CSF 2.0
HIGH-LEVEL SUMMARY
By E. S. Swanson
11/6/2023

A. New Direction

NIST needs to reframe the direction, i.e., the focus, of the Cybersecurity Framework (CSF) from the perspective of the business and not the technology. Sounds contradictory, doesn't it? Please note that my suggestions in no way imply that the cyber/ technological/security components in CSF 2.0 are a bad idea or not necessary – quite the contrary. As others have undoubtedly revealed to you, there is a lot of useful information in the CSF 2.0 version. However, what's missing and badly needed is to describe the Framework from a perspective of how businesses and other organizations – e.g., universities, charitable organizations, and governments, etc. – view cybersecurity.

Therefore, I'm taking the liberty of stating that businesses and other organizations perceive their worlds in terms of the applications that function to achieve those goals and objectives needed to keep remain ongoing and, with regard to businesses, profitable. My suggestion is to re-organize the contents of CSF 2.0 to emanate from the eyes of how businesses and other organizations view cybersecurity; that is, as a primary necessity to ensure that the applications and data used are secure, reliable, and available.

B. Find the "Thread"

In any style of writing, including technical, there needs to be a thread – a way for the writer to convey to the reader the message in a reasonably logical, understandable order. As people read the CSF Tables, they expect to see a chronology of guidelines to follow – i.e., the proverbial thread. These guidelines, referred to in the Framework as "Categories," "Subcategories," and "Implementation Examples," do **not** have to be ordered in a strict, step-by-step fashion – i.e., do this first, do this next, etc. However, they do have to flow in a logical pattern. In other words, anyone reading the Framework document should be able to easily find that logical thread.

There is a natural, logical order inherent within the Framework's six tables. The following page represents my attempt to reveal that order and revitalize the Framework by taking an application approach.

I've left out the GOVERN function as I truly believe that GOVERN cannot completely stand on its own – it needs to be associated with a Function. Putting GOVERN by itself in a Table is okay – as long as the applicable categories are associated with GOVERN functions. The following page is just a start – it is the beginning of a revised framework – and one that you may or may not choose to use. Also, as it's just a start – it needs polish and a lot of work.

SUGGESTED FORMAT TO RE-ORGANIZE THE FRAMEWORK:

THE ORGANIZATION NEEDS TO DO THE FOLLOWING:

1.) **IDENTIFY** its applications – e.g., Payroll, Purchasing, a University's Student Grading system, etc. – and then rate and prioritize these applications based on their criticality, i.e., the degree to which the organization relies on each application to remain operational.

IDENTIFY and map out the start-to-finish processes for each application, including components such as hardware and software, as well as the respective organizational context involved – who, what, where, when, and why.

IDENTIFY for each application, everything that could possibly go wrong, commencing with currently existing vulnerabilities and threats. Then estimate the risk i.e., the likelihood, that any of those threats might exploit a vulnerability, creating an incident that may adversely impact the organization.

IDENTIFY and review the formal policies and procedures in place to PROTECT the security of each application.

2.) **PROTECT** each application from the likelihood of incidents adversely impacting the organization by ensuring that security measures are in place to PREVENT incidents from negatively impacting business operations.

PROTECT the organization from events that appear harmless, but when grouped with other events can become incidents that negatively impact business operations.

3.) **DETECT** those incidents that the PROTECT security measures have failed to PREVENT. Assess these incidents to determine the degree of adverse impact they may have on the organization.

4.) **RESPOND** to detected incidents by re-assessing the incident to determine the degree of damage it could potentially cause – or already has caused – and take further action based on this assessment.

Quarantine the data if necessary to minimize the contagion.

Halt operations if necessary to prevent further damage.

5.) **RECOVER** if the RESPOND function analysis indicates that an incident has occurred that has had an adverse impact requiring data, system, or partial system restitution.

C. Subcategories Need to Clearly Relate Back to the Category

Each subcategory identified, i.e., -01, -02, -03, must substantiate or provide more detail for the category.

Upon examining the first category and first three subcategories from the first Table, i.e., Table 1, GOVERN, it is very clear that the first three subcategories clearly relate to the "Category." But, what about the next two subcategories? Does the wording in subcategory 04 and 05 clearly relate back to the Category? (See Example below.) Here, that thread is missing.

EXAMPLE:

The first three Subcategories clearly relate back to the Category. Do the next two?

