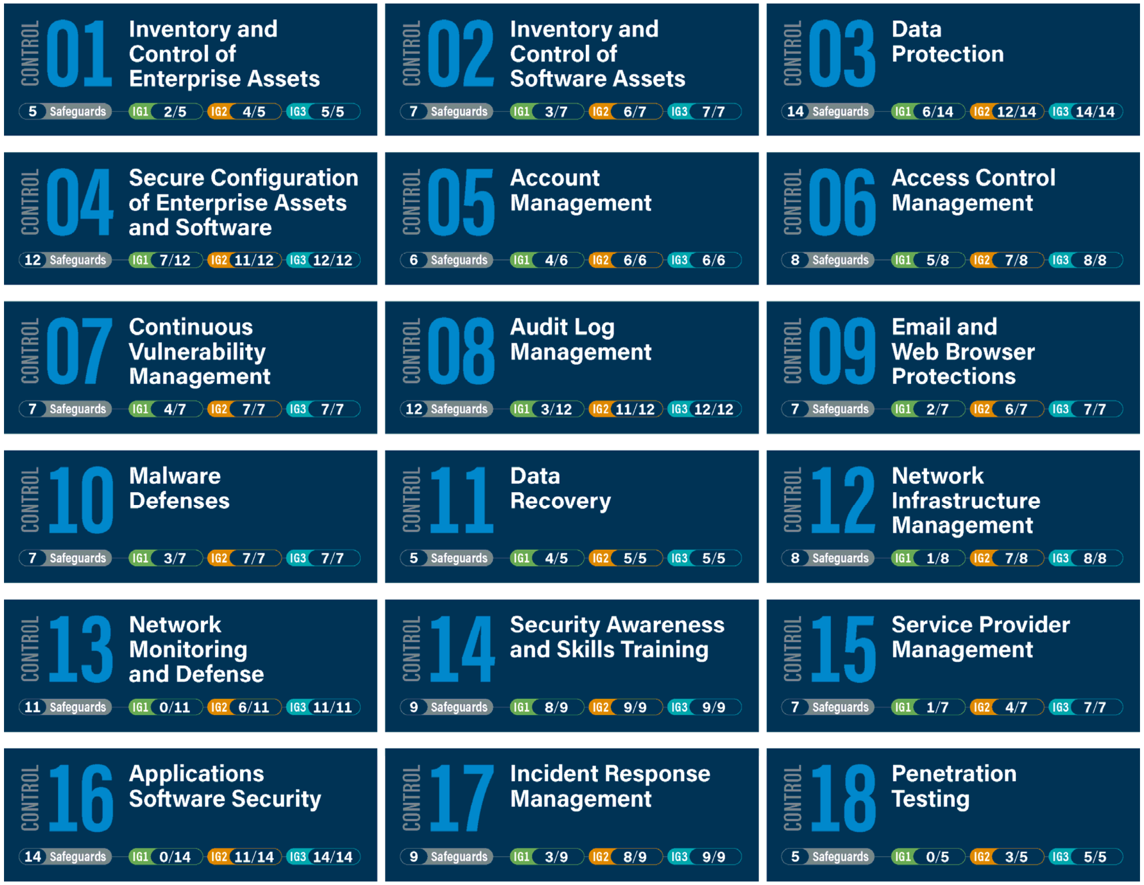


Understand
Assess
Prioritize
Communicate

- Manage and **reduce cybersecurity risks**
  - Companies that follow a framework achieve favorable compliance and security outcomes, report lower operational costs, less accepted risk, and better posture for defense and resiliency
- CSF assists its users in learning about and selecting **metrics and actions** to achieve specific outcomes
- Describe the current AND target cybersecurity postures
  - Determine **gaps**, and assess progress toward addressing those gaps
- Identify, organize, and **prioritize actions** for managing cybersecurity risks
  - Assure alignment with organization's mission
  - Consider legal and regulatory requirements, and risk management and governance expectations.

Read the book
One Second After

Another Framework to Consider: Center for Internet Security cisecurity.org esp. Multi-State Information Sharing and Analysis Center (MS-ISAC)



Control		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

CIS. Center for Internet Security®

Creating Confidence in the Connected World.™

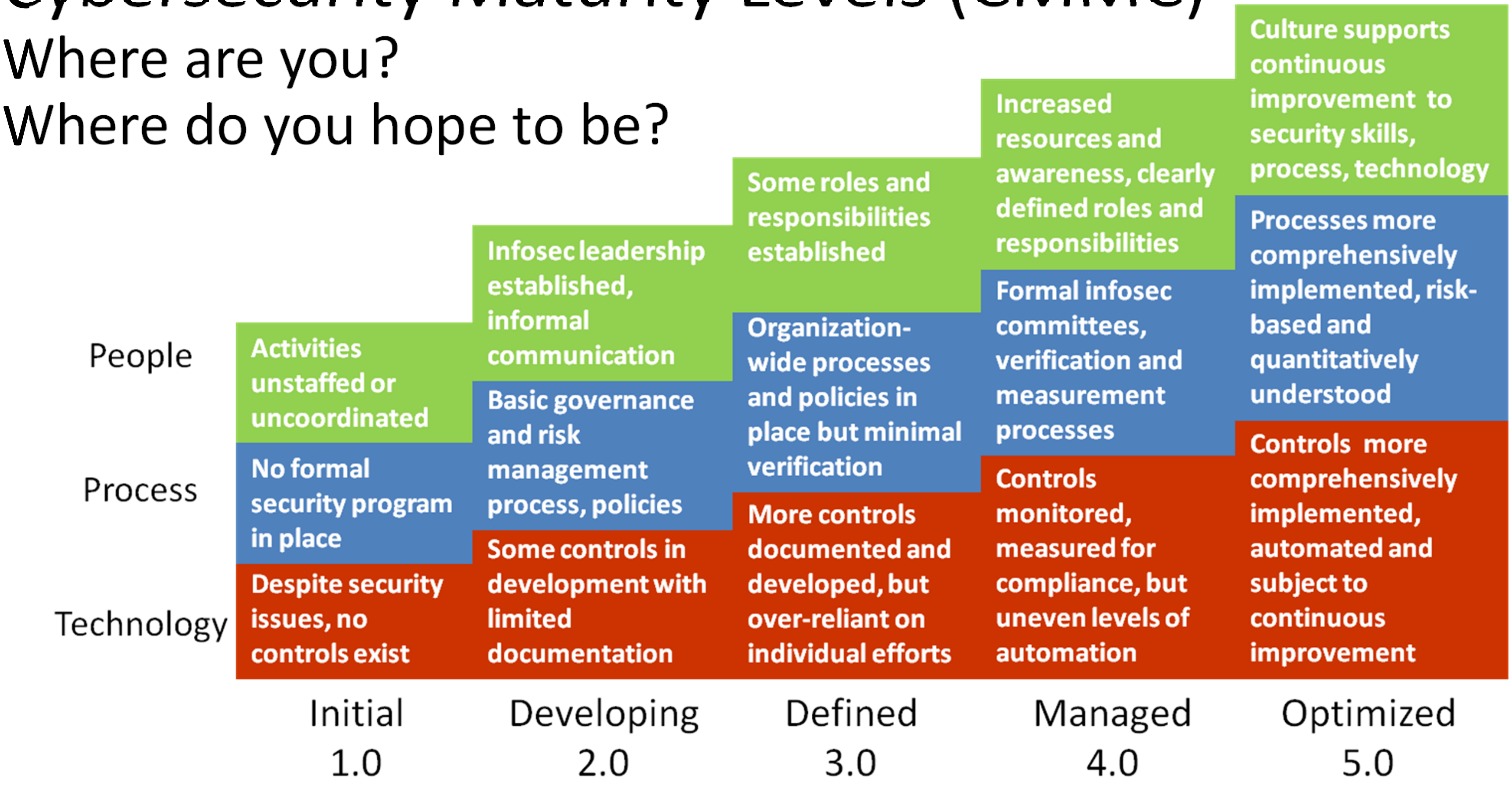
CIS (formerly SANS Top 20) has **"eighteen actions that can stop the vast majority of the attacks seen today"** via 150+ Safeguards.
(56 for Level 1… but must be done in sequence)
Mapping to CSF 2.0 (… just as good as a Cadillac)
Also pre-configured "hardened images" and 50+ benchmarks.

Whereas the NIST Cybersecurity Framework is less specific, CIS Controls are more prescriptive and may be easier to implement due to specific, detailed guidance.
Much is free, others at low cost to MS-ISAC members.

https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/nist-cybersecurity-framework-vs-cis-controls-version-8/

Cybersecurity Maturity Levels (CMMC)

Where are you?
Where do you hope to be?

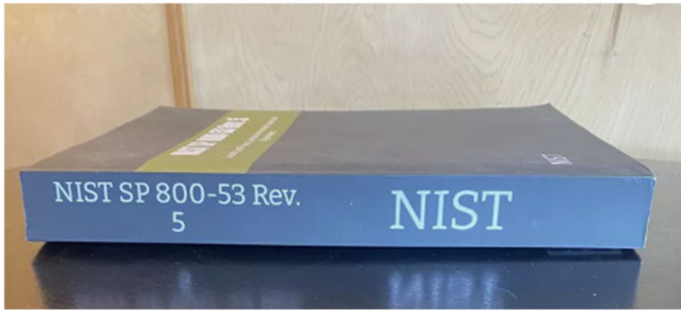


	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

It’s not just technology. Policy, Process and People come first!

A Framework is a Roadmap to set your direction and destination.

