

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
Submitted by Adam Meyer CyberWise Advantage Inc								
				9 & 10	New Content		<p>Replace the current "Implementation Tiers" with the process maturity definitions that are defined within the CERT- Resiliency Management Model (CERT-RMM) The outcome goal is to have process maturity which equates to a better ability to measure process effectiveness. Instead of creating another process maturity definition adopt one that has already been through peer review and is published by the same organization who manages CMMI. Even using the term "Implementation Tier" generates a tone of a one time event , when in reality everything needs to be repeatable and measurable. This is a program and not a project</p>	<p>Level 0 – Incomplete</p> <ul style="list-style-type: none"> - Represents an incomplete process - Indicates that one or more of the specific goals or a process area is not satisfied <p>Level 1 – Performed</p> <ul style="list-style-type: none"> - Represents a performed process - Provides improvement, but can be lost over time without institutionalization - Improvements can only be maintained and sustained by moving to higher capability levels <p>Level 2 – Managed</p> <ul style="list-style-type: none"> - Represents a performed process that has the basic infrastructure in place to support the process - The process is governed, planned, resources, evaluated, monitored, controlled and reviewed <p>Level 3 - Defined</p> <ul style="list-style-type: none"> - Represents a managed process that is tailored from the organizations set of standard process's - Process management is proactive not reactive
					New Content		Add the NIST NICE Cybersecurity Workforce Framework as a reference for ID.AM-6:	

							<p>We are vulnerable because we deploy vulnerable systems, Systems security Engineering best practices should be included so that organizations deploy new capabilities with the following philosophies:</p> <ul style="list-style-type: none"> • Privacy by Design • Security baked in rather than bolted on • Secure Application Development <p>At a minimum a SSE/Deploy a secure system control should be added to augment the current generic SDLC control</p>	<p>Reference could include</p> <ol style="list-style-type: none"> 1.The Information Assurance Technical Framework 2.Systems Security Engineering Capability Maturity Model 3.MIL-HDBK-1785 SSE Program Management Requirements (Dated but Valid) 4.Trusted Computing Group Standards 5. OWASP Secure Web Application Framework
--	--	--	--	--	--	--	--	---

New
19 Content

						<p>Within the Asset Management (AM) a specific Data and Information Governance control should exist. More and more it is being more commonly accepted that we need just as much effort placed into the “Protect the Data” rather than just the endpoints. This is a rather large challenge if you don’t know what data is being used where, by whom, for what purpose and for what value. If an organization does not promote data & information governance then they are forced to protect everything at a higher cost both in cash as well as increased liabilities. Gartner has a well written definition : information governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.</p> <p>The best way to protect data is to get rid of it and you can’t do that unless the organization knows the answers to the above definition. Lastly having robust Data & information Governance helps organizations better understand “What Normal Looks Like” a core principle for continuous monitoring</p>	5
					New 13 Content		

					New 21 Content	<p>Within the Maintenance (MA) control family, a sustainability and supportability control should be included. This control need to ensure that systems in operation are operating vendor supported applications and that “Tech Refresh” planning is conducted based on vendor life cycle milestones for their given products. Additionally it should be called out that an third party service providers i.e. cloud providers, outsourced developers etc have sustainability and supportability outlined within their service agreements. (also maps to supply chain risk)</p>	
					New 24 Content	<p>RS.PL-1 As breaches move through litigation there is a continuing need to have both an Incident Response Plan and a Breach Response Plan, with the Incident Response plan being more technical in nature generally used by IT Departments and a Breach Response Plan being a plan drafted for the organization as a whole and generally contains pre-planning activities such as data minimization, Data loss prevention and establishing vendor and law enforcement relationships. The Online Trust Alliance provides a superb guide</p>	

							<p>Impact & Priority Codes that are also cumulative in nature should be added to the framework controls to assist in helping organizations define their own roadmap since may organizations are in different states of cyber security posture. For example you can't realistically conduct a risk assessment until you understand your operating environment which alludes to an organization needing to complete certain Asset management control first. Therefore those supporting controls should be assigned a high priority code because there is a dependency on the information it produces. Secondly impact codes should also be used based on the level of Resilience that the control produces when implemented. This would be a much simpler model to give consumers of the frameworks some bread and butter guidance that is easier to digest then what the DOD has done in the past with mission assurance category (MAC) and confidentiality level (CL) codes or NIST's CIA Control Overlays. The more Bread & Butter" the framework is the more organizations are likely to adopt it, as well as how best to answer the questions of "How do I get there from Here?" and "what does "Good" look like?"</p> <p>An example may look like:</p>
						New Content	

							<p>Priority High; Resiliency High</p> <ol style="list-style-type: none">1. ID.AM-12. ID.AM-23. ID.AM-34. ID.AM-45. ID.AM-56. RS.AN-1 <p>Priority High; Resiliency Medium</p> <ol style="list-style-type: none">1. ID.RA-12. ID.RA-33. ID.RA-44. ID.RA-55. PR.IP-96. PR.PT-3 <p>And so on... the goal is to make it easy to digest and when in organization is in doubt, run down the list and execute.</p>	

Comments template for Preliminary
Cybersecurity Framework

Submitted by: _____

Date: _____

Comments template for Preliminary
Cybersecurity Framework

Submitted by: _____

Date: _____



Comments template for Preliminary
Cybersecurity Framework

Submitted by: _____

Date: _____



Comments template for Preliminary
Cybersecurity Framework

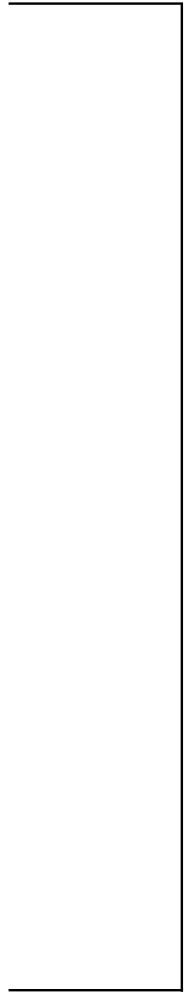
Submitted by: _____

Date: _____

Comments template for Preliminary
Cybersecurity Framework

Submitted by: _____

Date: _____

A large, empty rectangular box with a thin black border, intended for entering comments. It is positioned on the left side of the page, below the title.

Comments template for Preliminary
Cybersecurity Framework

Submitted by: _____

Date: _____