CATEGORY	SUBCATEGORIES
Organizational Context (GV.OC): The circumstances – **mission**, **stakeholder expectations**, and **legal, regulatory, and contractual requirements** – surrounding the organization's cybersecurity risk management decisions are understood	-01: **mission** -02: **stakeholders expectations** -03: **legal, regulatory and contractual requirements**
	GV.OC-01: The organizational **mission** is understood and informs cybersecurity risk management.
	GV.OC-02: Internal and external **stakeholders** are determined, and their needs and **expectations** regarding cybersecurity risk management are understood.
	GV.0C-03: **Legal, regulatory, and contractual requirements** regarding cybersecurity – including privacy and civil liberties obligations – are understood and managed.
	GV.OC-04: Critical objectives, capabilities and services that stakeholders depend on or expect from the organization are determined and communicated.
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are determined and communicated.

There are numerous examples of that missing or unclear thread throughout the document: the Subcategories need to clearly relate to the Categories.

Sometimes, it appears as if the Implementation Examples were included because they needed to be there. My point: reorganization is needed.

Additionally, the DETAILED NOTES DOCUMENT (attached) lists some additional issues common in the CSF Framework 2.0 documents. Below are sample examples:

- Cybersecurity risk management" is first discussed in the first Category of the GOVERN Table. Consider the Reader who has no idea what cybersecurity risk management is. Ditto for outcomes, capabilities and services. I'm not suggesting that you define these terms in an Appendix. What I am attempting to point out is the need for the Writer to redo these Tables in an order that communicates a logical flow, incorporating the definitions into the text as you progress.

- Additionally, some statements just "hang" – e.g., are understood and managed – by whom? How do you know someone understands something? Ditto for "are determined and communicated." Determined and communicated to whom?

ESS/11-11-2023

A. FORMATTING AND CONTENT SUGGESTIONS

1.) Punctuate all sentences with a period. All writings on Charts 1-6 (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER) are SENTENCES, and, therefore, NEED TO BE punctuated with a period.

2.) Instead of having the *Informative References* on the same page as the Framework Cores, include them in a separate Appendix. Additionally, on this Appendix, include all former references i.e., (Formerly ID.BE) and the like. Keeping both categories of references on the same pages as the Framework Core impedes readability.

3.) Each Table should stand by itself. What I mean by this is the Reader should be able to print out and read (or just read on the screen) each table individually, without having to refer to another Table for clarification.

4.) When you examine my second document entitled FUNCTION TABLES, you will note that the heading of each table comprises a description of each category identifier, category, and subcategory included. This format enhances readability. (See next page.)

5.) Additionally, for Function Tables 2-6 – i.e., IDENTIFY, PROTECT, DETECT, RESPOND, AND RECOVER – there is a designated section per function to include a big-picture objective related to GOVERN. Although keeping GOVERN as a separate function may be a great idea, something is missing from Tables 2-6 if the GOVERN function is absent. The circle diagram—i.e., Figure 2, page 6 of the *Initial Public Draft* says it all: GOVERN touches/impacts all other functions. Consider keeping GOVERN as Table 1, but go back and include main GOVERN functions for each Category. (See next page.)

6.) Although the Tables are individual documents, they also tie together. What I've attempted to do (started, but not finished) is include a section at the beginning of each Table (except the first, GOVERN) that describes Pre-Implementation Activities. In other words, for Tables 2-6 there is a starting point and ending point for each Function (process). So, at the beginning of the Tables, I've started to add a Pre-Implementation Activities section for purposes of ensuring that the listed activities have already been performed prior to needing the next function. (See page 3.)

7.) Note that questions have replaced statements for the Pre-Implementation Activity section. Why questions vs. statements? Well, it's psychological. Rather than giving the reader an instruction – which is what imperative sentences do under the Implementation Examples, readers will read these questions and ask themselves if the organization has done or needs to do 'X' on a regular basis.

THE NIST CYBERSECURITY FRAMEWORK, 2.0
FUNCTION TABLE 4
DETECT (DE):
Find and analyze possible cybersecurity attacks and compromises.

DE.CM	**DETECT Continuous Monitoring Activities**	**GV.XX**	**CATEGORIES GO HERE**
DE.AE	**DETECT Adverse Event Analysis**	**GV.YY**	**CATEGORIES GO HERE**

DETECT (DE) FAMEWORK CORE FUNCTIONS AND IMPLEMENTATION EXAMPLES

CORE FUNCTION CATEGORY	CORE FUNCTION SUBCATEGORY	IMPLEMENTATION EXAMPLES
DE.CM **Continuous Monitoring** Assets are monitored continuously for purposes of detecting all forms of potentially adverse events, including Indicators of Compromise (IoC) and other anomalies.		**GV.XX:** **GV.YY:** Include Govern examples here as they apply to Continuous Monitoring.

RESPOND function analysis indicates that an incident has occurred that has caused a malfunction requiring system and/or data recovery.

THE NIST CYBERSECURITY FRAMEWORK, 2.0
FUNCTION TABLE 6
RECOVER (RC):
Restore assets and operations that were impacted by a cybersecurity incident.