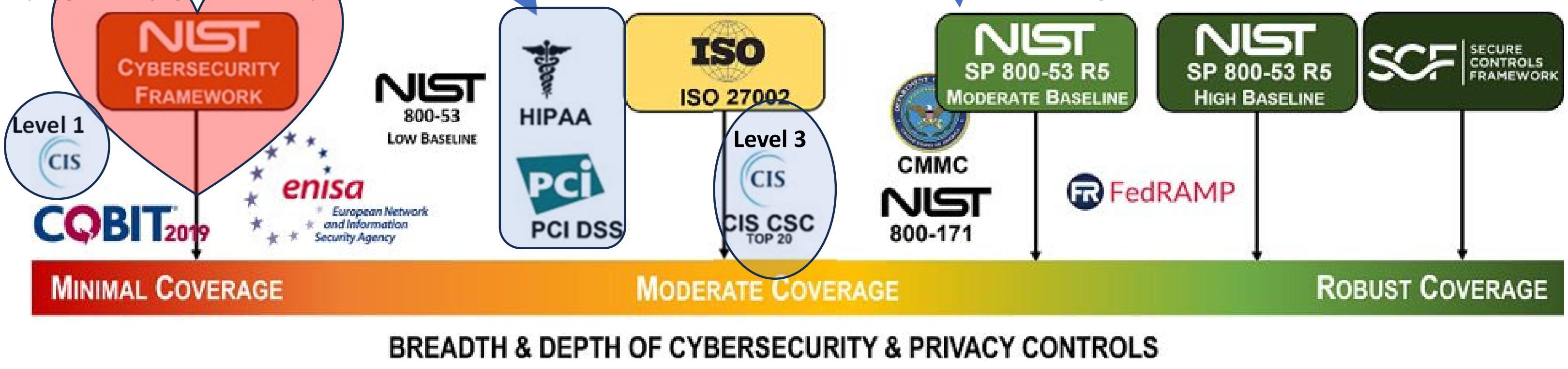
A Menu of Possible Frameworks



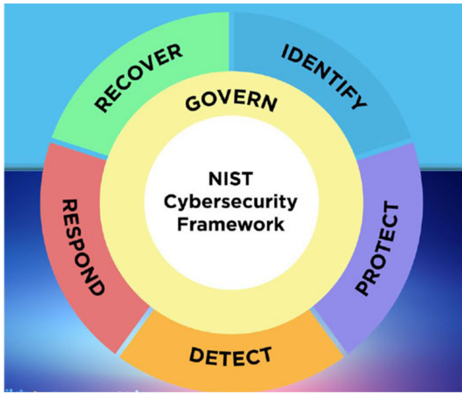
- NIST acknowledges numerous levels of security need and guidance for each.
  - Most Federal and State and Military use NIST SP 800-53 R5 Moderate.
  - **The lowest is "CSF 2.0 – Cyber Security Framework" and is a "short" guide for anyone to use**
  - The CSF has 108 controls and rather than writing its own controls, it references these Standard documents
  - Organizational-specific frameworks exist for banking and HealthCare

32 pages, 108 Controls, 6 Functions
14-page configuration spreadsheet

700+ pages, 300+ Controls, 14 Families
Plus the 400 Page "How to Audit" Guide



Overview of NIST Cybersecurity Framework (CSF 2.0) (Why We Are Here)



- 32 pages, plus some appendices (Core)
  - Details the Six Functions: **Govern, Identify, Protect, Detect, Respond, Recover**
  - (Gee I Probably Didn't Read it Right)
- **Download 108 achievable goals** (Profile in a 14-page Spreadsheet) aka Reference Tool
  - Easy to follow **taxonomy**
  - Explains each **goal** (aka SubCategory/Control) and provides example implementations
  - https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all
  - or
  - https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters
    - Export to Excel and ignore the "Withdrawn" rows
- Quick Start Guides and Communities

Imagine this: You can implement just 2 goals per week and change your security posture from a slouch into a rigid attention in a year.

Some Questions to Evaluate Your Current Readiness

(A Quick Show of Hands)

IPDRR

General Questions

- Are you state or local govt
- **Do you want to do business with the govt**
- Do you do International Business

Governance and Identification

Strategies, Policies, Roles

Asset Management, Risk Assessment

- **Risk – What are you protecting**
- **Who has an inventory** of all your hardware, software, data, system configuration and recovery documents
- Have you outsourced your IT or Cyber? Do you feel that protects you?
- Do you have separate IT and Cyber organizations? Do you have a CISO, Are you a CISO?
- Do you have cyber insurance?
- Are you a Cloud based operation and have a strong SLA regarding Cyber
- **Who has made a list of your top 10 risks**
- Who has revenues over $1 million
- Who spends more than 10% of annual revenues on cybersecurity
- Who has separate IT and Cybersecurity managers
- Have you done an **MTD and RPO** on email or customer orders

Some Questions to Evaluate Your Current Readiness

(A Quick Show of Hands)

IPDRR

Protection and Detection

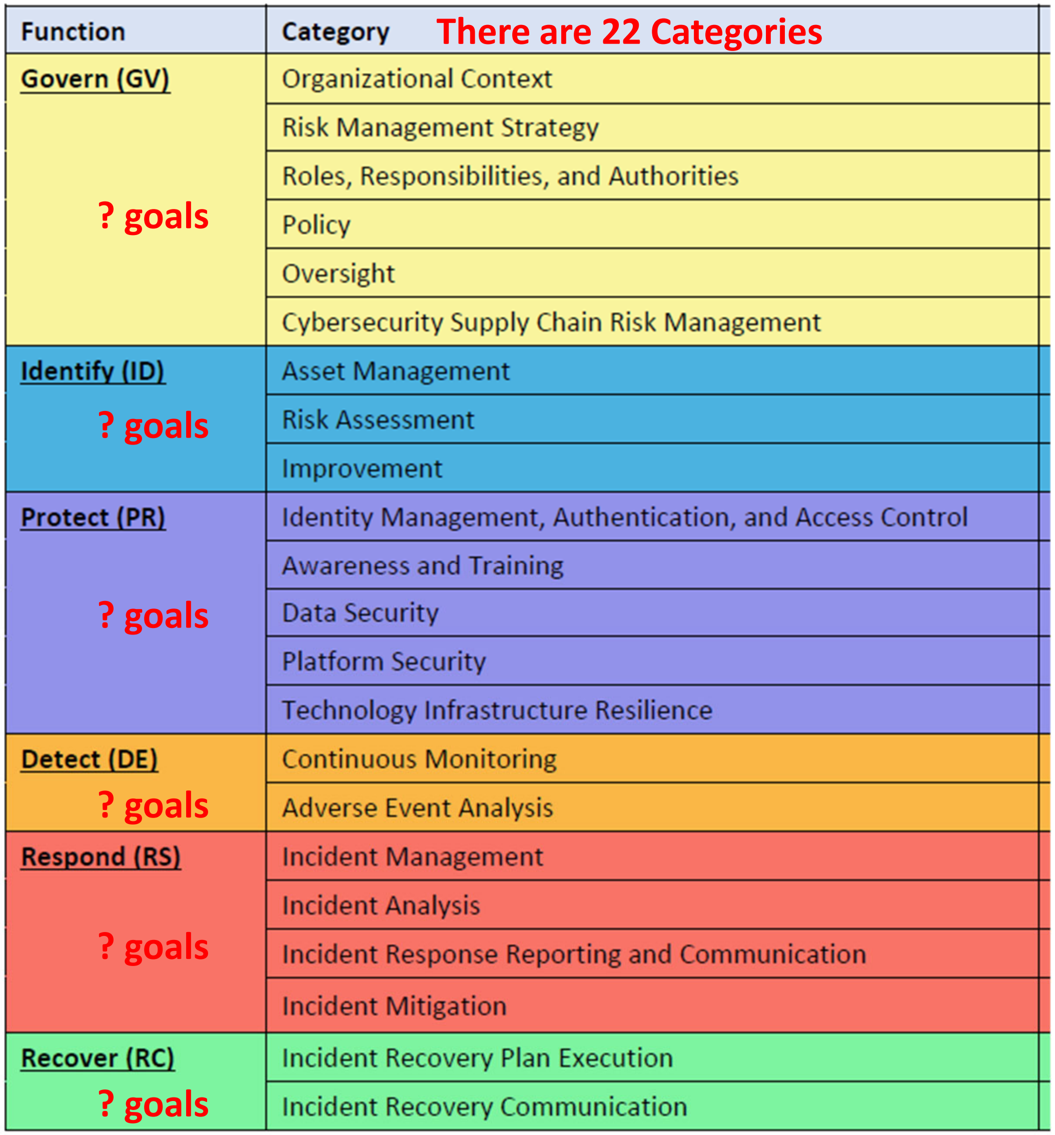
Technology and Controls, Monitoring and Event Analysis

- **Do you have a formal cyber framework selected**
- **How would you rank these in order of importance? Technology, Policy and procedures, People?**
- Who does tabletop exercises annually, On what topics?
- Who does **audits on accounts annually** to verify former employees are disabled and elevated accounts are only assigned as necessary?
- Who has a SIEM?
- **Who uses MFA** for elevated accounts? For all accounts?
- Who would be receptive to receiving pre-configured “hardened” systems from a federal agency
- **Who would be receptive to using a national cybersecurity infrastructure** that included firewall, intrusion detection.
- Who would be receptive to having an in-person consultation and recommendations from a national cybersecurity agency

Response and Recovery

Incident Review, Disaster Recovery, and Business Continuity

- Have you suffered a data breach, ransomware or major incident or disaster
- **Who thinks they could survive a 7-day outage** due to cyber attack
- Could your company reputation survive and breach, data exposure, or website defacement that makes state-wide news
- Who has a paper copy of Your DR and IR plans at your desk? At home?
- **Who has Cyber insurance**. Will it re-create your lost data

