From: Kim, David
To: cyberframework
Cc: [redacted]
Subject: Feedback - NIST Cybersecurity Framework 2.0
Date: Monday, November 6, 2023 10:15:29 PM
Attachments: image001.png

Hello NIST,

Thank you for the exciting opportunity to provide feedback. I focus on the Implementation Examples that relate to the NIST CSF 2.0 Public Draft.

Additional Implementation Examples for GV.RR-01 or GV.RR-02

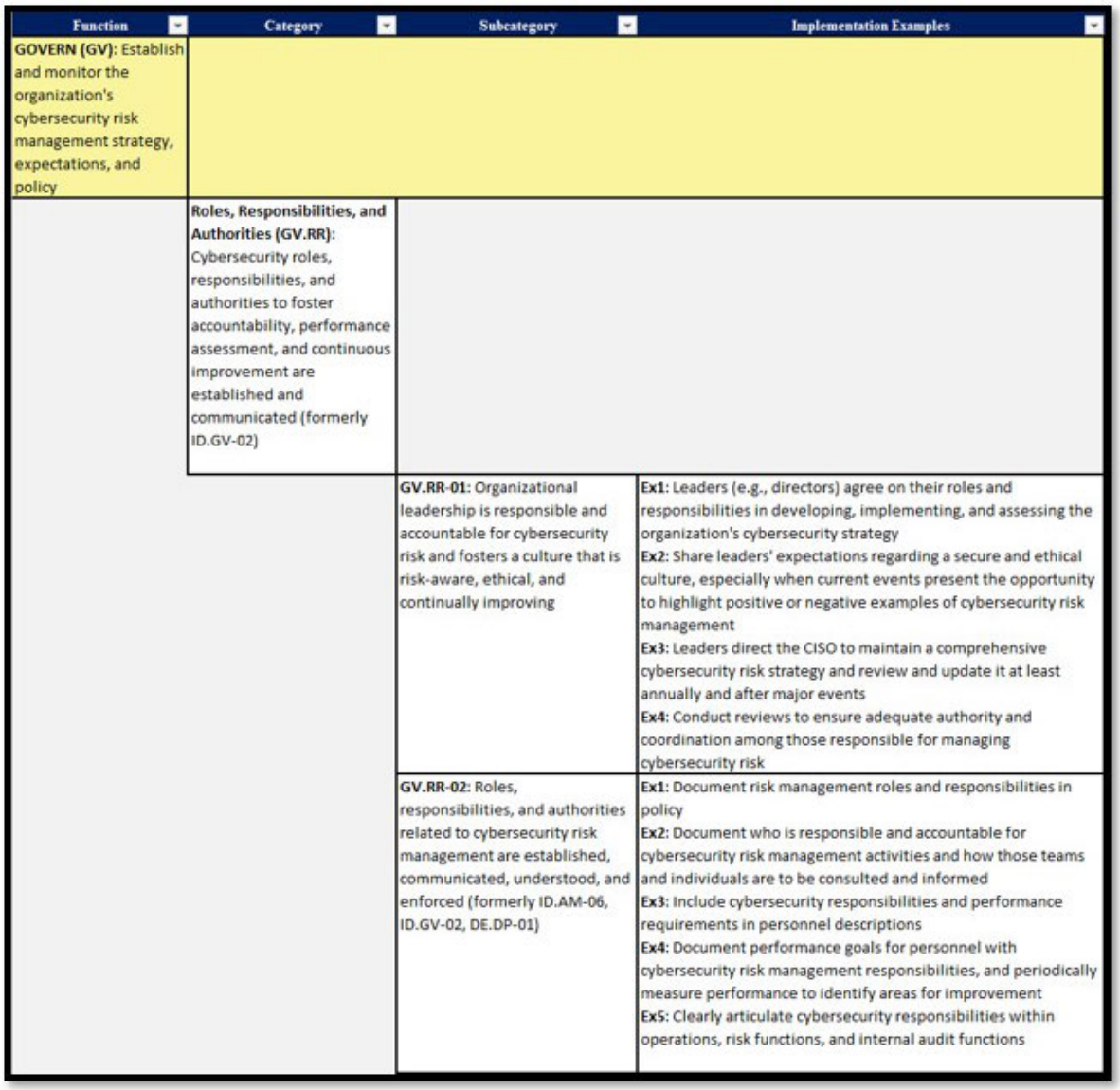
- Additional implementation example - **Ex:** Establish cybersecurity risk champions for each role (e.g. business analysts, Solution architects) employed by the organization. Empower role-specific champions to lead healthy discussions focused on cybersecurity risk management challenges & opportunities, that role practitioners are uniquely positioned to face & lead the organization through.