RC.PIA	Incident Recovery Pre-Implementation Activities	GV.	
RC.RP	Incident Recovery Plan Execution	GV.	
RC.CO	Incident Recovery Communication	GV.	

#	RECOVER (RC) PRE-IMPLEMENTATION ACTIVITIES	CSF REFERENCE
RC.PIA-01	Has the recovery portion of the organization's Incident Response Plan (IRP) been tested on a periodic basis with the results of those tests documented, and any changes to the IRP approved by management?	
RC.PIA-02	Has the list of contacts and accompanying contact information contained in the organization's IRP been updated with the most recent information?	
RC.PIA-03	Have all individuals with recovery-related responsibilities been made aware of those responsibilities well in advance of the organization's need to recover?	
RC.PIA-04	Have all individuals with recovery-related responsibilities obtained and tested their respective recovery authorizations well in advance of the organization's need to recover?	
RC.PIA-05	**Has the Incident Analysis component of the RESPOND (RS) function indicated a need to recover?**	

8.) Each IMPLEMENTATION EXAMPLE starts with an action verb that is in bold. Sometimes starting the sentence with a verb made the sentence wordier or less readable – in these cases, the first word is an adverb, and the second word is verb in bold. Examples: Routinely **inform** vs. **Inform** routinely.

9.) My only use of parenthesis within the Tables is to identify acronyms: (KPIs), (RTO), and (RPO) for example.
Even though it is not always a 100% correct practice, I've implemented the procedure of spelling out the acronym using capital letters for emphasis purposes, and then putting the acronym abbreviation in ( ) parenthesis:

- Key Performance Indicator (KPI),
- Recovery Time Objective (RTO), and
- Recovery Point Objective (RPO).

My rationale: consistency plus the fact that people who read these documents are often students or entry-level employees and learning the acronyms comes in handy.

Also, with regard to acronyms, my personal standard is to spell the acronym out the first time it appears in the document, and again if the same acronym appears on another page. So, if an acronym appears more than once on the same page, <u>usually</u> I only spell out the first instance. Sometimes, particularly for technical writing, I will spell out the acronym more than once on the same page. Why? Improved readability. In summary, most readers despise having to flip the pages back and forth to search for the acronym's full wording and hence, meaning.

Additionally, it's never a bad idea to have a separate ACRONYM APPENDIX.

10.) Often in the Tables documents one through six, NIST uses the term "leadership," or "senior leadership." Is this common practice these days? I'm accustomed to the term "senior management" to refer to executive levels, excluding the president and perhaps assistant directors. Whatever, the terms should be consistent throughout the document.

11.) There's a tad more white space on the Tables that I've re-created. To me, more white space equates to easier reading; however, it also equates to more pages and paper.

12.) To label the Implementation Examples, I've added an extra '0' – Ex.01 vs. Ex1 – in order to maintain the alignment of the numbers should they go over Ex.09.

13.) Suggestion: leave all function category identifiers with two characters, i.e., GV, ID, etc.

- Consider changing PR to PROTECT and PREVENT.
- Consider changing all sub-function category identifiers from two to three or even four characters. Why? First of all, longer character sets would be easier to remember: Instead of DS, use DSEC. Instead of PS, use PSEC.
- Secondly, having three-or-more characters suggests subfunction identifiers compared to the two-character functions identifiers.
- I've added a couple of Function Identifiers – they have three characters: Pre-Implementation Activities (PIA)

14.) I'd like to suggest a separate Appendix for words/terms that need to be and don't need to be hyphenated. Admittedly, I may have gone a little overboard with hyphenating in these documents. However, some sources indicate that certain words/terms should be hyphenated; other sources don't. Many of these ambiguities refer to words/terms that are system related.

15.) Suppliers and vendors are not the same thing. Include both when applicable.

16.) Change the word "organization" to enterprise throughout this document? NIST has used the enterprise term in the past; I'm not sure why this term is not used in these documents. There has to be a way to clarify businesses, i.e., profit-seeking companies and corporations, from existing concerns wherein profit is not the main, underlying objective, i.e., government agencies and charitable organizations.