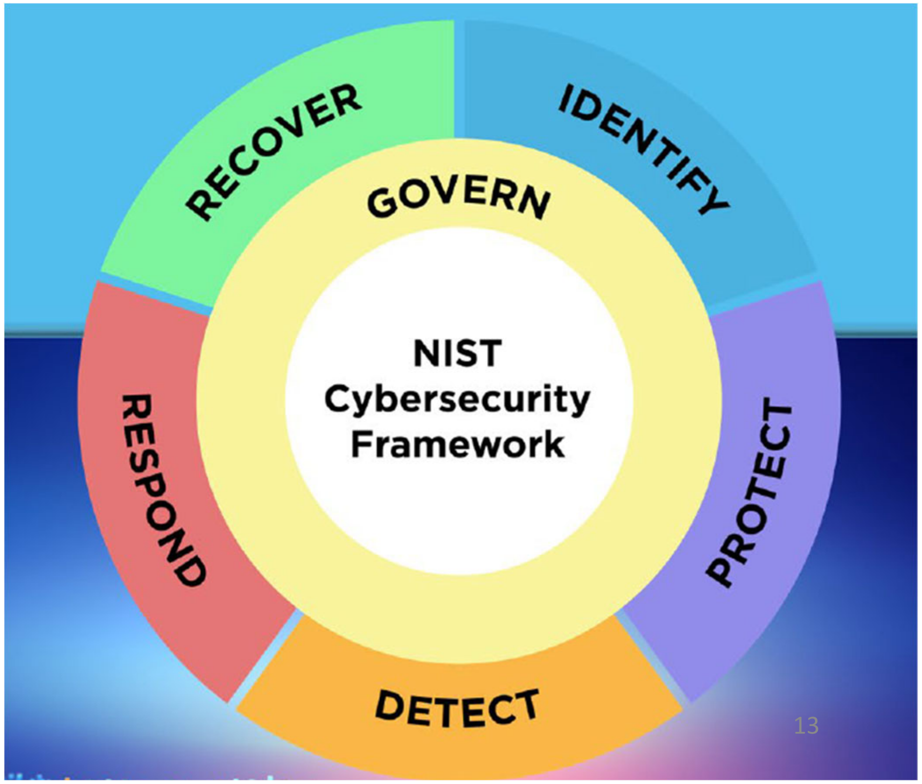


Function	Category **There are 22 Categories**
Govern (GV) **? goals**	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID) **? goals**	Asset Management
	Risk Assessment
	Improvement
Protect (PR) **? goals**	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE) **? goals**	Continuous Monitoring
	Adverse Event Analysis
Respond (RS) **? goals**	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC) **? goals**	Incident Recovery Plan Execution
	Incident Recovery Communication

Six Functions in CSF

Each function has between 8 and 31 goals

Where do you think the emphasis is?

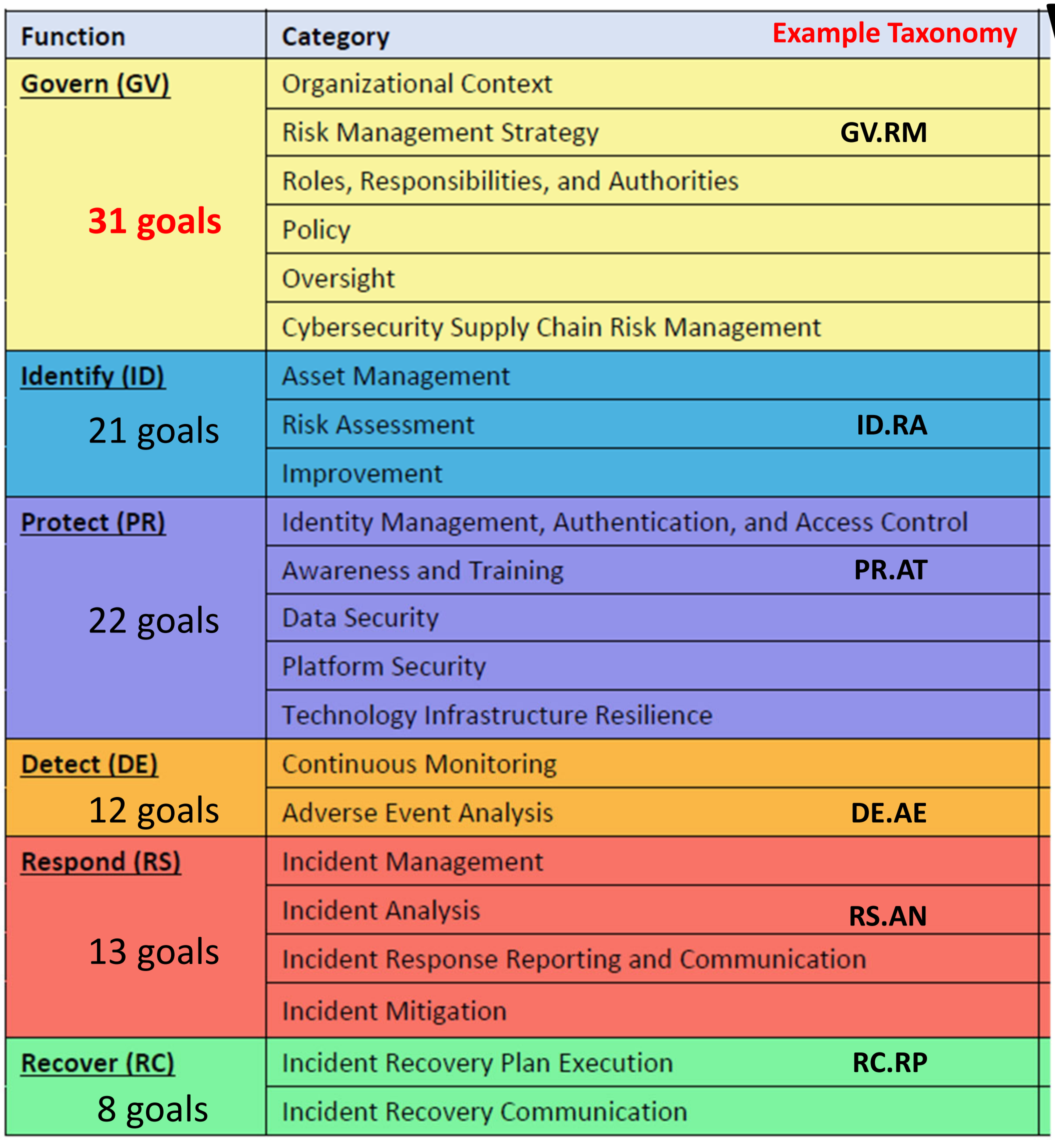


We’re From the Government and Here to Help

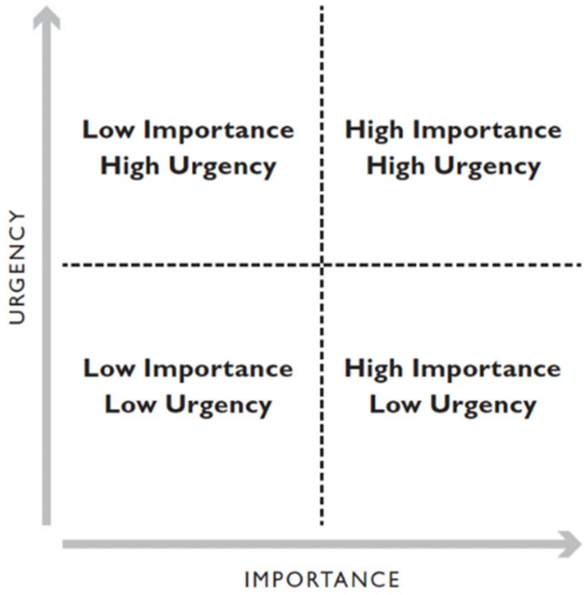
(And we have diagrams to prove it!)

6 Functions, 22 Categories, and 108 Goals

The Emphasis is On Planning and Organizational Issues.

