

Category Identifier	Feedback
GV	We recommend including subcategories pertaining to quantifying value of cybersecurity risks and investments, to support greater alignment to strategic objectives
GV.RM-03	While we agree with the generalization beyond critical infrastructure to encompass overall business environment, we recommend the mention of sector specific risk analysis be retained.
GV.RM-06	We recommend including language to include budget to ensure proper program funding/sustainment
GV.RR-01	We recommend including language to articulate what constitutes a baseline ethical standard, such as company values
ID.AM-07	We recommend including language indicating how an organization will categorize data as sensitive
ID.IM	The Improvement category could benefit from subcategories pertaining to establishment of a feedback loop for monitoring the business case / intended outcomes of security investments
ID.SC	While this section is thorough in how the organization can identify supplier risks through evaluation, we recommend including language to outline how suppliers would self-report risks to the organization
PR.AT	The subcategories currently bucket Awareness and Training as one function. Organizations may benefit from inclusion of subcategories more specific to awareness / culture campaigns.
RC.RP	We recommend including language to collect and implement lessons learned following each response