Initial Public Draft – The NIST Cybersecurity Framework 2.0 – Starting with Page 2, Introduction

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/SUGGESTIONS SUGGESTED ALTERNATIVES/ RATIONALE
Introduction Lines 97-98	Content -- outcome	The NIST Cybersecurity Framework (Framework or CSF) describes essential cybersecurity outcomes that can help an organization reduce its cybersecurity risk.	Cybersecurity outcomes? Granted, NIST mentions cybersecurity outcomes prior to the Introduction. However, the term "outcome" is not used on any of the six function tables, e.g., GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. This is very confusing. In business lingo, could the word *objective* be a synonym for the word "outcome"? Or, does outcome mean end-result?
Line 104	Wording	… understand, access, prioritize, and communicate about cybersecurity risks.	Cut the word about. … communicate cybersecurity risks to whom?
Lines 105 – 126	Usage	-	Understand, Assess, Prioritize, and Inform (Communicate) should be easy to trace to the six Tables. Maybe the Tables need to be reorganized into sections headed by Understand, Assess, Prioritize, and Inform – or similar words.
Lines 106, 107	Content	Describe an organization's current or target cybersecurity procedure …	Isn't it necessary to describe both the current and target? Not sure how to convey that.
Lines 109, 110	Wording	…existing or emerging threats or technologies, and assess progress toward addressing those gaps.	…and address progress toward assessing and rectifying those gaps.
Lines 112, 113	Wording	…or in a more focused area, such as a portion of the organization ….	Do you mean a specific department?
Line 119	Word usage	Inform decisions … Okay. We need to give him the information so that he can make an informed decision.	One informs people, departments, committees, boards of directors or the press = members, groups of people Did you mean inform decision makers?

		"Informed decision" is okay and commonly used. However, I've never heard anyone say or write, *We need to inform decisions.*	One updates, interprets, and evaluates decisions…one does not inform decisions…. Granted, language changes over time … but to the best of my knowledge, you can make informed decisions or risk-informed decisions, but you cannot inform machines or risks – or has the language changed with machine learning?
135-136	Outcome	…The outcomes are based on and are applied to existing global standards, guidelines, and practices.	Granted, the global standards, guidelines, and practices are a good idea – but please consider putting them in an appendix at the end of the document. Yes, some page turning will be needed. The readability of the document is important – too much information (TMI) on one page makes a more difficult read.
Box on page 3	1.) The word "like" 2.) The word "their" 3.) Content	1.) … Actions to reduce cybersecurity risk might benefit the organization in other ways, like … 2.) The word their – i.e., their own should be its own. 3.) Isn't "moving a major financial system from the organization's in-house data center to the hosting provider" a tad risky? Outsourcing any type of core service or product always adds risk. The reason why Border's Books failed is that they outsourced a core service.	1.) Use "for example" or "for instance." The word "like" should not be used to precede an example. 2.) Use the pronoun *its* when referring to companies and organizations – for hosting **its** own – not their own. 3.) Actions to reduce cybersecurity risk might benefit the organization in other ways; increasing revenue is one possibility. For example, the organization might consider leasing excess facility space to a commercial hosting provider. Then, to consider reducing expenses, as well as cybersecurity risk, the organization could relocate one or more of its current in-house systems to its new, hosting-provider lessee.
142-143	Hyphen usage	The Framework is forward-looking and is intended to apply to future changes in technologies and environments.	It is a forward-looking Framework. (hyphen needed) The Framework is forward looking. (no hyphen needed)

151-154	Sentence rewording suggestion	Does every single example need to be identified, e.g., boards of directors, acquisition professionals, HR specialists, etc. – or would limit listings to three examples enhance readability without really decreasing clarity or meaning?	The Framework can also assist executives, lawyers, auditor committee members, and others involved in managing or assessing risk to make better-informed cybersecurity decisions.
Box top of page 4	Two separate sources of quotations	Quotations from different sources need to be in separate paragraphs.	Consider separating the first paragraph in the box into two paragraphs. The first is the Executive Order; the second, the Enhancement Act of 2014.
Line 170	Notional		Consider using a more common word – Suggested, for example.
Lines 180-185	Content/Context Order	Additionally, the order of Functions, Categories, and Subcategories in the Core is not intended to imply the sequence --	Okay, the intention is not to prescribe an absolute sequence order to be followed; however, there is a natural order inherent to the functions – from IDENTIFY (#2) through RECOVER (#6). An adverse event is detected, responded to, and either or both the data and system is restored. Although there may be an occasion to RESPOND to events that are not detected, this practice would indicate a potential problem with the DETECT function. Will the employee or the business that makes it a practice to RECOVER data that is not missing or damaged be around for long? My point: there is a natural flow to these processes/functions. There is also an order to the categories and subcategories – not an absolute order but a flow of concepts and practices. Imagine reading through a list of six or seven **Implementation Examples** and the last

			one pertains to a policy that should be in place prior to any action taking place. = Huh?
223-225	Grammar: Subject-Verb parallelism	RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication …	RECOVER supports **the** timely impact Change **enable** to **enables (tenses must agree)** What is "appropriate" communication? And, how does RECOVER enable communication? It doesn't.
Fig. 1, pg 5 Line 261	Framework Core, Definition and Word Sequence	While Informative References and Implementation Examples are not considered part of the Core…	Figure 1 = *Cybersecurity Framework Core* A quick glance at this figure may lead one to believe that Functions, Categories, and Subcategories create Implementation Examples and Informative References and all are part of the Framework Core. = Confusing.

