| # | Organization | Commentor | Type | Page # | Line # | Section | Comment (Include rationale for comment) | Suggested change |
|---|---|---|---|---|---|---|---|---|
| 1 | Unified Compliance Framework | Dorian Cougias | E | 13 | | ID.AM-2 | You mention "software platform" but don't define it. There are several definitions of that term. Please define it. | Please define software platform. |
| 2 | Unified Compliance Framework | Dorian Cougias | E | 13 | | ID.AM-3 | The organizational communication and data flow is mapped - Communcations regarding which business functions? All of them? Those requiring Third Party Oversight? Those surrounding Supply Chain Management? Legal communication flows? Marketng Communication Flow? Be a tad more specific here. | Be specific about what you are suggesting to be mapped. |
| 3 | Unified Compliance Framework | Dorian Cougias | E | 13 | | ID.AM-4 | Use of Catalogue here wherein inventory was used before. | Standardize on your terms please. |
| 4 | Unified Compliance Framework | Dorian Cougias | T | 13 | | ID.AM-4 | External information systems are mapped - what are you asking for? | Are you asking for a network flow diagram? A Network Map? Or are you simply asking that the system be identified and added to the inventory? I highly doubt that Amazon AWS will allow any client to request, let alone obtain, an network map representing their IaaS offering. |
| 5 | Unified Compliance Framework | Dorian Cougias | E | 14 | | ID.AM-6 | This is two distinct mandates. One is the assign roles and responsibilities for the business functions, and the other is to assign roles and responsibilities for cyber security. Organizations don't put these two sets of roles and responsibilities into the same bucket. | Break this into two mandates. One to define roles and reponsibilities for business functions, the second to define roles and responsibilities for cyber security - as it pertains to the organizaiton's business function needs. |
| 6 | Unified Compliance Framework | Dorian Cougias | E | 14 | | ID.BE-1 | Document and communicate the organization's role in the supply chain | This is two mandates again. One is to document the organization's supply chain, and the second is to communicate the organization's role in the supply chain to all affected parties. |
| 7 | Unified Compliance Framework | Dorian Cougias | T | 14 | | ID.BE-2 | The organization’s place in critical infrastructure and their industry ecosystem is identified and communicated -- several problems here. | 1) Like the previous citation, this is actually two mandates. One is to identify and doducment the infrastructure, and the second is to communicate that.<br>2) "The organization's place in critical infrastructure" - and how does an organization *know* its place in the critical infrastructure? Is there a categorization standard that organizations can follow? Is this like a SIC code? |
| 8 | Unified Compliance Framework | Dorian Cougias | T | 15 | | ID.BE-5 | "Resiliency requirements". In English? | What are resiliency requirements? Are these to have a continuity plan? Does this go as far as to have a plan that is tested? Does this also include a pandemic plan? |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 9 | Unified Compliance Framework | Dorian Cougias | T | 15 | | ID.GV-1 | Organizational information security policy is established | In the light of this document, you want more than a simple policy. You are looking for an organizational information security framework, and possibly even an overall internaal control framework that addresses all aspects of compliance. |
| 10 | Unified Compliance Framework | Dorian Cougias | T | 15 | | ID.GV-2 | coordinated and aligned | Are you asking to align the roles with something? If so what? Shouldn't you fist ask the organization to *define* the roles and responsibilities? |
| 11 | Unified Compliance Framework | Dorian Cougias | T | 15 | | ID.RA-2 | "Threat and vulnerability information" | These are multiple feeds. These should be separated out.<br>1) Threat feeds come from organizations supporting the Common Alerting Protocol.<br>2) Technical Vulnerability feeds come from the US' National Vulnerability Database. |
| 12 | Unified Compliance Framework | Dorian Cougias | T | 16 | | ID.RA-4 | Potential impacts are analyzed | Is that potential impact of threats attacking through vulnerabilities?<br>Is that potential impact of threats, regardless of vulnerabilities? |
| 13 | Unified Compliance Framework | Dorian Cougias | T | 16 | | ID.RM-1 | "Risk Management processes" | As defined by FEMA, risk management processes are the combination of<br>- Asset value assessment<br>- Vulnerability assessment<br>- Threat assessment<br>feeding in to<br>- Risk assessment<br>in order to identify mitigating options so that<br>- Risk Management decisions can be made for which mitigating procedures, equipment, personnel, or capital investments should be applied.<br><br>In other words, you are restating that this entire NIST Cybersecurity document be agreed to? |
| 14 | Unified Compliance Framework | Dorian Cougias | T | 17 | | PR.AC-4 | Access permissions are managed | Access permissions include both physical and technical. Since this section has dealt with physical access as well as technical access, are we to assume you mean both? If so, then this should be two separate mandates. |
| 15 | Unified Compliance Framework | Dorian Cougias | T | 17 | | PR.AC-5 | Network Integrity is protected | Are you asking to protect the network access and boundary points?<br>Are you asking to protect the information flow (because that is what AC-4 of NIST 800-53 is about)?<br>Are you asking to perform penetration testing? |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 16 | Unified Compliance Framework | Dorian Cougias | E | 17 | | PR.AT-2 | Privileged users understand roles & responsibilities | 1) Please define "privileged users". Does that mean people with administrative authority? Root Access? Users having a higher standing in the organizational ladder?<br><br>2) Are you calling for an awareness program, a training program, or simply a certification from each individual that they understand their roles and responsibilities? |
