CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
GOVERN (GV)	Organizational Context (GV.OC)	GV.OC-04	The subcategory loses text from the previous version that guides the system owner and stakeholders to determine and communicate objectives/capabilities/services for all system states, not just the operational state.
GOVERN (GV)	Risk Management Strategy (GV.RM)	GV.RM-03	An "organization's business environment" is not the only factor in an organization's risk appetite and risk tolerance. The subcategory as worded only guides system owner's to consider business environment.
GOVERN (GV)	Risk Management Strategy (GV.RM)	GV.RM-04	This subcategory is vague. "Considered" is not an actionable verb, so the subcategory doesn't actually direct or guide anyone to do anything. This should be changed to "Cybersecurity risk management is carried out <alongside/as part of> enterprise risk management", or something along those lines.
GOVERN (GV)	Roles and Responsibilities (GV.RR)	GV.RR-01	What is organizational leadership "promoting continuous improvement" of? Examples could include system user cybersecurity training and secure system design. There is not enough context within the subcategory to make an assumption.
GOVERN (GV)	Risk Management Strategy (GV.RM); Roles and Responsibilities (GV.RR)	GV.RM-06; GV.RR-01/02	GV.RM-06 overlaps with GV.RR-01/02. "responsibility and accountability…for ensuring that the risk management strategy and program are resourced, implemented, assessed, and maintained" (GV.RM-06) is part of "organizational leadership takes responsibility for decisions associated with cybersecurity risks…" (GV.RR-01) and "roles and responsibilities related to cybersecurity risk management are established and communicated" (GV.RR-02). GV.RM-06 is a responsibility that should be assigned in GV.RR-02 and is accountability assigned to organizational leadership in GV.RR-01.
GOVERN (GV)	Policies and Procedures (GV.PO)	GV.PO-02	It is unrealistic to expect the same cybersecurity policies used internally to be applied to suppliers. Oftentimes, internal policies

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
			assume a base level of trust that you will not have with every supplier, so you may need stricter policies than you have internally. Furthermore, it may not be organizationally/technically possible to apply those policies to external parties, as they may have different workflows and their own policies to work around. However, it is realistic to have a baseline set of policies that every sponsor you work has to adhere to, which you can then further tailor on a supplier-by-supplier basis based on organizational environment and risk management strategy.
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-08	Systems, devices, and software are not the only assets that must be managed throughout their lifestyle. By only including a sub-set of the asset types listed in the examples of assets provided in the Asset Management category, many types of assets that need to be maintained are excluded. Facilities and people must be managed throughout their lifecycle as well. For example, as a person moves through the organization from project to project or by promotion, their access control needs change, and when an employee leaves the organization, their access must be terminated. It is possible that PR.AA-01 and PR.AA-02 may cover other assets. Yet having 'asset management' spread across elements would seem to 'hide' aspects of 'asset management' and having all aspects addressed in the ID.AM category is suggested as the better alternative.
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-08	ID.AM-08 aims to cover the topics covered in the former PR.MA-1/2 (the performance and logging of maintenance/repair of assets with approved and controlled tools) and fails to do so. ID.AM-08 mentions managing assets throughout their lifecycle and lists the lifecycle phases in which they must be managed. ID.AM-08 claims

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
			to cover PR.MA-1/2 but it does not cover the method of performance of maintenance.
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-07	ID.RA-07 is based on part of the former PR.IP-3, which addressed configuration change control. ID.RA-07 does not specify the types of changes that must be included in the change control program. Given the surrounding subcategories, this could be misunderstood to be changes to the risk management strategy or changes to risk responses decided prior. ID.RA-07 should be edited to "Configuration changes…" instead of "Changes…".
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-10	Subcategory is vague. Does "exceptions to security measures" mean times the organization approves organizational or technical security policies to be broken, as in approving a blacklisted OS to be installed on a device? Or does "exceptions to security measures" mean times the organization has accepted the risk, as in chosen not to avoid/mitigate/transfer it? If the former, it needs to be more concise, and if the latter, it's covered by ID.RA-06.
IDENTIFY (ID)	Improvement (ID.IM)	ID.IM-02	Lack of continuity across ID.IM subcategories. ID.IM-02 does not mention "…improvement across all Framework Functions" like its peers. As defined, ID.IM-02 will only improve cybersecurity risk management processes and activities via security tests and exercises; it will not improve activities across the Functions and their implementations.
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-03	PR.AA-03 attempts to cover the former PR.AC-3 and PR.AC-7. PR.AC-7 includes that risk tolerance plays a role in the chosen authentication method; PR.AA-03 leaves that out. PR.AA-03 loses value from the prior subcategories by only generalizing that authentication must happen. There are certainly circumstances in which stronger authentication is needed for a less-trusted user/process/device.