NOTE: THE FOLLOWING FUNCTION TABLES COMPRISE COMMENTS AND SUGGESTIONS. THEY ARE NOT PERFECT – THEY ALL REPRESENT IDEAS FROM MY FIRST READING. IN A SEPARATE DOCUMENT ENTITLED *CSF TABLES,* I'VE ATTEMPTED TO RE-CREATE THE TABLES. THESE RECREATIONS ARE FAR FROM PERFECT AS WELL. SOMETIMES I PLAYED AROUND WITH THE LANGUAGE IN AN ATTEMPT TO BETTER EXPRESS THE CONCEPT. SOMETIMES I RE-TYPED WHAT NIST ORIGINALLY WROTE AS IT WAS BETTER. SOMETIMES THE TWO DOCUMENTS, I.E., THIS COMMENTS DOCUMENT AND THE TABLES DOCUMENT, WILL NOT BE IDENTICAL.

ADDITIONALLY, MY INTENTION IS TO CONVINCE NIST THAT IT NEEDS TO REFOCUS THIS DOCUMENT FROM THE PERSPECTIVE OF THE APPLICATION – MY ATTEMPTS TO EDIT THESE TABLES DO NOT DEMONSTRATE THIS PERSPECTIVE.

FUNCTION TABLE #1 GOVERN (GV)

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/ SUGGESTED ALTERNATIVES/RATIONALE
GV.OC	Wording, punctuation, and a "hanging" concept (my terminology) = are understood…	The circumstances – mission, stakeholder expectations, and legal, regulatory and contractual requirements – **surrounding** the organization's cybersecurity risk management decisions **are understood**. Note: Grammar issue – many writers use "their" as the pronoun for an organization – "its" is preferable. An organization is aware of its responsibilities. Organizations are aware of their responsibilities.	The factors **contributing to and supporting** the organization's cybersecurity risk management decisions – factors including the organization's mission and vision statements, stakeholder expectations, and regulatory requirements – are understood. Understood by whom and for what purpose? How do you know if something is understood? Okay. "Understood" here means that the organization is expected to be knowledgeable. Make into an active sentences? The organization is aware of the contributing factors supporting its cybersecurity management decisions. These factors include the organization's mission and vision statements, stakeholder expectations, and regulatory requirements.
GV.OC-02	Inappropriate usage of the word *determined* -- hinders readability	Internal and external stakeholders are **determined** …	Internal and external stakeholders are **identified …** The subjects in this sentence are people, i.e., internal and external stakeholders. When reading the sentence, readers may initially think that the internal and external stakeholders are determined to do something. For example, internal and external stakeholders are determined to prevent cybersecurity attacks.
GV.OC-02 GV.OC-03	Understood Hanging concept	… are understood … are understood	Same issue as GV.OC. The more I read the Framework, the more I understand NIST's usage of the term, "understood." However, is it a good idea to use this term? The only way to really know if someone understands is to test – and

			testing higher level management or executives in any organization is tricky. Asking someone, "do you understand?" will often result in a "yes" answer to hide one's insecurity or lack of knowledge – no one likes to appear ignorant.
GV.OC-04 GV.OC-05	Determined – usage is okay Determined	Critical objectives, capabilities, and services…are **determined** … Same issue	The subjects in this sentence are not people, i.e., *critical objects, capabilities, and services* are things being determined; hence, using the word *determined* does not affect readability. However, one could also use *identified* in this sentence, or better yet, *established*. Same comments.
GV.RM	Wording	The organization's priorities, constraints, **risk tolerance and appetite statements,** and assumptions… Here, the writer needs to be clear that risk tolerance and risk appetite are related but separate concepts. See GM.RM-02: change the word order to risk appetite and risk tolerance.	The organization's priorities, constraints, and assumptions, as well as its risk appetite and risk tolerance statements are established, communicated, and used to support operational-risk decisions. I've separated *priorities, constraints, and assumptions* from *risk tolerance and risk appetite* for readability purposes and the fact that they are two separate categories.
GV.RM-02	Word order	**Risk appetite** and **risk tolerance** statements are …	Keep the order the same as in GV.RM – Risk appetite and risk **tolerance.** **Use the risk appetite and risk tolerance order for both GV.RM and GV.RM-02.** Why? The definitions. While risk appetite is the amount of risk an organization is willing to accept, risk tolerance is the acceptable deviation from the risk appetite. (Source = Tech Target, 8/3/ 2023). In other

