Fall

NONPROFIT NEWSLETTER

CONTENTS

baldwin CPAs

Implementing FASB ASU on Contributed Nonfinancial Assets

By Matt Cromwell

In September 2020, the Financial Accounting Standards Board issued Accounting Standards Update (ASU) 2020-07 Not-For-Profit Entities (Topic 958): Presentation and Disclosures by Not-For-Profit Entities for Contributed Nonfinancial Assets. The intent of ASU 2020-07 is to provide enhanced transparency related to the presentation and disclosure of contributed nonfinancial assets. These enhancements will allow a clearer understanding of both the volume and type of nonfinancial assets that are received and recognized by an entity. Additionally, the ASU provides improved transparency into "cash versus non-cash" contributions and the impact on an organization's operations. ASU 2020-07 does not change the historical valuation methodology used by the organization nor "how" that asset is recorded within the financial statements (only the "where").

Adoption is required for annual reporting periods beginning after June 15, 2021. Thus, the ASU is effective for the June 30, 2022 year-ends and later. The ASU must be applied on a retrospective basis and comparative presentation is required if the organization presents comparative financial statements. Additionally, the transition disclosure requirements must include the nature and reason for the change as well as how the adoption of the ASU was applied.

Let's take a step back however and determine what constitutes a nonfinancial asset.

Whatever was recorded previously as nonfinancial assets is now subject to the requirements of ASU 2020-07. This includes, but is not limited to, the receipt of donations of the following nonfinancial assets:

- Legal Services
- Accounting Services
- IT Services
- Pharmaceuticals
- Commodities
- Raffle Items
- Space
- Personal Protective Equipment
- Radio, Social Media and Television (Streaming) Advertising (PSAs)
- Travel (Airline Tickets, Hotel Nights, etc.)

So at this point you are asking yourself, then what really changes upon adoption of ASU 2020 07?

For most entities, there will be significant revisions to both the presentation and disclosure of nonfinancial assets. The overview below summarizes key changes for both of these areas.

Presentation

ASU 2020-07 now requires that nonfinancial assets be segregated from financial assets within all financial statements (statement of activities, statement of functional expenses, etc.). ASU 2020-07 does not mandate the disaggregated level that is required in the financial statements; however, in practice, many organizations are leaning toward multiple levels of disaggregation to ensure transparency considerations are adequately considered. For example, prior to adoption of ASU 2020-07, an organization may have presented a single line for contributions. Upon adoption of ASU 2020-07, at a minimum, the presentation would show a disaggregation into two lines labeled "contributions – financial assets" and "contributions – nonfinancial assets." Many organizations are further disaggregating their nonfinancial asset contributions into such line items as: "contributions — donated services," "contributions — donated equipment," "contributions - donated materials/commodities," etc. as these presentations will more fully align to the required footnote presentation discussed below.

ASU 2020-07 now requires that nonfinancial assets be segregated from financial assets within all financial statements (statement of activities, statement of functional expenses, etc.).

Disclosure

ASU 2020-07 requires significant enhanced disclosure(s) regarding nonfinancial assets. All of the following must be addressed by category of nonfinancial assets (see earlier discussion of consideration of groupings):

- The organization must disclose its policy on liquidating instead of using the donated nonfinancial asset(s) within the significant accounting policies (and, if the organization doesn't currently have a policy, one needs to be developed).
- Qualitative considerations on whether the contributed nonfinancial assets were liquidated or used during the reporting period.
- If the nonfinancial assets were used, a description of how the asset was utilized by the organization is required (i.e., detail of which program or supporting service utilized the nonfinancial assets).
- If there were any donor-imposed restrictions related to how the contributed nonfinancial assets were utilized.
- Valuation techniques utilized in assessing the value of the nonfinancial asset.

Example disclosure: The below example presents a general disclosure in a tabular format for an organization with multiple types of donated nonfinancial assets.

