**From:** Brian Ledbetter
**Sent:** Friday, October 6, 2023 6:24 PM
**To:** cyberframework <cyberframework@nist.gov>
**Subject:** Feedback on NIST CSF 2.0 Public Draft

Hello!

This feedback is regarding the "Govern (GV)" function. I propose that CSF 2.0 includes an additional category under the Govern function entitled "Culture Management" that would be defined as "Systematic efforts to establish and maintain a strong and proactive cybersecurity culture among internal stakeholders—fostering a collective mindset, as well as behaviors that prioritize and support cybersecurity best practices."
A supporting Excel doc should be attached for review (2023.10.06 NIST CSF Amendment Proposition.xlsx) that includes subcategories and implementation examples. If you have any questions or concerns, please let me know! I've been a practitioner for several years, and believe culture management to be an important piece that all current cybersecurity frameworks fail to properly address.
--

**Brian Ledbetter**
**Guidepointsecurity.com**

| Category | Subcategory | Implementation Examples |
|---|---|---|
| | | |
| **Culture Management (GV.CM):** Systematic efforts to establish and maintain a strong and proactive cybersecurity culture among internal stakeholders—fostering a collective mindset, as well as behaviors that prioritize and support cybersecurity best practices | **GV.CM-01:** Internal stakeholders outside of the cybersecurity team feel like an extension of the cybersecurity team | **Ex1:** Marketing teams often collaborate closely with the cybersecurity team, ensuring that security messaging aligns with marketing campaigns. This synergy makes internal stakeholders outside of the cybersecurity team feel like an extension of the cybersecurity team<br>**Ex2:** The IT department frequently participates in security training sessions, fostering a strong bond with the cybersecurity team. This shared knowledge and commitment make IT professionals feel like they are an integral part of the cybersecurity team<br>**Ex3:** Legal and compliance teams work hand in hand with cybersecurity, ensuring all regulatory requirements are met. Their seamless cooperation makes these internal stakeholders feel like they are a natural extension of the cybersecurity team |
| | **GV.CM-02:** Members of the cybersecurity team can rely on each other | **Ex1:** Recent polling data indicates a strong sense of trust and camaraderie within the cybersecurity team, highlighting their ability to rely on one another for support and collaboration<br>**Ex2:** In a recent survey, it was evident that the cybersecurity team members have built a solid foundation of mutual trust, demonstrating their capacity to depend on one another in safeguarding digital assets<br>**Ex3:** Polling results reaffirmed the cybersecurity team's cohesion, showing they can count on their colleagues to work together effectively, helping to ensure online security remains robust |
| | **GV.CM-03:** Cybersecurity champions exist throughout the disparate functional areas of the organization | **Ex1:** It was discovered that Cybersecurity champions are scattered across various departments within the organization. They were discovered in IT, HR, finance, and even marketing<br>**Ex2:** The existence of cybersecurity champions was validated through an organization-wide poll that revealed employees have witnessed repeated championing of cybersecurity best practices by cybersecurity champions in their respective units |
| | **GV.CM-04:** Cybersecurity team members feel comfortable speaking up in meetings | **Ex1:** Cybersecurity team members feel confident and comfortable expressing their ideas during meetings, fostering a more collaborative work environment<br>**Ex2:** The cybersecurity team feels self-assured about voicing their opinions during meetings, promoting a transparent and productive exchange of ideas |
| | **GV.CM-05:** Members of the cybersecurity team feel empowered with autonomy to constantly innovate | **Ex1:** Cybersecurity team members are experiencing empowerment and are leveraging their autonomy to drive ongoing innovation within the organization |
| | **GV.CM-06:** Respect is felt by each cybersecurity team member | **Ex1:** It was discovered that every member of the cybersecurity team feels a deep sense of respect within the group, fostering a positive and collaborative work environment |
| | **GV.CM-07:** Honest and ethical behavior is regularly exemplified by members of the cybersecurity team | **Ex1:** Polling found that members of the cybersecurity team consistently demonstrate honest and ethical conduct, earning them high trust within the organization |
| | **GV.CM-08:** Every member of the cybersecurity team feels like they are part of a cohesive unit that collaborates on a regular basis to overcome challenges together | **Ex1:** Each member reported a strong sense of unity, with regular collaborative efforts to conquer challenges, fostering a resilient team spirit |
| | **GV.CM-09:** Cybersecurity Awareness Month is something all internal stakeholders look forward to | **Ex1:** It is evident that Cybersecurity Awareness Month is highly anticipated by all internal stakeholders. They eagerly embrace this opportunity to stay informed and proactive in safeguarding our digital infrastructure |
| | **GV.CM-10:** All members of the cybersecurity team feel valued | **Ex1:** Polling data showed unanimous satisfaction within the cybersecurity team, with all members expressing that they feel valued and appreciated in their roles |
| | **GV.CM-11:** The pursuit of excellence is sought by each member of the cybersecurity team | **Ex1:** The pursuit of excellence is a common trait shared by all members of the cybersecurity team |