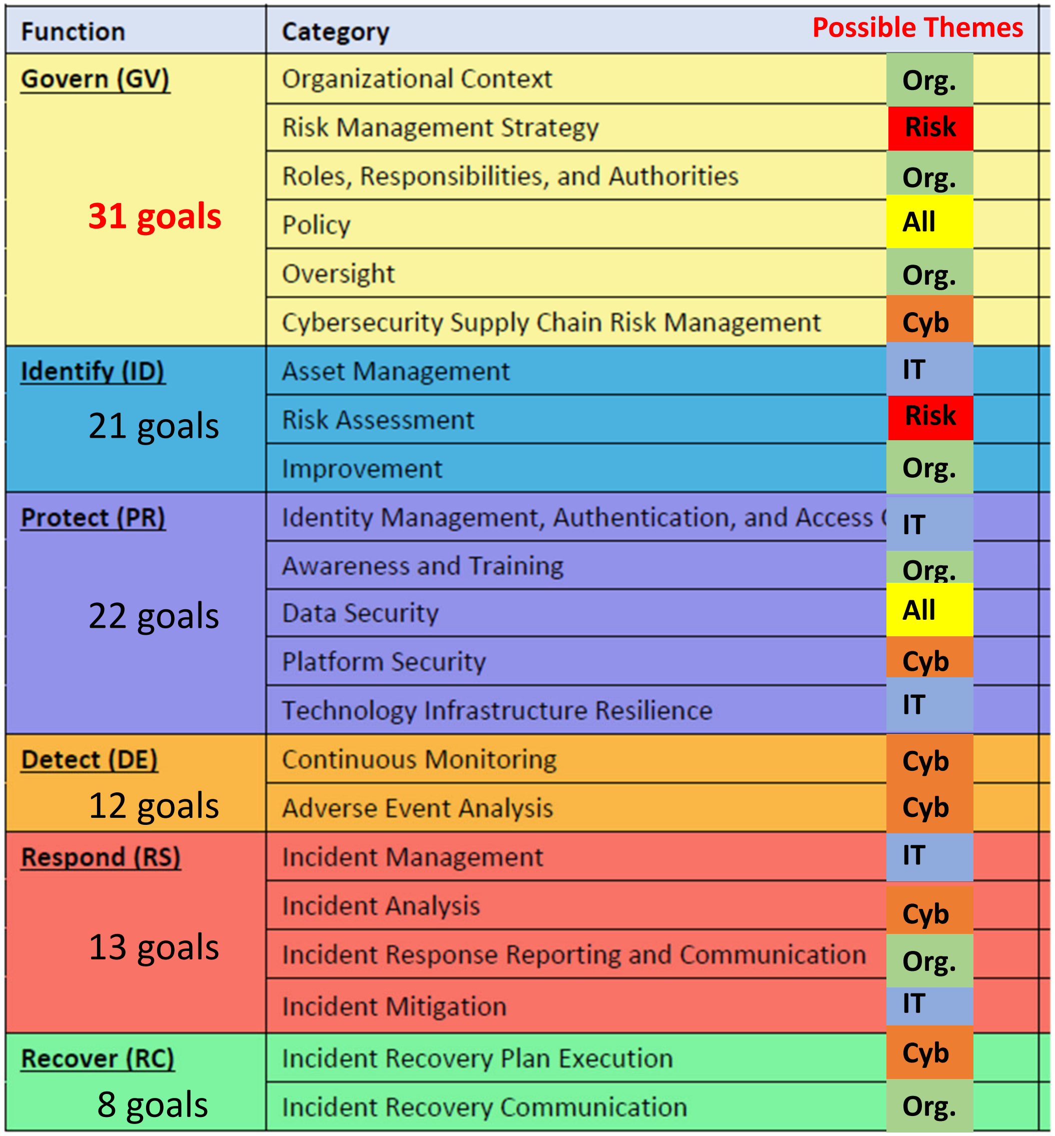


Function	Category	Example Taxonomy
Govern (GV) 31 goals	Organizational Context	
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	
	Policy	
	Oversight	
	Cybersecurity Supply Chain Risk Management	
Identify (ID) 21 goals	Asset Management	
	Risk Assessment	ID.RA
	Improvement	
Protect (PR) 22 goals	Identity Management, Authentication, and Access Control	
	Awareness and Training	PR.AT
	Data Security	
	Platform Security	
	Technology Infrastructure Resilience	
Detect (DE) 12 goals	Continuous Monitoring	
	Adverse Event Analysis	DE.AE
Respond (RS) 13 goals	Incident Management	
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	
	Incident Mitigation	
Recover (RC) 8 goals	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	



7.1 The Urgent/Important Matrix

Do the Important Stuff First and there will be Less Urgent and Unexpected Stuff (Gen. Eisenhower Matrix)

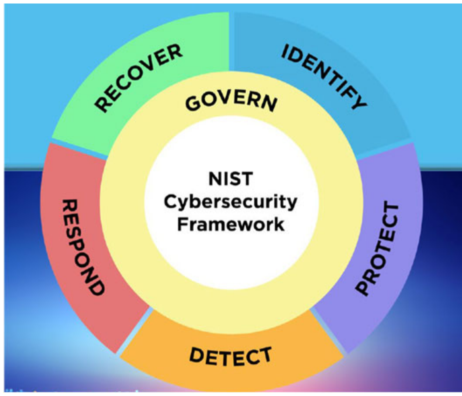


Function	Category	Possible Themes
Govern (GV) 31 goals	Organizational Context	Org.
	Risk Management Strategy	Risk
	Roles, Responsibilities, and Authorities	Org.
	Policy	All
	Oversight	Org.
	Cybersecurity Supply Chain Risk Management	Cyb
Identify (ID) 21 goals	Asset Management	IT
	Risk Assessment	Risk
	Improvement	Org.
Protect (PR) 22 goals	Identity Management, Authentication, and Access (	IT
	Awareness and Training	Org.
	Data Security	All
	Platform Security	Cyb
	Technology Infrastructure Resilience	IT
Detect (DE) 12 goals	Continuous Monitoring	Cyb
	Adverse Event Analysis	Cyb
Respond (RS) 13 goals	Incident Management	IT
	Incident Analysis	Cyb
	Incident Response Reporting and Communication	Org.
	Incident Mitigation	IT
Recover (RC) 8 goals	Incident Recovery Plan Execution	Cyb
	Incident Recovery Communication	Org.

One Bite at a Time

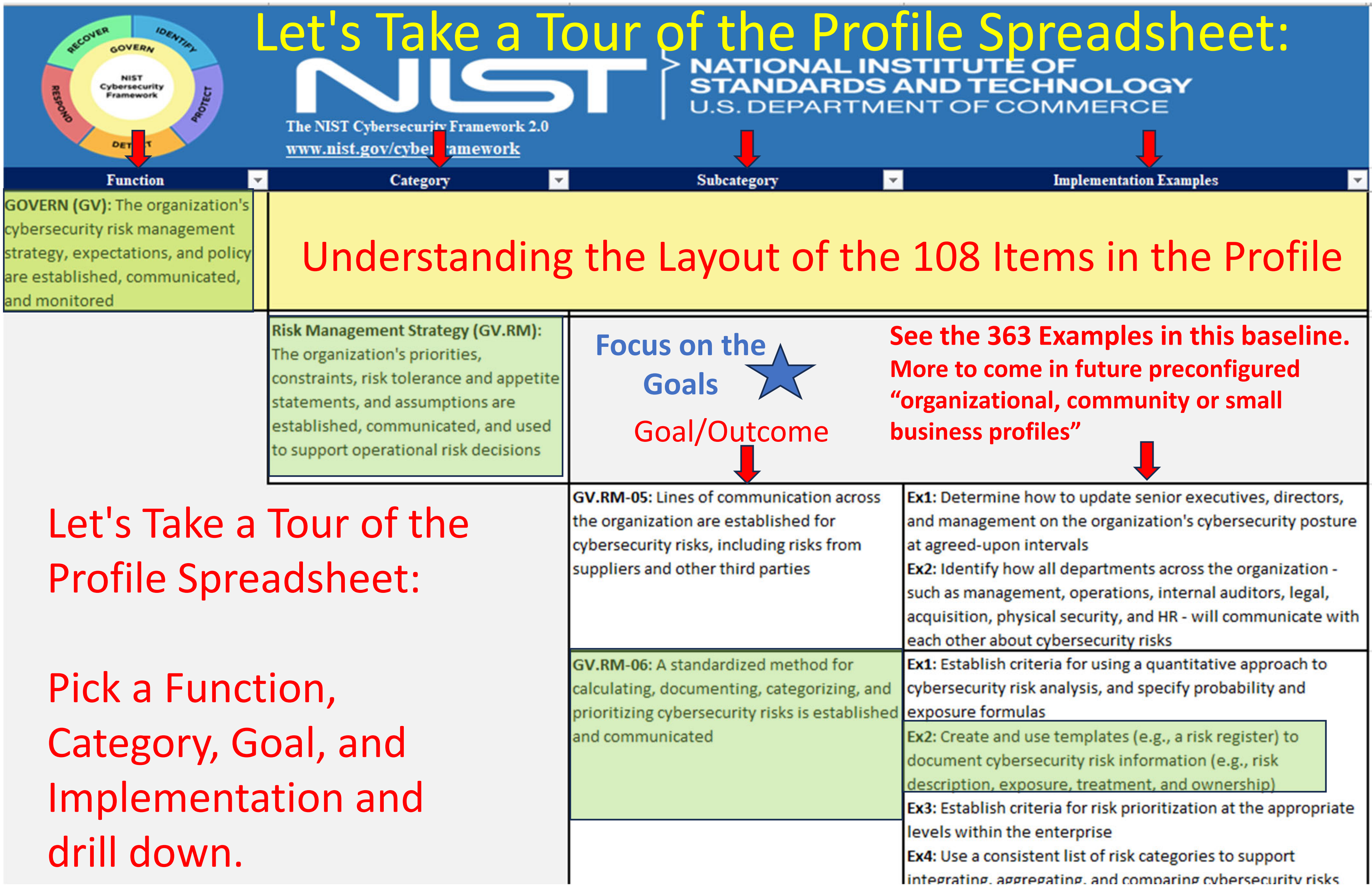
- Identify themes of expertise
- Create a strategic plan
  - Funding and staffing
  - Organizational and technical milestones
  - In-house vs Outsource
  - Cloud vs Local
- Start with Govern and then deploy working groups to work in parallel
- Create a prioritization matrix (Covered Later)
- Understand that it will take multiple passes
- Continuous improvement

Who Says You Don’t Need Governance?



- Quotes of the week
  - You cannot secure anything if you don't have a **functioning governance team** that not only has the **support** of upper management, but also where upper management gives you the **mandate to punish/chastise noncompliers.**
  - IT operations will build all kinds of **stupid crap that you have to clean up**. And they can spit in your face if you tell them that it's a bad idea.
  - It's 100% right for Governance to be a central part of any cyber security framework. Here are some of the things we want out of governance in our fledgling governance team:
    - Be empowered to tell trigger-happy **sysadmins (cowboys) with too many admin privileges** to slow the heck down
    - Be respected among your fellow IT folks, and to be **consulted before making** strategic or product **changes** that add considerable risk
    - Demand that **EVERYONE** (yes, event the IT and CIO) comply to policies
    - Be sure to have coverage for products that other people are responsible for (**eg vendor products**)
    - Demand that people actually **write documentation**, both technical and SOPs

Let's Take a Tour of the Profile Spreadsheet:



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored			
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions		
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Ex1:** Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2:** Identify how all departments across the organization - such as management, operations, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Ex1:** Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas **Ex2:** Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) **Ex3:** Establish criteria for risk prioritization at the appropriate levels within the enterprise **Ex4:** Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks

Understanding the Layout of the 108 Items in the Profile

Focus on the Goals ★

Goal/Outcome

See the 363 Examples in this baseline. More to come in future preconfigured "organizational, community or small business profiles"

Let's Take a Tour of the Profile Spreadsheet:

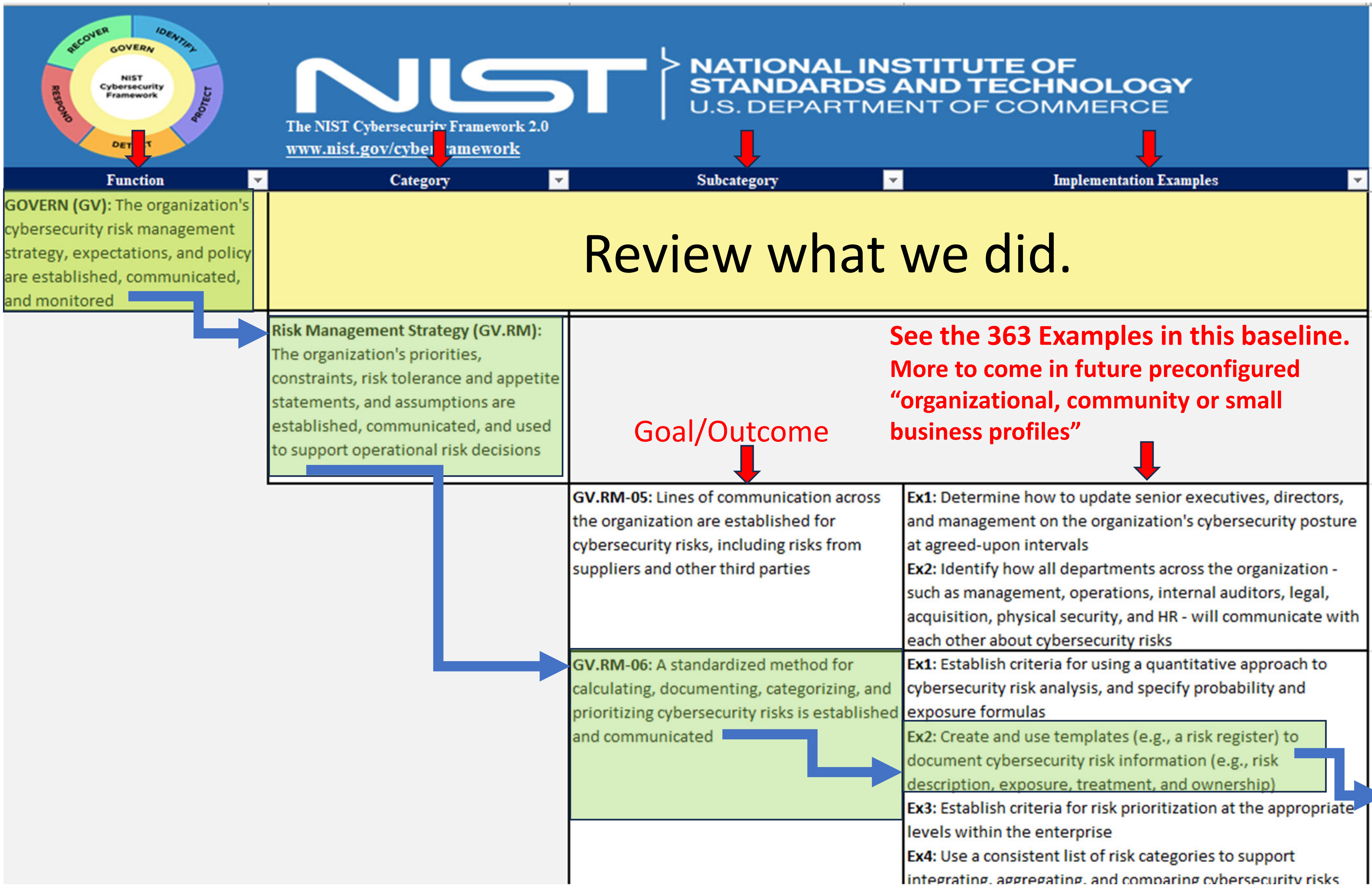
Pick a Function, Category, Goal, and Implementation and drill down.

Function 1: (6 Categories, 31 Goals) GOVERN (GV)
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

1. Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood
2. Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
3. Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
4. Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced
5. Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
6. Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

GOVERN (GV): Category: Risk Management Strategy (GV.RM) Sample Goal and Example Implementations

- Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
- **Goal: GV.RM-06**: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
- Ex1: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas
- Ex2: Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership)



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

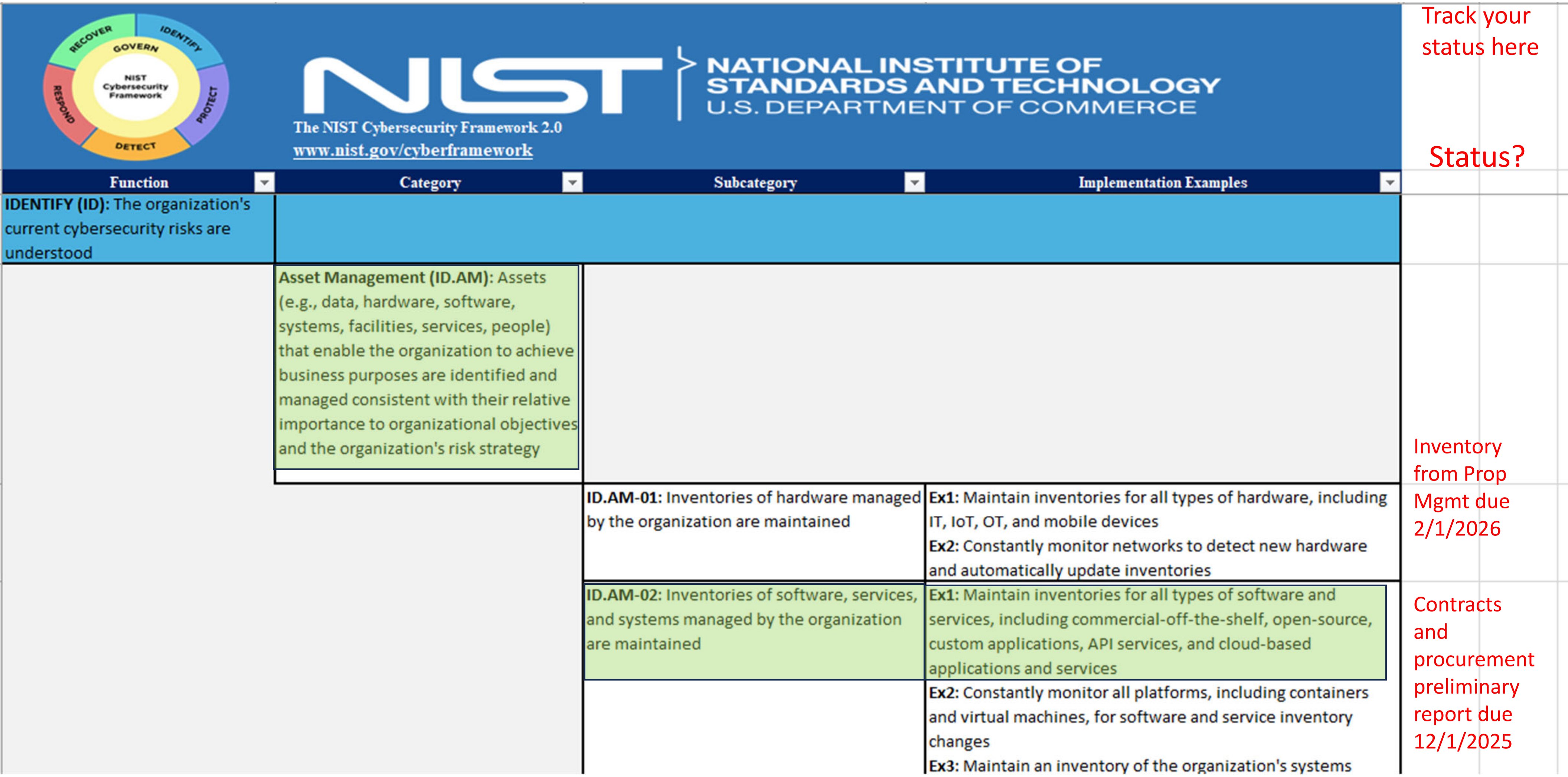
Review what we did.

Function	Category	Subcategory	Implementation Examples	Add this column Track your status here
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored				Status?
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions			
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Ex1:** Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2:** Identify how all departments across the organization - such as management, operations, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks	CIO/CFO/CTO /CEO committee meets Quarterly
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Ex1:** Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas **Ex2:** Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) **Ex3:** Establish criteria for risk prioritization at the appropriate levels within the enterprise **Ex4:** Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks	Risk register complete 2/24/24

Goal/Outcome

See the 363 Examples in this baseline.
More to come in future preconfigured "organizational, community or small business profiles"

