



November 6, 2023

National Institute of Standards and Technology

Re: Request for Comment on NIST CSWP 29 (Initial Public Draft) *The NIST Cybersecurity Framework 2.0*

To whom it may concern:

The American Institute of CPAs (AICPA) and Committee of Sponsoring Organizations (COSO) are pleased to provide a combined response to the National Institute of Standards and Technology's (NIST) request for comment on the public draft of *the NIST Cybersecurity Framework 2.0* (NIST CSF draft revision). We appreciate the opportunity to help inform NIST's efforts to address current and future cybersecurity challenges and to align with leading practices.

One of the current struggles that organizations face is the implementation of cybersecurity risk management that is responsive to an organization's mission and its objectives. We have drafted this letter to provide comments regarding the NIST CSF draft revision along with its alignment with organization-wide efforts to achieve organizational objectives, including those based on the COSO *Internal Control - Integrated Framework* (COSO Framework). The COSO Framework is a leading internal control framework widely used by both public and nonpublic organizations to integrate internal controls into business processes. We recommend highlighting alignment with the COSO Framework to aid in the implementation of the NIST CSF by any organizations that already use the COSO Framework. In addition, we have specifically addressed your request for feedback on the types of Examples that would be most beneficial to Framework users.

Originally formed in 1985, COSO is a joint initiative of five private-sector organizations (including the AICPA) and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. The COSO Internal Control Framework is a globally recognized framework which enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization.

The AICPA is the world's largest member association representing the CPA profession, with more than 431,000 members in the United States and worldwide, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting. The AICPA sets ethical standards for its members and U.S. auditing standards for private companies, not-for-profit organizations, and federal, state and local governments. It develops and grades the Uniform CPA Examination, offers specialized credentials, builds the pipeline of future talent, and drives professional competency development to advance the vitality, and quality of the profession.

The AICPA is a member of COSO and serves on COSO's Board of Directors. CPAs are well versed in COSO and cybersecurity risk management and regularly evaluate the effectiveness of internal controls based on the COSO framework, providing insight into how the framework is used by various organizations.

Making Reference to COSO

We believe that a specific reference to the alignment of the NIST CSF with the COSO framework will aid in the implementation of the NIST CSF for the many organizations, both public and nonpublic, that already use the COSO framework to design, implement, monitor and assess the effectiveness of their internal control.

The COSO framework is a leading framework for evaluating the effectiveness of control and is used by most U.S. public companies as well as many non-public companies and their auditors to effectively and efficiently develop and evaluate systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization. The vast majority of U.S. public company reports on internal control over financial reporting filed under Section 404 of the Sarbanes-Oxley Act of 2002 use the COSO framework for evaluation of the effectiveness of internal control over financial reporting. As such, a clear alignment between COSO and the NIST CSF could broaden the adoption of the NIST CSF by various public companies.

In response to the request for comment, we evaluated the NIST CSF draft revisions against COSO and determined that the NIST CSF would be useful for organizations that use COSO for designing controls to address organizational risks. The COSO framework recognizes that internal control is not a serial process, but rather a dynamic and integrated process. Similar to how the NIST CSF draft revision has emphasized governance through the creation of a new function that sits in the center of its CSF Functions wheel, the COSO framework identifies Control Environment, Risk Assessment, Information and Communication, and Monitoring as four of the five integrated components that should be present and working together for an effective system of internal control. The NIST CSF functions of Identify, Protect, Detect, Respond and Recover are similar to the COSO component of Control Activities which include actions to mitigate risks and achieve the entity's objectives. Appendix A shows these relationships in more detail.

We commend NIST's recognition of the importance of governance and risk management strategy as a separate overarching "Govern" function. The COSO Framework recognizes that an organization which establishes and maintains a strong control environment positions itself to be more resilient in the face of internal and external pressures. Equally important is an effective risk management process – from establishing objectives to identifying and assessing risks, risk assessment forms the basis for how risks will be managed. These concepts have been captured in NIST's new "Govern" function.

The Importance of Integrating of Cybersecurity Risk Management with Other Risk Management Domains

Alignment of cybersecurity risk management to the organization's efforts to achieve its mission and objectives through its system of internal control¹ can be difficult due to different frames of reference,

¹ The terms *risk management* and a *system of internal control* both refer to an organization's processes for mitigating the risks that threaten the achievement of its mission and objectives. They are primarily distinguished

lack of understanding, and communication challenges. Overcoming these difficulties is critical because organizations that fail to align these efforts are at serious risk of being unable to meet their operational, compliance, and reporting objectives, to the detriment of both their short-term and long-term mission and, for commercial enterprises, value creation potential.