			words, one cannot calculate risk tolerance w/o risk appetite – so, list risk appetite first.
GV.RM-05	Sentence construction *Other third parties*	… including **risks from suppliers** and other third parties	Lines of communication pertaining to cybersecurity risk are established; these lines **include supply-chain risk as well as risks from other third-parties including ???? cloud vendors and Internet providers.** Note the use of a semicolon (;). One could use a dash (–) instead of the semicolon. Would NIST consider the practice of always including an example or two when referring to "other something"?
GV.RM-06	Hanging concept	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and **communicated …**	…is communicated to whom and how? *Communicated* by itself just hangs… … is documented as a component of cybersecurity policy as well as distributed to and discussed with those management members and employees who have cybersecurity-related responsibilities.
GV.SC-01	Sentence Construction	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	A Cybersecurity Supply Chain Risk Management (C-SCRM) program comprises strategies, objectives, policies, and processes that are established and agreed to by organizational stakeholders.
GV.SC-03	Sentence Construction	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	Cybersecurity Supply Chain Risk Management (C-SCRM) is integrated into cybersecurity and enterprise risk management models and comprises risk assessment as well as process improvement components.
GV.SC-04	Weak	Suppliers are known and prioritized by criticality.	Products and services are purchased only from suppliers approved in accordance with the organization's Purchasing Policy. Lists of approved suppliers are maintained by the

			Purchasing Department and shared with pre-designated systems management members. Why? There's a potential control issue here. How does the organization define *criticality?* Is the organization only sole sourcing? If a system component suddenly needs a replacement part, are these parts stocked in house? Does the organization have more than one supplier for that critical part? After re-reading, I now understand that "criticality" refers to business continuity.
GV.SC-07	Pronoun misuse – its and *their* Word confusion -- *over* sentence construction *other third parties*	The risks posed by a supplier, **their** products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship. What type of *"other third parties"* is the writer talking about? Does other third parties refer to third parties of the supplier? If that's the case: The risks posed by a supplier, its products, services, and associated third parties…	The risks posed by **a supplier** and **its products** and services are identified, recorded, prioritized, assessed, responded to, and monitored **during** the course of the business relationship. Or … The risks posed by **suppliers** and **their products** and services are identified… … a supplier = singular -- use *its* products … suppliers = plural – use *their* products Replace over with during. Using "over" is not wrong; actually, it's perfectly acceptable. However, foreign speakers of English often become very confused with this construction, sometimes interpreting *over* as meaning "above." Suggested sentence with "other third parties included…"

			The risks posed by suppliers and their products and services coupled with the risks posed by other third parties and their products and services are identified, recorded, prioritized, assessed, responded to, and monitored during the course of the business relationship.
GV.RR	Sentence missing the word "designed"	Cybersecurity roles, responsibilities, and authorities **to** foster accountability, performance assessment, and continuous improvement are established and communicated.	Cybersecurity roles, responsibilities, and authorities **designed to** foster accountability, performance assessment, and continuous improvement are established and communicated with whom?. … throughout the organization.
GV.RR.01	Word added for meaning – and humor	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk aware, ethical, continuously improving, and *contagious*. Consider*: adopted throughout the organization* instead of contagious. *Contagious* may not be a good choice for a business document – but the term makes its point: organizational behavior is set by top management. Management's behavior sets the tone – and good, ethical behavior should spread from the top down and filter throughout the organization. Risk aware does not need to be hyphenated unless it is followed by a noun, i.e., risk-aware culture vs. a culture that is risk aware. *Continually improving* is an okay choice but the more common expression is "continuous improvement" – so in this sentence, the term would be **continuously improving**. The difference? *Continual* means with an occasional interruption; *continuous means ongoing without any interruption.* Actually, "continually improving" is saner.

GV.RR-02 Ex.05	Internal Audit functions Comment and clarification	Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions. For Internal Audit, "clearly articulate" refers only to general functions.	The role of the Internal Audit Department would normally be to provide reasonable assurance that the organization's cybersecurity processes are operating efficiently and effectively to achieve their designated objectives in a securely controlled environment – an environment in which the internal controls are functioning to protect the confidentiality, integrity, and availability of data. Basically, only the Internal Audit Director – a position which reports directly to the Internal Audit Committee of the Board of Directors – has the authority to tell an internal auditor how to proceed or how not to proceed. In other words, Director Bob Smith of the Accounting Department cannot demand that Internal Audit Director Jones or staff internal auditor Mary Lee who works for Internal Audit Director Jones, either investigate or disregard an accounting employee and/or any process or procedure undertaken by that employee. Accounting Director Bob Smith can suggest to any member of the Internal Audit Department that he would like something or someone reviewed or investigated. The better chain of communication for Bob Smith would be, however, directly with the Audit Director. In any event, only the Internal Audit Director would normally make the decision as to follow up on Accounting Director Bob Smith's request or not. Demanding or even insinuating to any member of the Internal Audit Department that someone or something should **not** be investigated or audited usually sends sparkling red flags. (Reference, Cynthia Cooper and World Com)