A Second Example: Function 2 is Identify



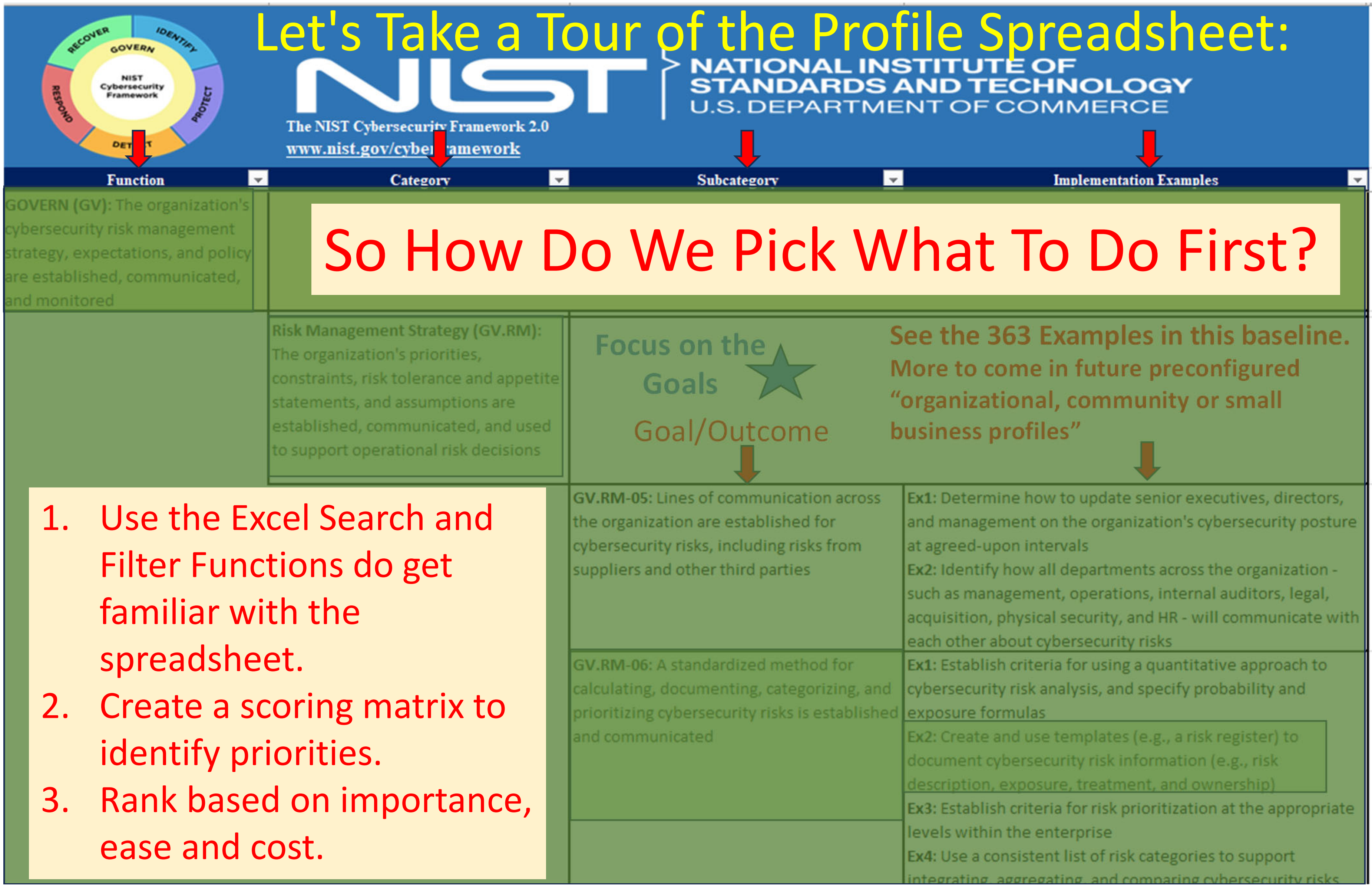
The NIST Cybersecurity Framework 2.0

www.nist.gov/cyberframework

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Function	Category	Subcategory	Implementation Examples	Track your status here Status?
IDENTIFY (ID): The organization's current cybersecurity risks are understood				
	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy			
		ID.AM-01: Inventories of hardware managed by the organization are maintained	**Ex1:** Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2:** Constantly monitor networks to detect new hardware and automatically update inventories	Inventory from Prop Mgmt due 2/1/2026
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**Ex1:** Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2:** Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3:** Maintain an inventory of the organization's systems	Contracts and procurement preliminary report due 12/1/2025

Let's Take a Tour of the Profile Spreadsheet:


RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
PROTECT
DETECT
RESPOND
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The NIST Cybersecurity Framework 2.0

www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored			
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions		
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Ex1: Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals Ex2: Identify how all departments across the organization - such as management, operations, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Ex1: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas Ex2: Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) Ex3: Establish criteria for risk prioritization at the appropriate levels within the enterprise Ex4: Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks

So How Do We Pick What To Do First?

Focus on the Goals ★

Goal/Outcome

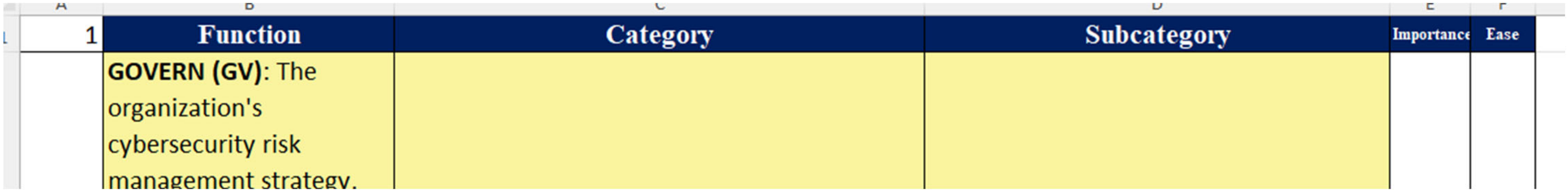
See the 363 Examples in this baseline. More to come in future preconfigured "organizational, community or small business profiles"

1. Use the Excel Search and Filter Functions do get familiar with the spreadsheet.
2. Create a scoring matrix to identify priorities.
3. Rank based on importance, ease and cost.

It’s Time to Get Our Hands Dirty

1. We will use the Excel Search and Filter Functions do get familiar with the spreadsheet.
   - NIST provides a complex “Organizational Profile Template” with 14 columns (See next slide)
   - But we will use just 2 columns for this exercise to provide a good first pass
2. We will break into 6 teams (GIPDRR) to create a scoring matrix to identify priorities.
3. We will consolidate and rank based on importance, ease and cost.
   - What do you do first?
     - Important, easy… or some combination?
     - Take credit for what you have already done.

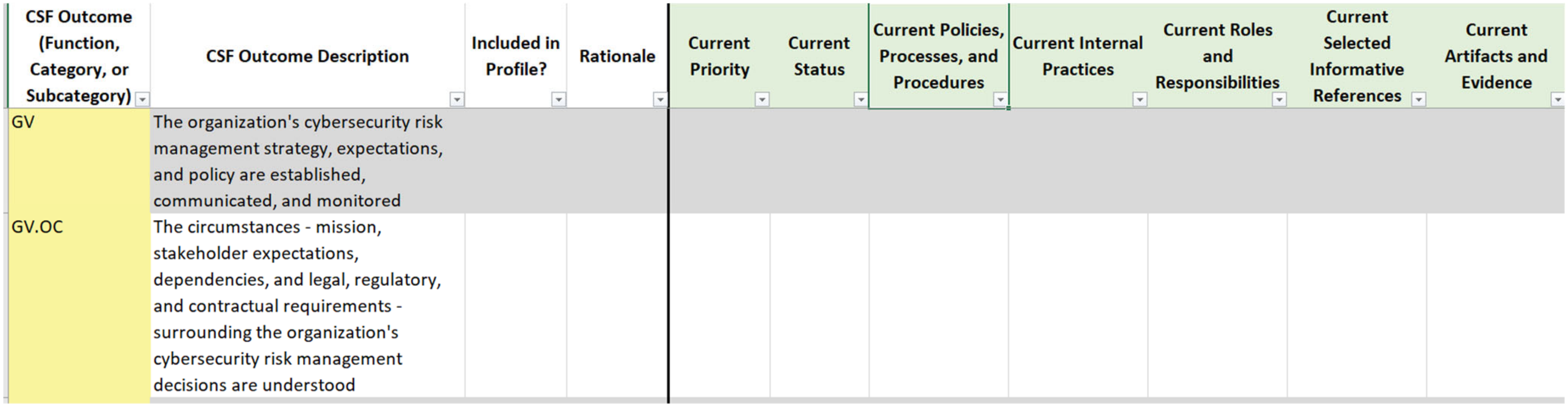
Our Format.....



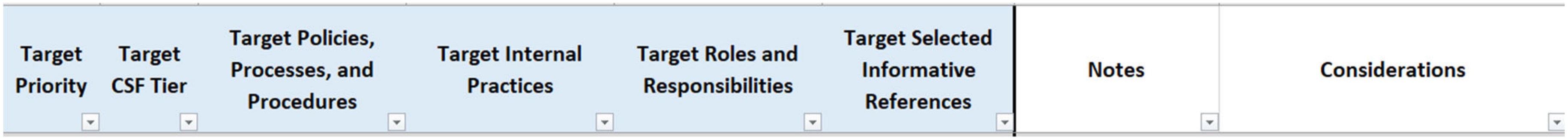
	A	B	C	D	E	F
	1	**Function**	**Category**	**Subcategory**	**Importance**	**Ease**
		GOVERN (GV): The organization's cybersecurity risk management strategy,				

When 6 columns are not enough:

Consider using the CSF 2.0 Organizational Profile Template Draft



CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedures	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative References	Current Artifacts and Evidence
GV	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored									
GV.OC	The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood									

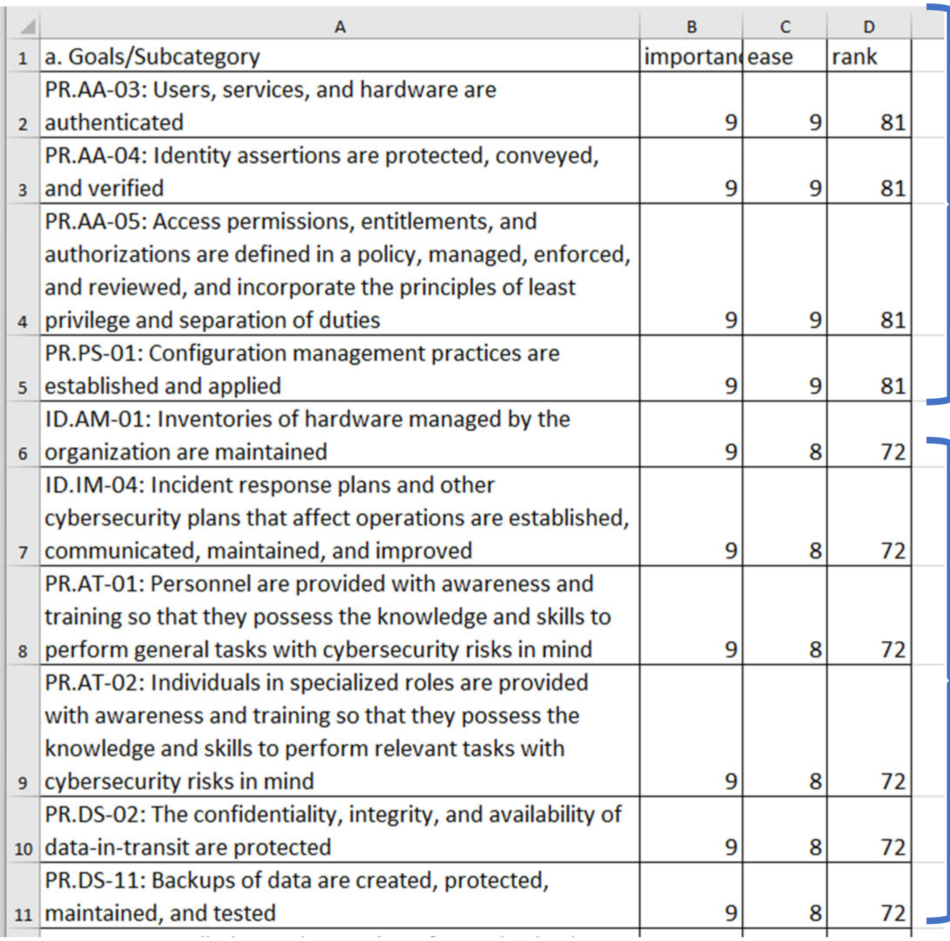


Target Priority	Target CSF Tier	Target Policies, Processes, and Procedures	Target Internal Practices	Target Roles and Responsibilities	Target Selected Informative References	Notes	Considerations