Financial Statement Disaggregation	Revenue Recognized	Utilization in Programs/Activities	Donor Restrictions	Valuation Techniques/Inputs
Contributions – Nonfinancial Assets	$6,000,000	Management & General	No Donor Restrictions	Estimated fair-market value based on legal invoices received to support time spent on organizational matters
Contributions – Nonfinancial Assets	$7,015,692	*IT in Schools* Program	No Donor Restrictions	Estimated value of specialty services provided for IT and cloud-computing system development.
Donated Medical Equipment	$18,502,402	*Health and Wellness* Program	Restricted for Use in Africa	Estimated value of like equipment based on open market comparative modeling considering contractual restrictions on distribution to very limited locations.
Contributed Radio, Digital and Other Media	$26,282,108	*Save a Life* Program	No Donor Restrictions	Value provided by entities that place media with television, radio and social media platforms. Values are based on time of airing, length of airing and/or website "hits" based on readily determinable values in the media space.

Implementation considerations

To date, the most important factor in successfully addressing ASU 2020-07 implementation has been ensuring a full inventory of donated nonfinancial services is available by taking a survey of the various departments of the organization. In addition, revisiting fiscal year 2021 to ensure the comparative presentation and disclosure requirements are addressed.

Many organizations feel the tabular option allows the reader of the financial statements easier access to disclosures supporting the presentation of nonfinancial assets in their financial statements.

Furthermore, most entities are enhancing their internal policies to succinctly address the use of nonfinancial assets and "intent" from the donor regarding donated nonfinancial assets. Finally, organizations' managements are finding the use of the tabular disclosure presentation, versus a solely narrative disclosure, provides a more transparent and informative presentation option. Many organizations feel the tabular option allows the reader of the financial statements easier access to disclosures supporting the presentation of nonfinancial assets in their financial statements.

• • • •

Written by Matt Cromwell.
www.bdo.com

GASB Statement No. 100, Accounting Changes and Error Corrections

By Sam Thompson

On June 13, 2022, the Governmental Accounting Standards Board (GASB) achieved a major milestone in issuing its 100th accounting statement, GASB Statement No. 100, Accounting Changes and Error Corrections (GASBS 100 or "Statement"). The Statement establishes accounting and financial reporting requirements for (a) accounting changes and (b) the correction of an error in previously issued financial statements (also referred to simply as "error correction"). The Statement supersedes guidance found in GASB Statement No. 62, Codification of Accounting and Financial Reporting Guidance Contained in Pre-November 30, 1989 FASB and AICPA Pronouncements (GASBS 62).

Background

Financial reporting requirements for accounting changes and error corrections were originally based on guidance issued in the 1970s. In 2010, the GASB issued GASBS 62, which became the primary guidance for accounting and financial reporting of prior-period adjustments, accounting changes and error corrections. In August 2018, the GASB added to its technical plan a project to reexamine the effectiveness of GASBS 62 related to prior-period adjustments, accounting changes and error corrections. Research performed by the GASB identified certain issues regarding the understanding and application of the requirements of GASBS 62, as well as information not previously required that financial statement users found valuable concerning accounting changes and error corrections. This article presents a summary of the updates included in GASBS 100.

Accounting Changes

GASBS 100 outlines three types of accounting changes: changes in accounting principles, changes in accounting estimates and changes to, or within, the financial reporting entity.

A change in accounting principle results from either (a) a change from one generally accepted accounting principle (GAAP) to another due to the newly adopted GAAP being preferable, or (b) the implementation of a new accounting or financial reporting pronouncement. A change in accounting principle under GASBS 100 does not include the initial adoption and application of an accounting principle to transactions or other events that are clearly different in substance from those previously occurring, occurring for the first time or that were previously insignificant. Moreover, a change in the application of an accounting principle that is not generally accepted under GAAP is considered an error correction, not a change in accounting principle.

A change in accounting estimate occurs when the inputs (e.g., data, assumptions, measurement methodology) used for the estimate change. Changes can occur due to changes in circumstance, information or experience. A change in accounting estimate due to a change in measurement methodology should be based on the new measurement methodology being preferable or a change required due to a GASB pronouncement. In determining whether a change in measurement methodology is preferable, only the qualitative characteristics of financial reporting should be assessed.

Changes to or within the financial reporting entity can occur due to:

- The addition or removal of a fund resulting from the movement of continuing operations within the primary government
- A change in a fund's presentation as major or nonmajor
- A change in a component unit's presentation as blended or discretely presented
- The addition or removal of a component unit for reasons besides the acquisition, merger or transfer of operations that result in the addition or removal of a discretely presented component unit under GASB Statement No. 69, Government Combinations and Disposals of Government Operations, or the reporting of a component unit pursuant to GASB Statement No. 90, Majority Equity Interests.

