May 2023, Stockholm

TRUESEC

Suggestions for NIST Cybersecurity Framework 2.0

Truesec response

1. Background

We who work with CSF here at Truesec appreciate NIST's efforts to improve the Cyber Security Framework (CSF) to better reflect the cyber security landscape's rapid threat changes.

Truesec is a cyber security company that deals with a lot of incidents and works full-time helping our customers with improving its cyber security posture and complying with statutory requirements. CSF has been a valuable resource for our customers, and we are pleased to have the opportunity to offer our insights and recommendations to further improve the framework.

As Cybersecurity Strategists at Truesec we regularly perform what we call a Holistic Cybersecurity Assessment, which is based on the NIST CSF 2.0 framework. This means we have put the controls in the CSF 2.0 in front of a variety of customers of different sizes and lines of business.

We favor a broader definition of supply chain resilience that looks beyond technical cyber risk and takes a broader approach to understanding what is needed to ensure continuity of service and operational continuity against non-technical risks such as administration, management, transfer of ownership, service degradation and concentration risk.

We have applied to the regulatory authorities' consideration of operational resilience the concept of 'Resilience by Design', assumes supplier failure by default and takes a two-pronged approach to mitigation associated risks which include, preventing supply chain failures (through cyber resilience solutions); and a reduction in the risk and impact of supply chain failures.

2. Recommendations

We recommend that NIST expand the response and recover capabilities to include more granularity

incident management and recovery planning guidance. We see that many organizations are facing an increasing number of cyber-attacks and must be prepared to respond and recover effectively. It would be great if NIST could support with more detailed guidance on incident response and recovery planning, it would really help organizations improve their cyber security resilience.

Another possibility for improvement would be to reassign some of the CSF subcategories to different function areas. Make sure that all subcategories from the protection categories are included within the recovery function.

This would allow for more accurate characterization of the organization's capacity and maturity, as well as reducing the risk of abuse of subcategory scores in risk measurements. The above considerations regarding risk measurements are particularly important because of the potential for incorrect reporting and decision-making.

Because practitioners usually equate the Protect function with "prevention" it is common for organizations to include PR scores as factors in estimation probability of loss event.

3. Regulations and other frameworks

Truesec recommends that NIST provide more detailed guidance on how CSF 2.0 can be integrated with other cybersecurity standards and frameworks, e.g., ISO 27001, IEC 62443, NIST SP 800-171 and Cloud Security Alliance CMM.

Many organizations must adhere to multiple frameworks and standards for cybersecurity and being able to offer extended guidance on how to implement CSF 2.0 alongside standards and the other frameworks really helps reduce the overall cost and effort required to comply.

Truesec recommends that NIST adapt CSF 2.0 to the EU's General Data Protection Regulation (GDPR) and the EU's NIS 2 directive and provide more.

Aligning CSF 2.0 with other standards and frameworks will help promote global cybersecurity best practices and facilitate compliance with multiple regulatory requirements using a common cybersecurity framework.

Truesec also suggests that NIST should develop more detailed guidance on how to measure the effectiveness of using CSF 2.0. Organizations must understand the effectiveness of their cyber security program and be able to track progress made over time. It would provide more guidance on how to measure the effectiveness of cybersecurity programs and help organizations identify areas of improvement and optimize their cyber security resources.

4. Feedback on the current concept paper

SECTION	TEXT	FEEDBACK
GV		We agree with breaking this out as its own category.
GV.OC	The organization's risk context, including mission, mission priorities, stakeholders, objectives, and direction, is understood (formerly ID.BE)	We feel like the focus here is too much on Cybersecurity Risk Management. A lot of smaller organizations do not have a formalized risk process, but they may still perform measures according to the controls in this sub-category.
GV.OC-01	Organizational mission is understood in order to prioritize cybersecurity risk management (formerly ID.BE-2 and ID.BE-3)	We would prefer a focus on alignment between IT and the rest of the organization rather than having this control be about IT understanding the organizational mission.
GV.OC-04	Critical objectives, capabilities, and services that stakeholders expect are determined and communicated (formerly ID.BE-4 and ID.BE-5)	Together we need to clarify how this control is different from GV.OC-01.