CV.RR-04	Context	Cybersecurity is included in human resource practices.	Cybersecurity practices are incorporated into human resource policies and practices to cultivate a security-awareness mindset throughout the organization.
GV.PO-01	Sentence construction – punctuation issue affects sentence meaning	Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced. These are two separate sentences!	Policies, processes, and procedures for managing cybersecurity risks are established based on business priorities – all of which are communicated and enforced throughout the organization. Or – use a semicolon: Policies, processes, and procedures for managing cybersecurity risks are established and prioritized based on organizational context and cybersecurity strategies; these priorities are then communicated and enforced throughout the organization.
GV.PO-02	Sentence construction – listing issue	Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission. Just mission and not visions?	Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, and technologies as well as the organization's mission. Policies, processes, and procedures for managing cybersecurity risks stemming from changes in an organization's mission are identified, reviewed, and updated; they are then communicated and enforced throughout the organization. Change *mission* to "goals and objectives"?
GV.OC-01	Context	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	Cybersecurity risk management strategies are periodically reviewed for purposes of adjusting strategic direction.

		Does "strategy outcomes" need definition?	Cybersecurity risk management strategic outcomes are periodically reviewed to determine if they protect the organization from events, incidents, and disasters.
GV.OC.02	Added re audit	#2 is added. Why? Often times a process can become ridiculously overcontrolled as to affect productivity in a negative way. And then, sometimes controls may be operating as designed, but "as designed" is not efficient or effective enough.	**Ex-01:** **Review** audit report findings to determine whether or not current cybersecurity internal controls are working as designed. **Ex-02:** **Review** audit report findings to determine if current controls that are working as designed efficiently and effectively prevent or detect the abnormalities that they were designed to control.
GV.PO-01	"organizational context" Need two separate sentences of punctuate differently	Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced.	Is NIST using the term "organizational context" in a project management sense, i.e., the firm's size, degree of centralization, degree of formalization, and managerial structure. Yes, I think so. (Source = ScienceDirect.com) Either add a comma after priorities or, better yet: Policies, processes, and procedures for managing cybersecurity risks are based on organizational context, cybersecurity strategy, and the organization's goals and objectives; these policies, processes, and procedures are communicated and enforced throughout the organization.

Function Table 2: IDENTIFY (ID)

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/SUGGESTED ALTERNATIVES/RATIONALE
Table 2. IDENTIFY (ID): One-line description	***Help*** determine the current cybersecurity risk to the organization	Recognize the current and potential future cybersecurity risks to the organization.	"Help" is the wrong term – it implies that employees and other human resources are only trying and not accomplishing. Compare: I will try to do my best vs. I will do my best. Do not limit the recognition of risk to current risks. Noticing a vulnerability that is currently not causing a problem but could be exploited in the future is tantamount to prevention.
ID.AM Asset Management	Misuse of an adjective (grammar issue) When you refer to how something is accomplished, you need an adverb.	**ID.AM** **Asset Management**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve its business purposes are identified and **managed consistent** with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM** **Asset Management**: Assets – including data, hardware software, systems, facilities, services, **and** human resources – which enable the organization to achieve its business purposes are identified and **managed consistently** in accordance with their relative importance to the organization's risk strategy. Or: … managed in a manner consistent with … managed in a manner commensurate with … All organizations have a business purpose but is using this term confusing? A governmental department has a purpose – but will Readers assume that a business purpose means a corporate purpose? Replace *business* with "goals and objectives"?

TABLE 3: PROTECT (PR) (**and/or PREVENT) Note: Prevent is how ISACA views this** --

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/SUGGESTED ALTERNATIVES/RATIONALE
PR.AA Identity Management, Authentication, and Access Control	Two sentences combined into one.	**PR.AA Identity Management, Authentication, and Access Control** Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access.	Make into two sentences, i.e., or use a semicolon. Access to physical and logical assets is limited to authorized users, services, and hardware. Access to physical and logical assets is managed consistently, commensurate with the assessed risk of unauthorized access. Access to physical and logical assets is limited to authorized users, services, and hardware; this access is managed consistently, commensurate with the assessed risk of unauthorized access.
Table 3: PR.AA-05	Sentence configuration	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.	Access permissions, entitlements, and authorizations are defined in a policy, and then managed, enforced, and reviewed. This is one sentence. Notice that defined, managed, enforced, and reviewed are all in the same tense and voice. Access permissions, entitlements, and authorizations incorporate the principles of least privilege and separation of duties. Another sentence with a different voice. Suggestion: rewrite into two separate SUBCATEGORIES.
Table 3: PR.DS	Adverb needed	Data is managed consistent with …	Data is managed consistently … Data is managed in a manner consistent with …