Changes in accounting principle (absent other specific requirements addressing the circumstance) should be reported retroactively in single period financial statements by restating beginning net position, fund balance or fund net position, as applicable, for the cumulative effect, if any, of the change to the newly adopted accounting principle on prior periods. Changes in accounting principle reported in comparative financial statements should include restating financial statements for all prior periods presented, if practicable.

In determining whether a change in measurement methodology is preferable, only the qualitative characteristics of financial reporting should be assessed.

Any cumulative effect of the change to the newly adopted accounting principle on prior periods not presented should be reported as a restatement to beginning net position, fund balance or fund net position, as applicable, for the earliest period presented. If restatement of all prior periods presented is not practicable, any cumulative effect should be reported as a restatement in the earliest period for which it is practicable.

Changes in accounting estimate (absent other specific requirements addressing the circumstance) should be reported prospectively by recognizing the change in accounting estimate in the reporting period in which the change occurs.

A change to or within the financial reporting entity should be reported by adjusting the current reporting period's beginning net position, fund balance or fund net position, as applicable, as if the change occurred as of the beginning of the reporting period.

The notes to the financial statements should disclose the nature of the accounting change, the reason for the change and the financial statement line items affected. A change in accounting principle should include disclosure in the notes identifying the new pronouncement and an explanation why the newly adopted accounting principle is preferable. For comparative financial statements, if prior periods presented are not restated because it is not practicable to do so, the reason why the restatement is not practicable should be disclosed. A change in accounting estimate resulting from a change in measurement methodology should be accompanied by a disclosure of the reason for the change and an explanation why the new measurement methodology is preferable.

Error Corrections

The application of GAAP to transactions or other events previously accounted for using accounting principles not generally accepted is considered an error correction.

Errors can occur due to mathematical mistakes, mistakes in the application of accounting principles, or oversight or misuse of facts that existed at the time the financial statements were issued about conditions that existed as of the financial statement date. A fact is considered to have existed at the time the financial statements were issued if the fact could reasonably be expected to have been obtained and taken into account at that time about the conditions that existed as of the financial statement date.

An error correction to single period financial statements should be reported retroactively by restating beginning net position, fund balance or fund net positions, as applicable, for the cumulative effect of the error correction on prior periods. An error correction reported in comparative financial statements should be reported retroactively by restating all prior periods presented. The cumulative effect of the error correction on earlier periods not presented should be reported as a restatement of beginning net position, fund balance or fund net position, as applicable, of the earliest period presented. Each individual prior period presented should be restated to reflect the period-specific effects of correcting the error.

The notes to the financial statements should disclose the nature of the error and correction, the periods affected and the financial statement line items affected. The effect on the prior period's change in net position, fund balance or fund net position, as applicable, had the error not occurred, should be presented for single period financial statements. The notes to comparative financial statements should likewise disclose the effect of the error correction on the change in net position, fund balance or fund net position, as applicable, of the prior period.

Other Reporting Requirements

Accounting changes and error corrections that do have an effect on beginning net position, fund balance or fund net position but result in a reclassification in the financial statements should be accompanied by a disclosure in the notes to the financial statements covering the nature of the change, financial statement line items affected and the reason for the change. For comparative financial statements, amounts should be reclassified in all prior periods presented, if practicable. If not, the reason why it is not practicable should be disclosed.

For all accounting changes and error corrections affecting beginning net position, fund balance or fund net position, as applicable, the aggregate amount of adjustments and restatements to each should be displayed by reporting unit. To the extent the financial statements themselves don't disclose the beginning balances as previously reported by reporting unit, the note disclosures should include a table presenting the effects on beginning net position, fund balance or fund net position, as applicable, of the earliest period adjusted or restated, which reconciles to beginning balances as previously reported to the beginning balances as adjusted or restated by reporting unit. Each column in the basic financial statements, excluding total columns, is considered a reporting unit for the purposes of these requirements.