GV.RM-07, GV.RM-08	Risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks. Effectiveness and adequacy of cybersecurity risk management strategy and results are assessed and reviewed by organizational leaders	This is the first example of controls which we feel shouldn't be controls in themselves but should be part of a maturity ladder for the associated controls (Risk Management, in this case). Surely the performance of *all* controls should be "reviewed and adjusted" and have their "effectiveness and adequacy ... assessed and reviewed"? This is our major complaint about version 1.1 of the NIST CSF: Some of what are referred to as controls are actually measures of maturity rather than actual controls. In some cases there is a question of whether the process is documented, but not in all. In other cases there is a questions of whether the process is improved upon continually, but not in all.
GV.RR	Cybersecurity roles and responsibilities are coordinated and aligned with all internal and external stakeholders to enable accountability, performance assessment, and continuous improvement (formerly ID.GV-2)	This is another area which we feel come closer to measuring maturity than providing actual cybersecurity. We want to have roles and responsibilities identified for *all* controls, in our mind.
GV.RR-03	Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated (formerly ID.AM-6)	We think this belongs more in the area of Organizational Context rather than RR, which to me has a somewhat more limited scope.
GV.RR-07	Cybersecurity is included in human resources practices (e.g., training, deprovisioning, personnel screening) (formerly PR.IP-11)	It's unclear what is included in this control, outside of what is expressed in the PR.AT subcategory.
GV.PO-01	Policies, processes, and procedures for managing cybersecurity risks are	We feel like some organizations will stumble on the word "risk" here. We are talking about "risk management strategy", but I think we actually

	established based on organizational context, risk management strategy, and priorities and are communicated (formerly ID.GV-1)	mean “Cybersecurity strategy” here, where risk management is one component.
GV.PO-02	The same policies used internally are applied to suppliers	While we would love to be able to push our own policies and procedures onto all our suppliers, I just don’t see it being realistic. I agree supply chain security is critically important, but I would prefer to see an organization have a structured method and documented process with different levels of security requirements for suppliers based on the relationship, the number of technical integrations and a classification of the type of information that is exchanged.
ID.AM-01	Inventories of physical devices managed by the organization are maintained	Should we look for devices that are “managed by the organization” here, or those that are used to access the organization’s applications and information? In a BYOD scenario, for instance, we still want to have insight into a user’s devices.
ID.AM-03	Representations of the organization’s authorized network communication and network data flows are maintained (formerly ID.AM-3 and DE.AE1)	Good consolidation of controls from 1.1
ID.AM-04	Inventories of external assets and suppliers are maintained	We think we need to modernize the language in this control to make it clear that this includes IaaS, PaaS, SaaS and cloud services as well as Apps. Almost everything an organization does today is on some level an “external asset”, depending on how we define the term.
IT.AM-05	Assets are prioritized based on classification, criticality, resources, and organizational value	A lot of organizations we deal with get stuck on the word “prioritized” in this control. We would prefer it be worded something along the lines of “Assets are classified based on criticality and organizational value, and operational and security resources are allocated accordingly”.

ID.AM-07	Sensitive data and corresponding metadata are inventoried and tracked	We would like to see this control expanded to include Information Classification in general, as part of taking inventory of devices, software and services. This classification can then lead to specific measures for specific types of information and data.
ID.AM-08	Systems, devices, and software are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, transfers, end-of-life, and disposition (formerly PR.DS-3, PR.IP-2, PR.MA-1, and PR.MA-2)	A very important control, but we think it belongs in the PR category where it was previously. We are talking about specific protective actions here, not actions related to identification of assets.
ID.RA-03	Threats, both internal and external, are identified and recorded	How is this different from ID.RA-02 (“Cyber threat intelligence is received from information sharing forums and sources”)
ID.RA-04	Potential business impacts and likelihoods are identified and recorded	“impacts and likelihoods” of what? Vulnerabilities? Threats? Risks?
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated (formerly ID.RA-6 and RS.MI-3)	Very good, this needed to be expanded a bit. Any risk analysis is useless unless it results in actual responsive measures.
ID.RA-07	Changes are managed, assessed for risk impact, and recorded (formerly part of PR.IP-3)	This one looks like it doesn’t really belong in the ID.RM subcategory. Change Management is very important, and should maybe have its own subcategory under PR. Important to differentiate between types of changes such as software development, patch management, network configurations, application configurations and master data changes.
ID.RA-09	Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-5)	We feel like this could be coordinated with ID.RA-01

ID.RA-10	Exceptions to security measures are reviewed, tracked, and compensated for	Incomplete sentence
ID.SC-06	Supplier termination and transition processes include security considerations	A very good addition. A lot of people forget to think about what happens to their data after an agreement is over. This should be spelled out in the agreement itself.
ID.IM	Improvements to organizational cybersecurity risk management processes and activities are identified	As mentioned above, I feel like this is more a measure of maturity than an actual control. And, *all* work in cybersecurity should be continually improved.
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-6)	We get a lot of questions about what this control is asking for, and we feel it needs to be clarified. Are we making sure that access that is granted to the actual person the request was made for?
PR.AA-06	Account activities and access events are audited and monitored to enforce authorized access (formerly PR.AC-1 and PR.AC-3)	We think this needs to be clarified. “Account activities” can mean almost anything. I don’t think we want an organization to log everything. We also want to be careful to use the word “audited” by itself, as many would interpret this as being part of a formal IT Audit. “Logged” and “Reviewed” are useful synonyms, depending on the scenario. As a monitoring control, should this be a part of the DE category?
PR.AA-07	Physical access to assets is managed, monitored, and enforced (formerly PR.AC-2 and PR.PT-4)	We think we need to clarify that we mean “digital assets”, and even so we may want to clarify that we are referring to centralized assets such as servers and network equipment. We don’t think we want to “manage, monitor and enforce” access to client devices, for instance.