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-04	PR.AA-04 is at a different level of granularity than PR.AA-03. PR.AA-03 only generically guides that authentication should be used, and then PR.AA-04 specifically guides that SSO should be used. PR.AA-04 should be specifically for "If federated assertions are <used>,…" and then guidance on securing them.
IDENTIFY (ID); PROTECT (PR)	Asset Management (ID.AM); Data Security (PR.DS)	ID.AM-07; PR.DS-09	These subcategories overlap. ID.AM-07 specifically calls for sensitive data and metadata to be inventoried and tracked, but then PR.DS-09 calls for all data to be managed throughout its lifecycle. How can non-sensitive data be managed without being inventoried (as mentioned in ID.AM-07 for sensitive data)? Arguably, inventory is part of the data "discovery" life cycle phase, meaning ID.AM-07 can be removed, or ID.AM-07 can be expanded to include non-sensitive data and PR.DS-09 can be removed.
PROTECT (PR)	Platform Security (PR.PS)	PR.PS-01	The subcategory is vague. It's meant to reconcile the former PR.IP-1, PR.IP-3, PR.PT-2, and PR.PT-3 into one subcategory, but instead it calls for generic "configuration management practices" and then gives "least functionality" and "least privilege" as examples. "Configuration management practices" cannot stand alone – there's too many things that fall into that category that without at least linking to a directive of what is included in that category, its meaningless. Value is lost by making configuration management practices a generic statement and then providing two specific examples; system baseline creation and maintenance, removable media policy, etc are likely to be lost.
PROTECT (PR)	Platform Security (PR.PS)	PR.PS-03	Hardware should also be added commensurate with risk; i.e.: Hardware is added, maintained, replaced, and removed commensurate with risk.
PROTECT (PR); DETECT (DE)	Data Security (PR.DS); Platform Security (PR.PS); Technology		Categories are not peers, with items in one category directly-contributing-to/being-a-part-of items in another:

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
	Infrastructure Resilience (PR.IR)		Categories Platform Security (PR.PS) and Technology Infrastructure Resilience (PR.IR) [particularly subcategory PR.IR-02], and function Detect (DE) are all an important part of achieving Data Security (PR.DS). It seems that PR.DS cannot be achieved without them.
PROTECT (PR)	Data Security (PR.DS)	PR.DS-01/02/10	'Holistic' subcategories that appear to be themselves the totality of the cybersecurity need: If PR.DS-01/02/10 is provided (confidentiality, integrity, and availability of data-at-rest, data-in-transit, and data-in-use), then what more is needed? Either the taxonomy has issues or there is a lot of 'implied' in these.
PROTECT (PR)	Technology Infrastructure Resilience (PR.IR); Platform Security (PR.PS)		Confusing titles: It is unclear why PR.IR is Technology Infrastructure Resilience while PR.PS is Platform Security; especially since there is no PR.IR subcategory that reads like 'resilience' (as in some form of 'fight through').
DETECT (DE)	Adverse Event Analysis (DE.AE)	DE.AE-04	The subcategory is vague and likely misplaced. When does the estimation of impact and scope of adverse events determined? If this is meant to occur before an event occurs, that should be part of risk assessment or risk management strategy. If this is meant to occur while a discovered event is occurring or immediately after, it's part of response. Either way, it determining the impact/scope of adverse events is not a detection action.
DETECT (DE)	Adverse Event Analysis (DE.AE)	DE.AE-08	The subcategory is likely misplaced. Categorization of events and escalating potential incidents for triage are not detection actions – they do not actively aid an event in being found, whether by utilizing tools, alarms, or integrating information into the detection

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Subcategory	Comments
			environment. Instead, they are part of the initial response to detecting something.
RESPOND (RS)	Incident Management (RS.MA)	RS.MA-03/04	These subcategories can be combined; i.e.: Incidents are categorized, prioritized, and escalated as necessary. They both aim to cover the former RS.AN-2 and there's not enough content difference for them to need to be separated into two subcategories.
RESPOND (RS)	Incident Management (RS.MA)	RS.MA-05	Defining the criteria to initiate incident recovery procedures needs to happen outside of a response. If an organization waits until an incident response is necessary to define the criteria necessary to initiate recovery, they are losing valuable time. Applying is the part of this subcategory that should remain in RESPOND; defining should be moved to IDENTIFY or PROTECT. The establishment and communication of response and recovery plans is in PR.IR-01, defining criteria to initiate an incident recovery belongs near that.
RECOVER (RC)	Incident Recovery Communication (RC.CO)	RC.CO-02	'Holistic' subcategories that appear to be themselves the totality of the cybersecurity need: An organization's reputation being repaired after an incident is what they wish to obtain. It something that the organization hopes comes from managing public relations (RC.CO-01), managing external stakeholder expectations (RC.CO-03), managing internal organization feelings (RC.CO-03), and improving based on lessons learned (ID.IM-03). It is not actionable guidance and should not be a subcategory, as it is not something completely in their control.