N°	Function	Rules	Comments
1	Global	N/A	European network and information security directive (NIS) relies on 4 pillars: Governance, Protection, Defense, Resilience. The mapping between NIST CSF 2.0 functions and NIS II pillars is approximately as follow: - Governance (NIS II) => Governance and Identify (NIST CSF 2.0) - Protection (NIS II) => Protect (NIST CSF 2.0) - Defense (NIS II) => Defense and Respond (NIST CSF 2.0) - Resilience (NIS II) => Recover (NIST CSF 2.0) It could be interesting to notify this mapping as a try to bridge US and European approaches
2	Global	N/A	European Union member states are actually defining national laws to take into account the network and information security directive published in late 2022 (https://eur-lex.europa.eu/eli/dir/2022/2555). This new directive will be applicable to small businesses which have no resource nor the cybersecurity maturity to "deep dive" into cybersecurity . Some of our comments are based on France thoughts on - requirements we can apply to these small businesses based on their resources and capabilities to comply with them - requirements that are too demanding for small businesses Does this cybersecurity framework apply to all kind of organization, small or big ? It could be interesting to precise this in a scope section. Or to indicate at a subcategory level which one apply to all kind of organizations and which one apply to big organizations
3	Global	N/A	It could be interesting to bring some terms and definitions in the document in order to bring a common comprehension. Some terms we think could be defined: - stakeholders: in particular, does national cybersecurity authorities are considered stakeholders (referring to some of our comments) - cybersecurity events (for example in DE.CM-09) - etc.
4	Governance	GV.RM-07	It could be interesting to precise the periodicity of risk management strategy's revisions. This proposal tends to make the link with the continual improvement the NIST CSF 2.0 promote. We propose: "[…] *review at planned intervals and when significant changes or incidents occur* […]"
5	Governance	GV.RM-08	It could be interesting to precise the periodicity. This proposal tends to make the link with the continual improvement the NIST CSF 2.0 promote. We propose: "[…] *review at planned intervals and when significant changes or incidents occur* […]"
6	Governance	GV.RR	It could be interesting to add a dedicated subcategory for top management in order to explicit their cybersecurity responsibilities within the organization and ensure that cybersecurity is taken into account at all levels in the organization
7	Governance	GV.RR-02	It could be interesting to add that roles and responsibilities should be agreed or validated by top management / leadership
8	Governance	GV.RR-03	It could be interesting to add that roles and responsibilities should be agreed or validated by top management / leadership
9	Governance	GV.RR-03	It could be interesting that roles and responsibilities for customers, partners and other third-party stakeholders should be documented in contractual language such as it is specified in GV.RR-04
10	Governance	GV.PO-01	It could be interesting that policies and procedures should be validated by top management. It could be interesting to have a dedicated subcategory on the information security policy in the organization that should be validated by top management
11	Identify	ID.AM	We consider that the subcategories listed in this category are too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them. For example, in the NIS II context, we require small businesses to maintain a list of their information systems and networks with, for each, a functionnal description, the availability needs in terms of MTPD et RPO. We also demand that small businesses maintain a list of their digital suppliers.
12	Identify	ID.AM-02	It could be interesting to precise that this subcategory apply whether the organization manages directly the services or if it relies on external providers (*for example: Cloud provider*)
13	Identify	ID.AM-03	We consider that this subcategory is too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them. It could be interesting to focus only on information systems, networks and data flows that are exposed to third parties (*for example: Internet*)
14	Identify	ID.AM-04	It could be interesting to also inventory interconnection with third parties networks
15	Identify	ID.AM-07	We consider that this subcategory is too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them (see global comment on ID.AM).
16	Identify	ID.RA	The risk assessment category does not mention residual risks and how they are manage. In our view, it could be interesting to add a subcategory here to indicate that residual risks should be validated by top management
17	Identify	ID.RA	Experience shows us that small businesses does not have the resources nor the capability to realize a risk analysis. In some cases, they are not even capable to intiate such a process. For some others, the risk treatment plan resulting from the risk analysis only list cybersecurity hygiene measures. These observations tend to not require small businesses to perform a risk analysis. Instead, we require them to comply with requirements lawmaker has defined in order to handle threats this businesses could face.
18	Identify	ID.RA	It could be interesting to add a subcategory dealing with the review process of the risk assessment
19	Identify	ID.RA-01	We do not think necessary to validate vulnerabilities. Which role is responsible for this validation ?
20	Identify	ID.RA-06	It could be interesting that risk responses should be validated by top management in order to obtain resources need to implement those responses.
21	Identify	ID.RA-09	In our view, this subcategory could be in the detection or response function such as defined in the previous version.
22	Identify	ID.RA-10	It could be interesting that exceptions should be validated by top management.
23	Identify	ID.SC	It could be interesting to centralize all subcategory dealing with supply chain. For example: GOV.RR-04, GOV.PO-02, ID.AM-04, ID.RA-08, ID-IM-02
24	Identify	ID.IM-02	It could be interesting to mention the coordination with authorities
25	Protect	PR.AA-06	In our view, small businesses do not have resources nor the maturity to correctly log events and analyze them

26	Protect	PR.PS-02	It could be interesting to precise this subcategory to introduce an exception when operational constraints does not allow an organization to update its systems (*for example: operational systems such as ICS*)
27	Protect	PR.PS-04	We consider that this subcategory is too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them.
28	Protect	PR.IR.01	We consider that this subcategory is too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them.
29	Protect	PR.IR.02	In our view, this subcategory could be in the identity management, authentication and access control.
30	Detect	DE	We consider that this function is too demanding for small businesses that do not have resources nor cybersecurity maturity to apply them.
31	Response	RS.CO-02	It could be interesting to precise that incidents' notification can be a contractual requirement. Furthermore, it could be interesting to precise that authorities can be a recipient of incidents' notification
32	Recover	RC	It could be interesting to add category / subcategories dealing with crisis management. A security incident can have dramatic consequences which could lead to requalify it as a cybersecurity crisis. In this case, organizations should have: - a crisis management organization with role and responsibilities both at a strategic and operational level - processes to determine in which case the organization should switch in an crisis organization and when to return to normal - lists of * providers that could help in cybersecurity crisis situation (for example: cybersecurity response team, insurance) * employees that are willing to be participate to manage the crisis with directory and contact information - contacts with authorities and precaution to take in order to file a lawsuit - communication strategy and tools - etc.