| 17 | Unified Compliance Framework | Dorian Cougias | E | 18 | | PR.AT-3 through PR.AT-5 | ...understand roles & responsibilities | Are you calling for an awareness program, a training program, or simply a certification from each individual that they understand their roles and responsibilities? |
| 18 | Unified Compliance Framework | Dorian Cougias | E | 18 | | PR.AT-2 through PR.AT-5 | The naming of different groups | This can be accomplished by simply stating that all interested parties or all constituents be trained. |
| 19 | Unified Compliance Framework | Dorian Cougias | E | 18 | | PR.DS-1 & DS-2 | Protection and Securing | Standardize on one term or the other. |
| 20 | Unified Compliance Framework | Dorian Cougias | E | 19 | | PR.DS-6 | Intellectual property is protected | This could cover everything from trade secret management, through patent and trademark filing, through digital rights management, through data loss prevention. A statement as broad as this is worthless as a direction.<br>We will take this to mean digital rights management for now until further clarification. |
| 21 | Unified Compliance Framework | Dorian Cougias | T | 19 | | PR.DS-7 | Unecessary assets are eliminated | What makes an asset uncecessary? Are you inferring that assets at the end of their lifecycle should be disposed of? Are you inferring that every organization should "Spartanize" their asset list and get rid of things like Coke machines (because they aren't *necessary* to the business)?<br><br>In addition, you've cross referenced this with NIST's sections on separation of duties. What does separation of duties have to do with asset elimination? |
| 22 | Unified Compliance Framework | Dorian Cougias | E | 19 | | PR.DS-9 | Privacy of individuals and personally identifiable information (PII) is protected | Are you suggesting that organizations develop a fully-functional and fully-implementable PII protection program that meets all state, federal, and international guidelines? If so, in the Unified Compliance Framework there are 638 distinct Common Controls that fall under this broad category alone. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 23 | Unified Compliance Framework | Dorian Cougias | T | 19 | | PR.IP-1 | A baseline configuration of information technology/operational technology systems is created | In the Unified Compliance Framework there are 4,625 distinct Common Controls that fall under this broad category alone. If you are suggesting that each organization create baseline configurations for *all* systems in the organization, versus *some* systems that would fall under a scoping methodology, you are out of your collective minds.<br><br>On top of that, programs like SCAP (for automating configurations) are weaker than published. The system types that *don't* have configuration standards outweigh the systems that *do* have configuration standards by 5 to 1. |
| 24 | Unified Compliance Framework | Dorian Cougias | E | 19 | | PR.IP-2 | A System Development Life Cycle to manage systems is implemented | Are you referring to the planning, development, or implementation phase of an SDLC? Or are you referring to the need for the organization to incorporate all four phases when designing and building systems? |
| 25 | Unified Compliance Framework | Dorian Cougias | T | 20 | | PR.IP-7 | Protection processes are continuously improved | Are you asking for after-action reports once an incident has occurred to ensure that protection mechanisms are updated? Or are you asking that there be a general improvement/quality assurance plan for the organization's compliance and security program? Or are you asking that the organization simply communicate updates to its policies, standards, and procedures? |
| 26 | Unified Compliance Framework | Dorian Cougias | T | 20 | | PR.IP-8 | Information sharing occues with appropriate parties | Is this about sharing information (i.e., disclosure), or is this about information flow management (following such guidance as EAR, ITAR, and NISPOM)? |
| 27 | Unified Compliance Framework | Dorian Cougias | T | 20 | | PR.IP-9 | Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed | These are three individual mandates, not the same mandate. These fall under different organizational roles functionally and are put into place and excercised quite differently -- unless you are stating that the BCP and DRP plans should be organized to fall *under* the leadership of an overarching incident plan and incident team. |
| 28 | Unified Compliance Framework | Dorian Cougias | T | 22 | | PR.PT-5 | Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS) | Are you asking that the organization establish and maintain information system assurance categories? |
| 29 | Unified Compliance Framework | Dorian Cougias | T | 22 | | DE.AE-1 | A baseline of normal operations and procedures is identified and managed | A baseline of normal operations *for what?* For every department? For a system's functions, such as a system playing a critical path role in the organization's supply chain? |
| 30 | Unified Compliance Framework | Dorian Cougias | E | 22 | | DE.AE-2 | Attack Target | What is an attack target? The only definition found online is that of some monster in a game. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 31 | Unified Compliance Framework | Dorian Cougias | T | 22 | | DE.AE-3 | Cybersecurity data are correlated from diverse information sources | Which information sources are you referrng to? Internal sources? External sources, such as the National Vulnerability Database, or any of the Common Alert Protocol providers?<br>Or, are you asking the organizaiton to implement some type of SIEM tool with a correlation engine? |
| 32 | Unified Compliance Framework | Dorian Cougias | E | 23 | | D.CM-7 | Unauthorized resources are monitored | What is your definition of an "unauthorized resource"? A rogue computer on the network? A logon attempt that failed? A supply chain resource that "appeared" in the organization without purchase history? A person or group hired to perform a task without proper authorization? A technical intrusion attempt? |