  Rationale

  There is a need to dispel the notion that only Leaders, Managers, or those with "Risk" or "Security" within the role title, are responsible & accountable for cybersecurity risk, its management, and its governance. All practitioners and roles within an organization have a part to play in the governance of information security. Aligns with the spirit of the NICE Workforce Framework for Cybersecurity.
- Additional implementation example - **Ex**: Setup an ethics hotline assuring anonymity for employees who want to raise a concern (concern as relevant to cybersecurity risk management) but may not feel comfortable doing so.

  Rationale

  An anonymity-assured ethics hotline is one way that an organization can proof its commitment to the strongest ethics.



Function	Category	Subcategory	Implementation Examples
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy			
	Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)		
		GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	**Ex1**: Leaders (e.g., directors) agree on their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy **Ex2**: Share leaders' expectations regarding a secure and ethical culture, especially when current events present the opportunity to highlight positive or negative examples of cybersecurity risk management **Ex3**: Leaders direct the CISO to maintain a comprehensive cybersecurity risk strategy and review and update it at least annually and after major events **Ex4**: Conduct reviews to ensure adequate authority and coordination among those responsible for managing cybersecurity risk
		GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01)	**Ex1**: Document risk management roles and responsibilities in policy **Ex2**: Document who is responsible and accountable for cybersecurity risk management activities and how those teams and individuals are to be consulted and informed **Ex3**: Include cybersecurity responsibilities and performance requirements in personnel descriptions **Ex4**: Document performance goals for personnel with cybersecurity risk management responsibilities, and periodically measure performance to identify areas for improvement **Ex5**: Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions

Comment about ID.RA-09

- Rephrasing of Ex4 within GV.SC-06, to capture the essence of ID.RA-09 and perhaps remove ID.RA-09 from Identify (ID) - **Ex4:** Determine a process to assess the authenticity and integrity of hardware and software prior to acquisition and use.

  Rationale

  ID.RA-09 may need to move to a different Function, away from Identify (ID). ID.RA-09 can move to GV.SC-06 as an additional implementation example. Implementation Example Ex4 within GV.SC-06, seems to capture what ID.RA-09 describes. Thus, this Ex4 may be re-phrased (Re: the rephrasing above), to capture the essence of ID.RA-09.

Function	Category	Subcategory	Implementation Examples
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization			
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to the organization, assets, and individuals.		
		ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)	**Ex1**: Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use

Function	Category	Subcategory	Implementation Examples
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy			
	Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)		
		GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Ex1**: Perform thorough due diligence on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship **Ex2**: Assess the suitability of the technology and cybersecurity capabilities and the risk management practices of prospective suppliers **Ex3**: Conduct supplier risk assessments against business and applicable cybersecurity requirements, including lower-tier suppliers and the supply chain for critical suppliers **Ex4**: Assess the authenticity, integrity, and security of critical products prior to acquisition and use

Kindest regards,
David

Youngjoo David Kim (he/him), BEng, CBAP, CISSP
Manager, Information Security Governance | Global Information Security Office
GREAT-WEST LIFECO INC.
canada life™ Irish Life EMPOWER Putnam INVESTMENTS

Visit greatwestlifeco.com