NIST Cybersecurity Framework 2.0
Reveal Risk's Feedback
May 2023

GV.RM-05: "Strategic direction describing appropriate risk response options, including cybersecurity risk transfer mechanisms (e.g., insurance, outsourcing), investment in mitigations, and risk acceptance is established and communicated"

This control would be stronger and more informative if it would describe example risk response/treatment options vs calling out "risk transfer mechanisms" and mentioning insurance and outsourcing but no broader examples. We would recommend either sharing examples of each risk treatment option or not sharing examples at all. These 2 examples are often misunderstood as to the context of how much of the risk is truly transferred; so highlighting them as the only examples probably does more harm than it helps.

GV.RM-04: Cybersecurity risk management is considered part of enterprise risk management (formerly ID.GV-4)

Consider updating the control to allow for situations where the ERM function is not established within an organization. "…, where ERM is established and operational." While not ideal, the cyber risk function can and should be created and matured regardless of the condition of the broader ERM function. The ultimate goal should be as currently stated in the control.

Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions (formerly ID.RM)

In GV.RM, there are references to both "cybersecurity risk management" and "risk management." "Cybersecurity risk management" is descriptive and sets the scope for the reader, but the "risk management" term is broad, and a reader could interpret it as extending beyond cyber. Is this the intent of the controls that only reference "risk management," or should the reader still assume the scope is cyber risk? Consider updating the language for clarity.

GV.OC, GV.RM, GV.RR, GV.PO

Consider updating the order of these categories to keep the governance first (GV.OC), then the roles and responsibilities (GV.RR), then Policies and Procedures (GV.PO), followed by Risk Management (GV.RM). Defining how a program is governed first is important to set the stage. Explaining R&Rs next allows the reader to understand how the governance is managed and executed and by whom. Having the policy and procedure concepts next explains to the reader

how the governance and R&Rs will be enforced and operated. And finally, the risk management section tells the reader what the program will do.

GV.PO-02: The same policies used internally are applied to suppliers

There may be situations where internal policies may or should not apply to suppliers. Consider updating the language to something like, “Assess internal policies to determine applicability to suppliers and apply policies based on assessment outcomes.” Also, consider including “third-party partners” in this control to match the terms and scope in ID.SC.

PR.AT-01: Awareness and training are provided for users so they possess the knowledge and skills to perform relevant tasks

Consider including the need for the cyber organization to train on requirements in addition to enabling knowledge and skills. In some cases, employee understanding of requirements on how to conduct work in a secure manner is as important as improving knowledge and skills. One could argue that enabling knowledge meets the goal of communicating requirements, but stating it simply may help define the intent of the control.

RS.MA-01: The incident response plan is executed

This control requires the execution of the response plan, but the framework does not define a requirement to create a response plan. Consider including additional language in RS.MA-01 to also include the development and maintenance of a plan.

RC.RP-01: The incident recovery plan is executed

This control requires the execution of the recovery plan, but the framework does not define a requirement to create a recovery plan. Consider including additional language in RC.RP-01 to also include the development and maintenance of a plan.