For changes in accounting principle, required supplementary information (RSI) (including management's discussion and analysis) and supplementary information (SI) should be adjusted or restated to match the basic financial statements for reporting periods presented in the basic financial statements. Prior reporting periods presented earlier than those presented in the basic financial statements should not be restated in the RSI or SI. If prior-period information in the RSI or SI is not consistent with current-period information as a result of the change, an explanation should be included in the RSI or SI, as applicable.

RSI and SI should be restated for error corrections affecting the reporting periods presented in the basic financial statements. To the extent practicable, earlier periods presented in RSI and SI should be restated for errors affecting such periods. Periods affected should be identified as restated or not restated, as appropriate, with an explanation of the nature of the error. If it is not practicable to restate RSI or SI, an explanation of why it is not practicable should be provided.

Effective Date

The requirements of GASBS 100 are effective for accounting changes and error corrections made in fiscal years beginning after June 15, 2023. Earlier application is encouraged.

• • • •

Written by Sam Thompson.
www.bdo.com

"Is There Something I Can Read That Describes Our Compensation Program?"

By Sam Thompson

Numerous organizations invite new individuals to get involved in the administration of their executive compensation program or hire new executives with a desire to know more about the program. This question is asked many times and often the answer is no.

Every year, we consult with members of many nonprofit boards as they address the annual compensation decisions for their organizations' senior executive positions. In some cases, these are first-time projects and others are relationships that have spanned several years. There is a considerable range in the size of these organizations and the scope of services they offer. As you might expect, there is a similar range of experience and knowledge with pay-related matters among the board members we serve.

Somewhat surprisingly, the governance and administrative practices for board management of compensation are sometimes not as well developed as the size of the organization would suggest.

Somewhat surprisingly, the governance and administrative practices for board management of compensation are sometimes not as well developed as the size of the organization would suggest. A significant number of organizations have a rudimentary process in place with not much more than the calendar and the checkboxes on Form 990 and Schedule J guiding compensation decisions for the leadership team. Solely getting through the chief executive officer (CEO) / executive director's annual pay discussion and completion of the IRS forms seem to be the focal points of the board's attention to compensation.

I am not suggesting the absence of a robust process means that pay-related matters are not getting the board's attention. In most cases they are but often without the benefit of a formal compensation program and its processes to guide them. In these cases, a process of sorts takes shape based on the particular issue that needs to be addressed or the individuals who happen to be involved in addressing it.

This can lead to a variety of situations that frustrate board members and executives alike, for example:

- Questions are raised about the size, type, performance or location of organizations used for competitive pay comparisons.
- Similar concerns arise about the type of external benchmark position used for competitive comparisons.
- Confusion may arise about the authority of the board versus the chief executive to make a pay decision for a particular position.
- There may be difficulty arriving at a consensus about the positioning of pay level for the organization in relation to the range of competitive pay (e.g., median, 75th percentile, etc.) and how it is achieved (e.g., salary only, salary plus bonus, etc.).

Individuals joining the compensation decision-making process for the first time often find themselves struggling to "catch up" with the group and understand the issues involved. Individuals experienced with the ad hoc approach sometimes become exasperated with the absence of any guidelines and lengthy deliberations to arrive at a consensus on a particular issue. As one board member told me: "We have a compensation policy. We develop a new one every time we meet!"

There is a downside to this lack of a defined compensation policy and process more serious than suboptimal use of board members' time. We see instances where compensation decision-making goes off track. This puts the organization and all parties at risk. In some instances, a problem was created inadvertently. A well-intentioned desire to "do something nice" for a long-tenured executive, a large salary adjustment, or the adoption of a trendy new component for the executive's compensation plan may create the problem. In some cases, a tally of all components of the compensation program for an executive has never been made. The total compensation could be alarming. Excessive pay, or pay that appears excessive, can create reputational and / or regulatory risk for the organization.

The opposite situation also occurs. In their efforts to be conservative, good stewards of the organization's resources, compensation may fall far enough below competitive levels that the organization cannot retain or recruit qualified personnel for critical roles. Paying too little can also be problematic.

Of course, the examples I have cited are the more extreme ones. Most organizations do manage to handle executive compensation satisfactorily. What I am suggesting is that there's a better way for almost every type of nonprofit organization to manage compensation for its executives.