Exploit the Spreadsheet Format with a Ranking Process:

Once You Understand the Taxonomy, Try a First Pass and Find the Highest Priorities

Try a sample ranking process for example…. Priority = Function of Importance and Ease



	A	B	C	D
1	a. Goals/Subcategory	importan	ease	rank
2	PR.AA-03: Users, services, and hardware are authenticated	9	9	81
3	PR.AA-04: Identity assertions are protected, conveyed, and verified	9	9	81
4	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	9	9	81
5	PR.PS-01: Configuration management practices are established and applied	9	9	81
6	ID.AM-01: Inventories of hardware managed by the organization are maintained	9	8	72
7	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	9	8	72
8	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	9	8	72
9	PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	9	8	72
10	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	9	8	72
11	PR.DS-11: Backups of data are created, protected, maintained, and tested	9	8	72

Consider this 1 day exercise with IT, Cyber and Executive Management

For the 108 Goals, create a scoring matrix for your chosen criteria.
I picked Importance (Critical=10) and Ease (Easy=10) multiplied them.

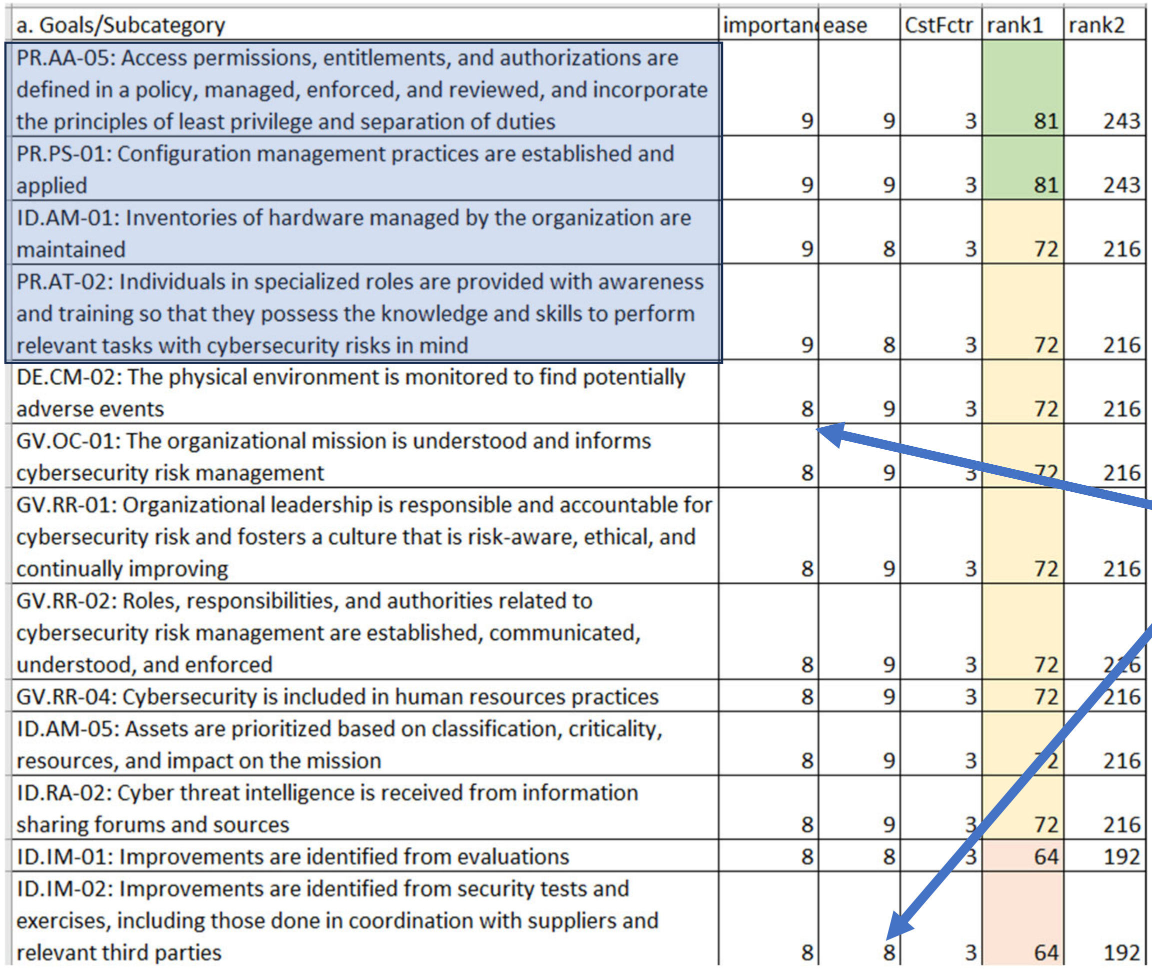
(You could add columns for cost, a toggle for in-house vs outsource, etc).

Based on my initial assessment it appears that Authentication and Authorization (maybe MFA and RBAC) should be addressed first at my company.

Then Asset Inventory, Cyber Awareness Training, Backup Integrity, and Incident Response.

Exploit the Spreadsheet Format with a Ranking Process:

What happens if you give weight based on a cost factor?



a. Goals/Subcategory	importan	ease	CstFctr	rank1	rank2
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	9	9	3	81	243
PR.PS-01: Configuration management practices are established and applied	9	9	3	81	243
ID.AM-01: Inventories of hardware managed by the organization are maintained	9	8	3	72	216
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	9	8	3	72	216
DE.CM-02: The physical environment is monitored to find potentially adverse events	8	9	3	72	216
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	8	9	3	72	216
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	8	9	3	72	216
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	8	9	3	72	216
GV.RR-04: Cybersecurity is included in human resources practices	8	9	3	72	216
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	8	9	3	72	216
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	8	9	3	72	216
ID.IM-01: Improvements are identified from evaluations	8	8	3	64	192
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	8	8	3	64	192

Do you want to do the "Easy" first or the "Free" first, or some combination of both.

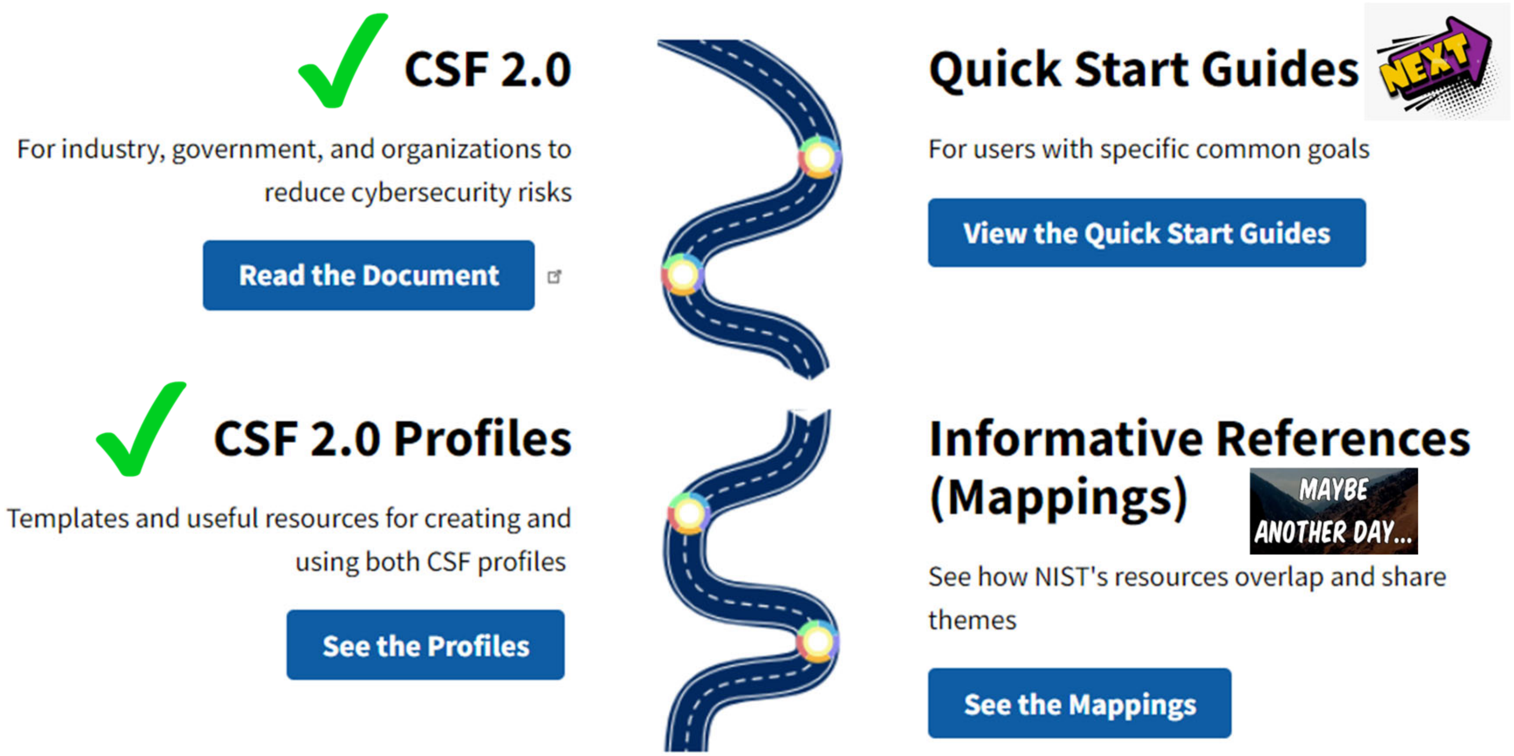
Cost Factor
1 = Expensive
2= Moderate cost
3= Free

This changes the priority.
Lots of stuff is easy and free, although not as important.

