

**From:** [Thomas Trappler](#)  
**To:** [cyberframework](#)  
**Subject:** NIST Draft CSF 2.0 Comment  
**Date:** Tuesday, August 29, 2023 8:36:49 PM

---

Dear NIST,

Kudos for your efforts to date in adding Cybersecurity Supply Chain Risk Management (GV.SC) to the CSF. Successful management of supply chain cybersecurity risk requires a solid partnership among IT/security, Procurement, legal, and other key organizational stakeholders. Procurement can often serve as a key checkpoint to ensure the organization has conducted appropriate review of third party services prior to acquisition, as well as ensuring contracts/agreements with third party services providers include provisions appropriate to address cybersecurity rights and responsibilities. For these reasons, I strongly recommend revising the draft to specifically identify Procurement as a function that contributes to cybersecurity supply chain risk management. There are multiple places where this role could be highlighted, but at a minimum propose that GV.SC-01, Ex 4 be revised to read:

"Establish a cross-organizational mechanism that ensures alignment between functions that contribute to cybersecurity supply chain risk management, such as cybersecurity, IT, procurement, legal, human resources, and engineering"

Thank you for your time and consideration.

Kindest regards,  
Thomas Trappler