A formal executive compensation program is the resolution. Some may call it compensation philosophy, pay strategy or guiding principles. A formal compensation program is a comprehensive collection of answers to all the key questions and issues about executive pay. The most effective programs are developed by, and tailored to, your organization. The topics covered in a formal compensation program are fairly standard, and the detailed contents require specific input based on your organization's needs and beliefs about pay.

Excessive pay, or pay that appears excessive, can create reputational and / or regulatory risk for the organization.

Key sections of a formal compensation policy and some of the topics within them often include the following:

Program Governance

- Identification of program participants including board, compensation committee, chief executive officer and outside advisor(s)
- Table of responsibilities and authorities
- Calendar of activities

Guiding Principles and Program Considerations

- Overall role of total rewards program
- Relevant competitive marketplace(s)
- Sources and uses of competitive information
- Regulatory compliance

Program Characteristics

- Overall competitive positioning goal
- Guiding principles, for example:
  - Emphasis on team in relation to individual results.
  - Support of shorter results in relation to longer-term results.
- Compensation ranges and management of individual's compensation within ranges
- Communication of compensation information

Program Components and Their Roles

- Pay components
- Benefit components
- Perquisites

The four broad sections of a formal program discussed above cover most of the issues and questions that routinely arise in administering compensation. The benefit of the formal compensation program is realized because key topics have been addressed in a comprehensive and coordinated manner. All parties in the process know their respective roles and have established policies and processes to guide them. New participants can quickly get acquainted with the program, and the number of future meetings or situations devoted to ad hoc decisions is virtually eliminated. Board and compensation committee members and management involved with compensation follow a schedule of meetings with each devoted to an area of the program's governance and administration. Necessary preparatory materials are sent in advance of each meeting. Participants understand the expected objective for each meeting.

The process for creating a program begins with the thoughtful development of a series of broad policy positions for the organization's compensation. Some organizations take shortcuts. They adopt glib generalities as their pay principles (e.g., "above average," "… able to recruit, motivate and retain…," "…competitive within our industry…," "pay for performance," etc.) Others "borrow" programs from organizations.

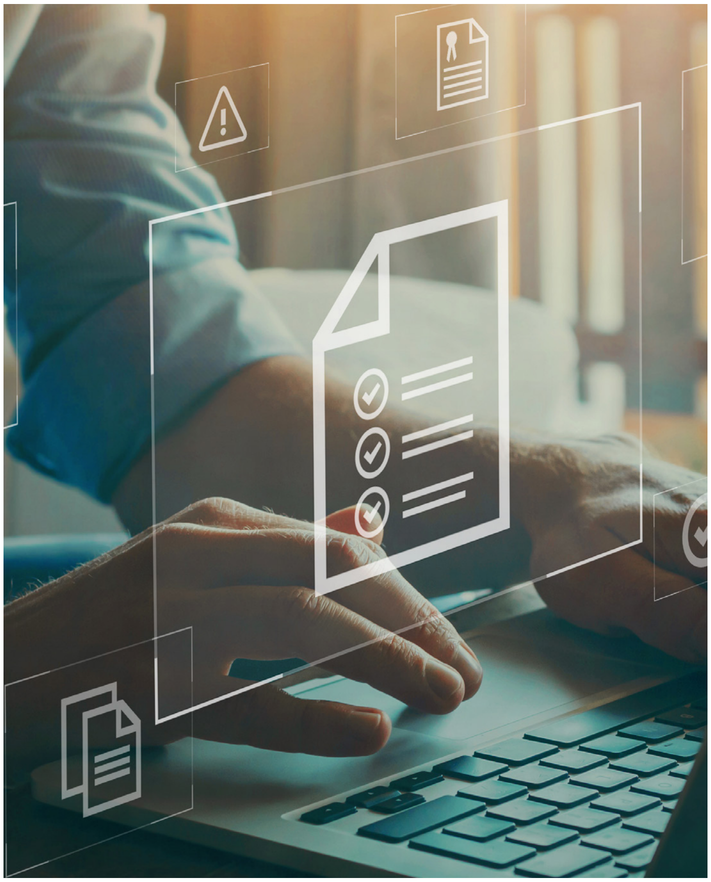
The time and attention devoted to development of a compensation program tailored to the specific needs of the organization will determine its usefulness.