PR.DS-09	Data is managed throughout its life cycle, including discovery, maintenance, and destruction (formerly PR.IP-6)	Good clarification
PR.DS-10	The confidentiality, integrity, and availability of data-in-use is protected (formerly PR.DS-5)	Very good to include data-in-use in this subcategory.
PR.DS-11	Backups of data are conducted, protected, maintained, and tested (formerly PR.IP-4)	Should this be a part of the RC category? Backups themselves have no purpose besides enabling a recovery.
PR.PS-01	Configuration management practices are applied (e.g., least functionality, least privilege) (formerly PR.IP-1, PR.IP-3, PR.PT-2, and PR.PT-3)	To me “least privilege” is an access principle rather than a configuration management practice.
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	Glad to see verbiage about repair of equipment being removed.
PR.PS-04	Log records are generated for cybersecurity events and made available for continuous monitoring (formerly PR.PT-1)	We think this belongs in the DE category.
PR.PS-06	Backups of platform software are conducted, protected, maintained, and tested	Very similar to PR.DS-11. We feel like this also belongs in the RC category.
PR.PS-08	Supply chain security practices are integrated and their performance is monitored throughout the technology product and service life cycle	This is very similar to some of the ID.SC controls.
PR.IR-01	Response and recovery plans (e.g., incident response plan, business continuity plan, disaster	We feel like this belongs in the RS category.

	recovery plan, contingency plan) are communicated and maintained (formerly PR.IP-9)	
PR.IR-02	The organization's networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-3, PR.AC-5, PR.DS-7, and PR.PT-4)	The wording of this control is very general, and I feel like it overlaps many of the other controls (which have more specific language in them). The old PR.AC-5 was an important control in that it was one of the few places we could point to network segregation and segmentation. If this requirement still is part of this new control it's not obvious to me. Development security (such as addressed by the old PR.DS-7 control) needs to be a subcategory of its own in our mind.
DE.AE-05	Incident alert thresholds are established	It would be more clear if we continued using the term "Adverse Event" in this control (as we do in the preceding DE.AE controls).
DE.AE-08	Adverse cybersecurity events are categorized and potential incidents are escalated for triage	This sounds very similar to DE.AE-05. If it's different it needs to be clarified. It also may make more sense to consolidate with RS controls such as RS.MA-03.
DE.CM-01	Networks and network services are monitored to find adverse cybersecurity events (formerly DE.CM-1, DE.CM-4, DE.CM-5, and DE.CM-7)	Good consolidation of controls.
DE.CM-02	The physical environment is monitored to find adverse cybersecurity events	The way it's worded this is a bit contradictory. An adverse even in the physical environment could constitute a threat to the digital environment, but it's not necessarily a cybersecurity event. e.g. someone opening the door to the wiring closet.

DE.CM-03	Personnel activity and technology usage are monitored to find adverse cybersecurity events (formerly DE.CM-3 and DE.CM-7)	This is another control that confuses many customers (and consultants). Similar to DE.CM-02, I think it's possible to monitor personnel activity as a way to indicate a threat to the digital environment, but it's not necessarily an adverse cybersecurity event.
DE.CM-06	External service providers and the services they provide are monitored to find adverse cybersecurity events (formerly DE.CM-6 and DE.CM-7)	We should decide: Either supply chain security is its own subcategory and then it should be consolidated to ID.SC, or it needs to be part of every other subcategory.
RS-MA-01	The incident response plan is executed (formerly RS.RP-1)	An oddly worded control. The old language ("Response plan is executed during or after an incident") was better, in our eyes. Perhaps the control should make sure there is such a thing as an incident response plan, and that it's a documented process.
RS.MA-04	Incidents are escalated or elevated as needed (formerly RS.AN-2)	How is this different from DE.AE-08? In our mind this control falls under Incident Management, and logically belongs in the RS category.
RS.AN-03	Analysis is performed to determine what has taken place during an incident and the root cause of the incident	In our eyes this is two different functions: Determining "What has taken place" is an incident management function, while determining "the root cause" most frequently belongs in a problem management function.
RS.CO-05	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Most customers have a hard time figuring out what this means in reality.
RC	Restore assets and operations that were impacted by a cybersecurity incident.	We would expect to see more controls related to backups and DR to be part of this category.

RC.RP-01	The incident recovery plan is executed	“Incident Recovery Plan” is not something we talk about very often. Most customers won’t really know what this is. Is it the same thing as a DR Plan, or something else? Needs to be clarified.
RC.RP-02	Recovery actions are determined, scoped, prioritized, and performed	How is this different from the execution of the IR Plan mentioned in RC.RP-01?
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	Shouldn’t this integrity be tested continuously?

TRUESEC