Category	Subcategory	Implementation Examples for Academia (PreK-12)	Input to NIST for CSF 2.0
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization’s cybersecurity risk management decisions are understood (formerly ID.BE)	GV.OC-06: The deliberations and decisions of organizational leaders reflect an understanding of data privacy and cybersecurity and the policies and regulations set clear expectations for the protection of stakeholder data privacy and security, as well as the transparent use of data.	Agendas and/or minutes from leadership meetings demonstrating that groups such as an organizatonal governing board or other leadership groups regularly engage in thoughtful discussions about oganizational compliance with federal, state laws and local norms, and consider organizational policies and practices related to ensuring that rigorous stakeholder data privacy and security measures are in place. Organizational policies and/or regulations explaining procedures employees are to follow to ensure the privacy and security of stakeholder data, and how the organization communicates to the community the purposes for which it collects and maintains stakeholder data.	Recommend adding a subcategory GV.OC-06
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.GV02)	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: Title(s) and job description(s) of individual(s) responsible for development and implementation of both privacy and security policies and practices, along with an organizational chart demonstrating that the role(s) sit at the executive level for the organization.	Add Example 3
Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01)	GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced (formerly ID.GV-01)	Ex1: Create, disseminate, and maintain a risk management policy with statements of management intent, expectations, and direction Ex2: Periodically review policies and procedures to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy Ex3: Require approval from senior management on policies Ex4: Communicate cybersecurity risk management policies, procedures, and processes across the organization Ex5: Require personnel to acknowledge receipt of policies when first hired, annually, and whenever a policy is updated Ex6: Leaders provide transparent, updated and accessible communications regarding the collection, management and use of community and stakeholder data, such as newsletters, website pages, or other materials intended for the community that explain how the organization collects, manages and utilizes its data.	Add Example 6