The development process is straightforward. Potential policy positions covering broad program areas are explored, alternatives are examined, and a final position is then adopted by the organization's leadership. Once established, each policy is then further developed with plans and processes used to implement it. A series of well-structured work sessions can complete the process in three or four work sessions. They are designed to methodically engage program stakeholders in key decisions that will define the specifics of their organization's compensation program. The time and attention devoted to development of a compensation program tailored to the specific needs of the organization will determine its usefulness.

Is it time for your organization to develop a formal compensation program?

• • • •

Written by Sam Thompson. Copyright © 2022 BDO USA, LLP. All rights reserved. www.bdo.com



Implications and Impacts of NSPM-33 on Research Institutions

By David Clark and Jackie Bernal

On Jan. 14, 2021, just one week before the end of his term in office, former President Trump signed National Security Presidential Memorandum 33 (NSPM-33) to "direct actions to strengthen protections of the United States Government-supported Research & Development (R&D) against foreign government interference and exploitation." NSPM-33 was formally endorsed by the Biden Administration in August 2021 and the National Science and Technology Council's (NSTC) Subcommittee on Research Security published Guidance for Implementation of NSPM-33 in January 2022.

The directive responds to challenges within the fundamental activities and openness of America's government-sponsored research, recently highlighted by undisclosed conflicts and participation in programs sponsored by foreign governments, most notably the People's Republic of China and its Thousand Talents Program. Since 2018, such undisclosed and unwanted engagement with foreign governments and the misappropriation of intellectual property from U.S. government-funded projects has been a focus of the Department of Justice.

Background

The objective of NSPM-33 is to prevent foreign governments from obtaining any non-public results of U.S.-funded research, whether by conflicts of interest or commitment or a research security breach. The memorandum highlighted a need for enhancements to key areas of government oversight and protection of funded research activities, including:

- Restrictions and education for federal personnel regarding participation in foreign government-sponsored talent recruitment programs.
- Strengthened vetting processes for foreign students and researchers.

- Increased disclosure requirements for research grant applications and ongoing recipient reporting, to be standardized across agencies to the greatest extent practical.
- Implementing policies regarding the use of a Digital Personal Identifier (DPI) for federally funded researchers.
- Establishing requirements for research security programs at research institutions.

In an effort to maintain America's commitment to openness, transparency and honesty in research, federal departments and agencies, recipient organizations and individual researchers will need to join together to implement and comply with the requirements of NSPM-33.

While many agencies have published updated guidance and templates regarding what, when and by whom information must be disclosed, work continues to establish DPI standards and processes for analyzing and working with the collected data.

NSPM-33 Implementation Progress

NSPM-33 is a call to action for all federal agencies to standardize and strengthen disclosure activities, under NSTC's leadership. In January 2022, NSTC issued NSPM-33 implementation guidance to agencies, summarizing the varying expectations and time frames for compliance in the following five key areas:

1. Disclosure Requirements and Standardizations
2. Digital Persistent Identifiers (DPI)
3. Consequences for Violation of Disclosure Requirements
4. Information Sharing
5. Research Security Programs

While more detailed standards and requirements related to disclosure processes and research security programs are expected to emerge, here is what we know so far.

Updated Disclosures

Agencies were given 120 days to address certain expectations, including enhancements to disclosure processes and collection of broader, consistent levels of information within grant proposals and throughout the life of federal awards. The National Institutes of Health (NIH), National Science Foundation (NSF) and Office of Science and Technology Policy (OSTP) co-chaired an interagency working group to coordinate and cooperate in the design and implementation of new disclosure requirements. While agencies attempted to standardize disclosure expectations as much as possible to ease administrative burden, the uniqueness and nuances of programs offered by the various agencies made a single, common disclosure form and process impractical.

While many agencies have published updated guidance and templates regarding what, when and by whom information must be disclosed, work continues to establish DPI standards and processes for analyzing and working with the collected data.