Table 3: PR.PS	Sentence configuration Adjective/Adverb issue (consistent) Pronoun misuse (their)	**PR.PS** **Platform Security** The hardware, software (e.g., firmware, operating systems, applications), and the services of physical and virtual platforms are managed consistent with the organization's risk strategy, to protect their confidentiality, integrity, and availability.	The hardware, software – e.g., the firmware, operating systems, and applications – as well as the physical and virtual platform services are managed in a manner consistently with how the organization's risk strategy is managed: to protect the confidentiality, integrity, and availability of what? *And* is added after the last item in a list. *As well as* replaces "and" to minimize the # of ands in the sentence. **What does the pronoun *their* refer to? It's difficult to determine the way this sentence is written.** **Or:** The physical and virtual platform services are managed to protect the confidentiality, integrity, and availability of data in a manner similar to how the organization's risk strategy is developed and managed.
			PR.DS-01 The confidentiality, integrity, and availability of data at rest are protected from prying eyes, theft, unapproved alteration, and inappropriate destruction. Does the example only refer to digital data or would clean desk policy apply here? Is prying eyes acceptable here? Note: PR.DS-09 specifies destruction of paper; this tells me the Framework pertains to more than digital.

FUNCTION TABLE 4: DETECT (DE)

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/SUGGESTED ALTERNATIVES/RATIONALE
Table 4: DE.CM	Definitions needed? "Adverse events" is the term used in subcategories, e.g., DE.CM-01 through DE.CM-09 and DE.AE-02, DE.AE-06. Yet in both DE.CM and DE.AE, in addition to "Adverse events," anomalies and indicators of compromise are also listed.	**DE.CM** **Continuous Monitoring** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. **DE.AE** **Adverse Event Analysis** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and to detect cybersecurity incidents. Or: instead of *other anomalies* use "other suspicious activities"?	What is the difference between an anomaly, indicator of compromise, and an adverse event? Does this definition comply with the NIST definition? • Anomaly detection systems (ADS) use machine learning algorithms to identify patterns of behavior that are outside of the norm. (source = otifyd.com) SUGGESTION: If NIST's definition of "anomaly" is generalized and not specific to machine learning, consider re-writing DE.CM and DE.AE as follows: **DE.CM** **Continuous Monitoring** Assets are monitored continuously in order to detect all forms of potentially adverse events, including known Indicators of Compromise (IoC) and other suspicious activities. **DE.AE** **Adverse Event Analysis** All potentially adverse events, including indictors of compromise (IoC) and suspicious activities, are analyzed to determine whether or not the specific events themselves or the patterns of events

			detected are, or could be, considered cybersecurity incidents.
Table 4: DE.CM-03		Personnel activity and technology usage are monitored to find potentially adverse events.	*Personnel* is somewhat antiquated, at least in corporate environments. "Human resources" is a more common term used for the name of departments, i.e., the Human Resources Department. Personnel could be used in this document when referring to people – or use the term, "employee" – but the usage should be consistent throughout the document.
Table 4: DE.CM-03a	added		I realize this example is not really cybersecurity related…but I also envision that this type of monitoring will come under one security umbrella someday: ACTIVITY: Monitor the organization's databases for potentially fraudulent events – a use case follows: Identify purchased products sorted by specific departments. One such list identifies 24 DeskJet printers purchased by the Sales Department during the last six months, i.e., four printers per month. Further investigation reveals that all Purchase Orders from the Sales Department were appropriately authorized by the Department Head and the expenditures were within authorized dollar limits. The Purchasing Department Head Officer is authorized to sign for purchases under $2,000 dollars without requiring another approval signature. Upon reading this information, you think

			it's strange as there are only four employees currently employed in the organization's Sales Department. Why would four employees need 24 printers? What's even more interesting is that all 24 printers were delivered to an out-of-state address. One consequence of this discovery is that you recognize the importance of having continuous auditing software – software that continuously examines data and identifies and reports potentially fraudulent activities.
Table 4: DE.CM-09 Ex02:	Sentence meaning	Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse.	Monitor authentication attempts to … identify attempts to steal credentials ??? Does unauthorized credential reuse mean … someone beside me has used my credentials and they use them again? Should this read, "… and unauthorized credential use?" Or, is the author specifying replay attacks?

See the Six Tables file for more information.

FUNCTION TABLE 5 RESPOND (RS)

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/SUGGESTED ALTERNATIVES/RATIONALE
RS.MA	Hanging (my term) concept	**RS.MA** **Incident Management** Responses to detected cybersecurity incidents are managed to do what?	

FUNCTION TABLE 6 RECOVER (RC)

ISSUE LOCATION	ISSUE TYPE	NIST WRITING	COMMENTS/QUESTIONS/SUGGESTED ALTERNATIVES/RATIONALE