Increasingly, organizations fail to achieve their mission and business objectives due to the realization of a business threat through an IT system or process vulnerability, or through a component of IT systems. In fact, many business threats are cybersecurity threats and cybersecurity threats are business threats. Consequently, the close integration and alignment of cybersecurity risk management with other organizational risk management efforts is essential for effective risk management at the organizational level.

The NIST CSF “provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them.”² and the CSF then lays out a framework to explicitly manage those risks. The NIST CSF draft revision has laid the groundwork by encouraging users to consider both cybersecurity and other organizational risks in Section 4 which discusses integration of all risk management efforts at a high level by using enterprise risk management (ERM). ERM includes risks such as financial, legal, operational, physical security, reputational, safety and privacy in addition to cybersecurity risks. The section also references the use of *NIST IR 8286 Integrating Cybersecurity and Enterprise Risk Management* to enable risk practitioners to integrate cybersecurity risk management activities more fully into the broader enterprise risk processes.

We believe that additional guidance on integration of these efforts is necessary for the CSF to be fully effective. We recommend that NIST continue to build out guidance in this area. For example, *GV.RM-03: Enterprise risk management processes include cybersecurity risk management activities and outcomes* would benefit from examples that link business objective threats to cybersecurity threats:

Ex#: Use operational, compliance, reporting and other business threats identified through enterprise risk assessment to inform the identification and evaluation of cybersecurity threats.

Additional Recommendations for Development of Examples

NIST has also sought input on what other types of Examples would be most beneficial to Framework users. We have the following comments:

from each other in that they start from different frames of reference. *Risk management*, as defined by OMB circular A-130, is the program and supporting processes to manage risk to the agency’s operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time. The focus is managing risk, which includes processes. A *system of internal control*, as defined by COSO, is processes, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. It’s frame of reference focuses on achievement of the organization’s objectives whereas risk management focuses on the risks to those objectives.

² National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. **74-76**. <https://doi.org/10.6028/NIST.CSWP.29.ipd>

- In reviewing subcategory ID.IM-02: *Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements*, it is not clear whether the guidance relates to both business continuity and disaster recovery tests and exercises when referring to security tests and exercises. We recommend that Implementation Example Ex1 be updated to clarify the guidance related to business continuity.

Ex1: Identify improvements for future incident response activities based on findings from **security, business continuity and disaster recovery** incident response assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits)

- ID.RA-01: *Vulnerabilities in assets are identified, validated, and recorded* focuses on the identification related to information technology related assets and facilities. However, vulnerabilities may also exist in manual processes and human behavior that may be exploited by cybersecurity threat actors. While we do not believe that a separate category needs to be developed, we believe that ID.RA-04: *Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded* would benefit from an example that addresses such vulnerabilities.

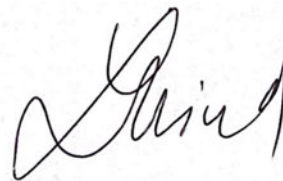
Ex#: Vulnerabilities in manual processes and in human behaviors are considered in evaluating the potential impacts and likelihoods of threats exploiting vulnerabilities and such risks are identified, validated, and recorded.

We appreciate the opportunity to comment and look forward to future engagement. If you have any questions, please don't hesitate to contact Carrie Kostelec, the AICPA's Lead Manager for SOC and Related Services, at [REDACTED]

Respectfully,



Susan S. Coffey, CPA, CGMA
Chief Executive Officer – Public Accounting



Lucia M. Wind
COSO Board Chair

Appendix

The following table further demonstrates the alignment between the Functions identified in the NIST CSF draft revision and the Components identified in the COSO Framework.

| NIST Functions | COSO Components ³ |
|--|---|
| <p>GOVERN – <i>Establish and monitor the organization’s cybersecurity risk management strategy, expectations, and policy.</i></p> <p>GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.</p> | <p>CONTROL ENVIRONMENT - <i>The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.</i> The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.</p> <p>RISK ASSESSMENT - <i>Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.</i> Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.</p> <p>INFORMATION AND COMMUNICATION - <i>Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives.</i> Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control.</p> |

³ 2013 Internal Control–Integrated Framework

| | |
|---|--|
| | <p><i>Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.</i></p> <p>MONITORING ACTIVITIES - <i>Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.</i></p> |
| <p>IDENTIFY – <i>Help determine the current cybersecurity risk to the organization.</i></p> <p>PROTECT – <i>Use safeguards to prevent or reduce cybersecurity risk.</i></p> <p>DETECT – <i>Find and analyze possible cybersecurity attacks and compromise.</i></p> <p>RESPOND – <i>Take action regarding a detected cybersecurity incident.</i></p> | <p>INFORMATION AND COMMUNICATION - <i>The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.</i></p> <p>CONTROL ACTIVITIES - <i>Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology</i></p> |

| | |
|--|---|
| <p>RECOVER – <i>Restore assets and operations that were impacted by a cybersecurity incident.</i></p> | <p>environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.</p> |
|--|---|