But Training/Awareness, Authentication and Authorization as well as Inventory and Configuration Management are still key.

Navigating The Framework Website and Beyond

- https://www.nist.gov/cyberframework



✓ **CSF 2.0**

For industry, government, and organizations to reduce cybersecurity risks

✓ **CSF 2.0 Profiles**

Templates and useful resources for creating and using both CSF profiles

Quick Start Guides

For users with specific common goals

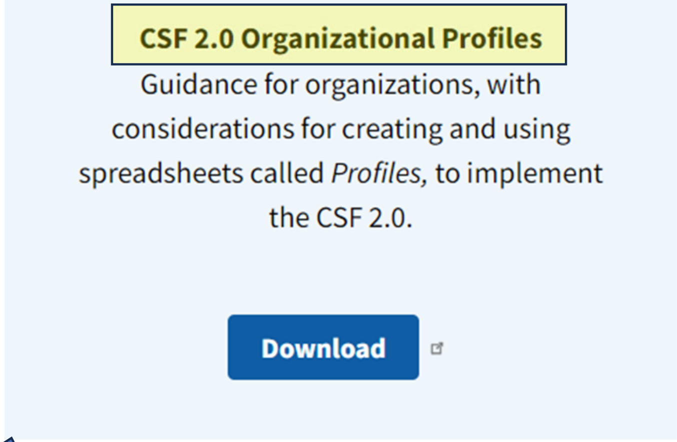
Informative References (Mappings)

See how NIST's resources overlap and share themes

NIST will continue to build and host additional resources to help organizations implement the CSF, including Quick Start Guides and Community Profiles https://www.nist.gov/quick-start-guides

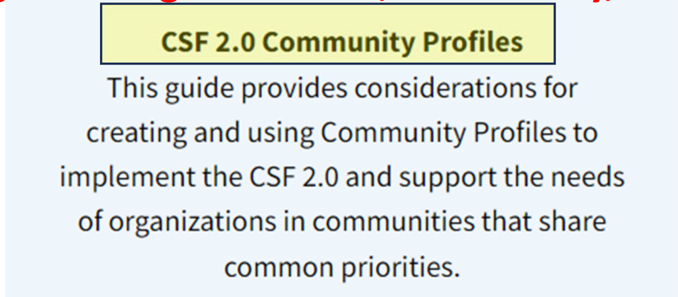
Your Next Steps: Quick Start Guides and Profiles

Use the Default, or select a preconfigured "organizational, community, or small business profile"



CSF 2.0 Organizational Profiles

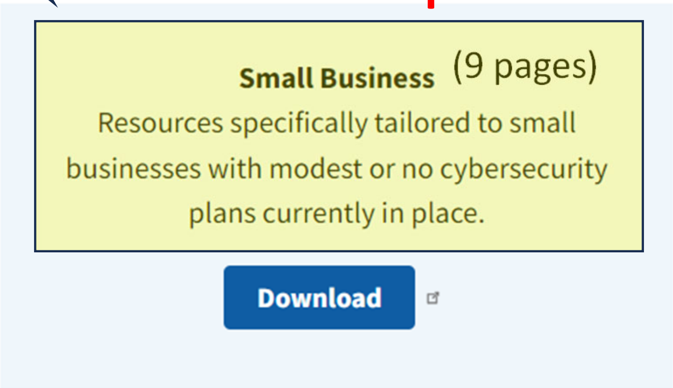
Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.



CSF 2.0 Community Profiles

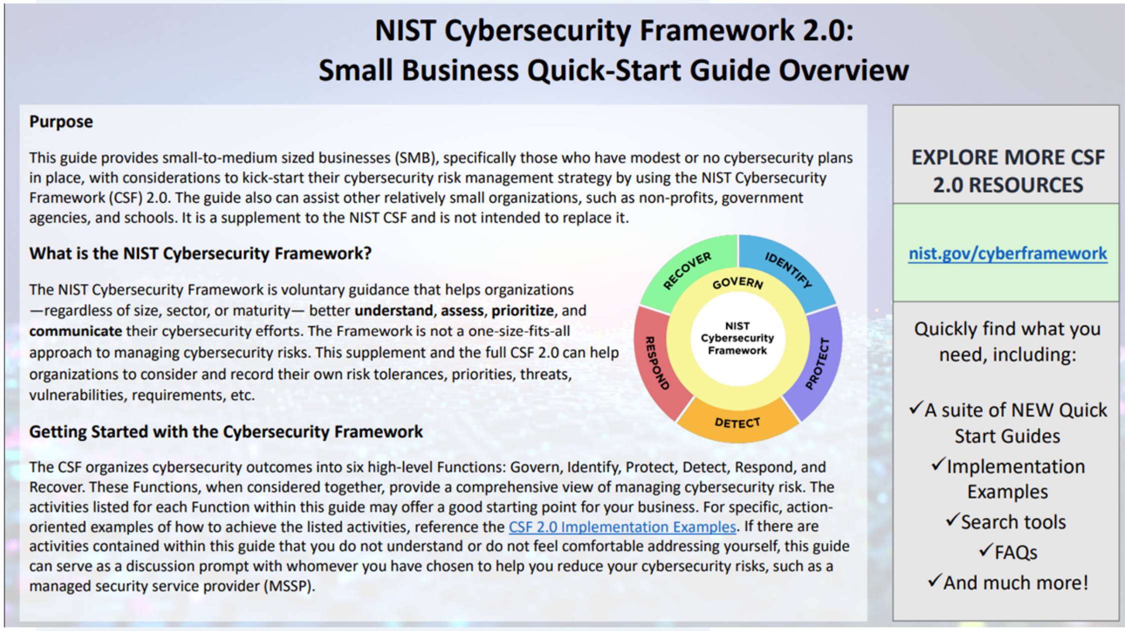
This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.

Take the first step now!



Small Business (9 pages)

Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.



NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the CSF 2.0 Implementation Examples. If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).

EXPLORE MORE CSF 2.0 RESOURCES

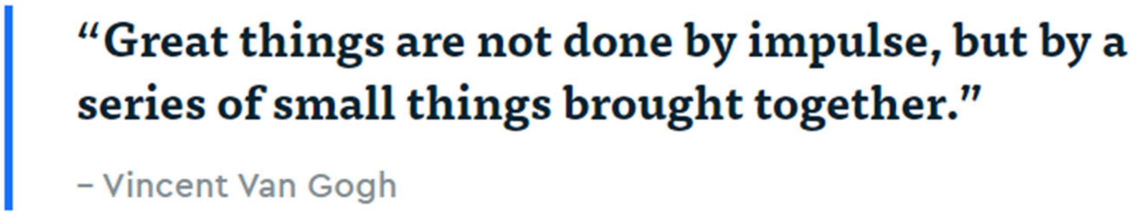
nist.gov/cyberframework

Quickly find what you need, including:

✓A suite of NEW Quick Start Guides
✓Implementation Examples
✓Search tools
✓FAQs
✓And much more!

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

Summary and Conclusions



“Great things are not done by impulse, but by a series of small things brought together.”

– Vincent Van Gogh

- NIST CSF 2.0 is a **viable and recognized** cyber framework for the “rest of us”
  - Useful as a **catalyst for change (Gee I Probably Didn't Read it Right)**
    - Govern, Identify, Protect, Detect, Respond, Recover
  - Plain language, field tested, frequently updated
  - Flexible, not prescriptive but gentle nudges
  - Well **structured spreadsheet** of Goals and Implementation Ideas (and your status column)
- It should be implemented as part of a **3 year IT/Cyber/Business strategic plan**
- Adoption and Adherence is helpful in many ways
  - **Reduces risk**, identifies gaps, prioritizes implementations
  - Brings Cybersecurity to the **front burner** in C-Level meetings
  - Helps justify funding and staff. Brings **IT and Cyber to the same table** with a common goal.
  - Builds **trust and confidence** within your company and with other businesses
  - Serves as **evidence** to the outside world and insurers that you are making a good effort
  - Provides **secondary benefits** like accurate asset inventory, system documentation
- It’s never too late to start. You might find you are better off than you realize.

CipherFidget.com

- This 3D-Printed Caesar Cipher Decoder Ring serves as a hands-on tool to explore the basic principles of encryption and decryption.
- At its core, this ring is designed to demonstrate the Caesar cipher, one of the simplest and oldest forms of encryption.
- It utilizes a **substitution cipher** where each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- **Using Your Cipher Ring:**
- Each notch represents a single letter shift in the alphabet. Assign your shift and easily encrypt or decrypt a character.

A NIST Cybersecurity Framework for Everyone: Presenting CSF 2.0 Questions????

Barry Hudson, CISSP
bhudsoncissp@gmail.com
bhudsoncissp.com
www.linkedin.com/in/barry-hudson-cissp-ab9b2136/