Research Security Program

Beyond the enhanced disclosure requirements, organizations receiving in excess of $50 million per year in "total federal research funding" will be required to complete a certification that they have implemented a research security program following the expectations of NSPM-33. While exactly how this certification will be accomplished is still in development by OSTP, the NSTC Subcommittee on Research Security, and the Office of Management and Budget (OMB), organizations meeting the funding threshold must address the currently vague guidance related to enhancing processes and controls around:

- Cybersecurity
- Foreign travel security
- Research security training
- Export control training

Research organizations must appoint a research security point of contact (POC) and provide a publicly accessible means (such as through a website or social media) to contact that individual. Organizations subject to other existing federal security standards, such as those involving classified or controlled unclassified information (CUI) can combine research security POCs, but would not need to apply the most stringent requirements associated with classified information or CUI to all research within the general program.

Challenges and Criticisms

While it is understandable that the government felt the need to move toward NSPM-33, challenges still exist for impactful implementation. Beyond the difficulties coordinating standardization of disclosure forms and processes across agencies and the condensed timeline to complete development, implementation and communication from the government, the largest concern raised is related to how this shift impacts the overall intent and purpose of fundamental research conducted across the country. The openness of the federally funded research enterprise within the U.S. has been paramount to our ability to improve healthcare, ensure the safety and well-being of Americans, advance technology and promote innovation around the globe. Further, disclosures will be the responsibility of individual researchers and key project employees, so the urgency of training, education and monitoring will be paramount to ensuring these enhanced processes yield their intended effect.

While agencies attempted to standardize disclosure expectations as much as possible to ease administrative burden, the uniqueness and nuances of programs offered by the various agencies made a single, common disclosure form and process impractical.

• • • •

Written by David Clark and Jackie Bernal. www.bdo.com

Cybersecurity Best Practices for Your Organization

By Matt Cromwell, Sam Thompson, David Clark, Jackie Bernal, Matthew Becker and Cathryn McAleavey

According to a study by N-able, managed service providers (MSPs) report that 82% of their customers have seen an increase in attempted cyberattacks since the pandemic. Even MSPs themselves are a target for cyber criminals, which can have wide-reaching impacts on their customers and network of resources if breached. As threats become more prevalent, it's imperative organizations not only implement cybersecurity best practices, but also work with strategic advisors who value the same practices.

The Cybersecurity & Infrastructure Security Agency released a report detailing how MSPs and their customers should be protecting against cyber threats.

Here Are 10 Cybersecurity Best Practices That Should Be Top of Mind for Your Organization.

Take Preventive Measures to Mitigate Cyberattacks

First and foremost, your organization should take every preventive measure possible to prevent cyberattacks. Mitigation tools and resources can help you prevent initial compromise, thus making it less likely an attacker will disrupt business operations or pose a significant threat to your business.

If you're unsure of your current level of cyber maturity, then cyber assessments are a great place to start. An assessment can help you understand what your biggest risks are, where you should focus your efforts and investments, and how to help improve your maturity and strengthen your defenses.

Be Diligent and Thorough with Your Logging and Monitoring Process

Logging and monitoring are critical components of a cybersecurity program. The reality is it can be months before an incident is detected within an environment, and with so many threats and an abundance of data to continuously comb through to identify an incident, it's critical for organizations to implement and maintain a logging and monitoring solution.

It is recommended the logging solution retain your most relevant and important logs for at least six months. Logging and monitoring provide additional visibility into incidents, aids in threat hunting, and reduces the time needed to triage and investigate a potential incident.

If you are working with an MSP to deliver a logging and monitoring solution, make sure they can deliver on necessary contractual obligations to help ensure success.For example, a vendor should be able to do the following:

- Implement a comprehensive security information and event management (SIEM) solution that enables logging and monitoring.
- Deliver visibility and communication as it relates to the providers' access, presence, activities and connections to the customer environment (are the MSPs' accounts properly monitored and audited?).
- Notify the customer when a confirmed or suspicious event/incident occurs on the provider's infrastructure and administrative networks. The provider should conduct a thorough analysis and investigation.

Deploy Multifactor Authentication (MFA) and Pay Attention to Account Privileges

As more entities shift to a hybrid or fully remote work environment, the need for MFA is more apparent than ever. Deploying MFA adds that extra foundational layer of security when you have employees accessing organization networks from varying locations and devices. It's important that any business advisor you work with not only mandates the use of MFA, but also requires MFA within their own business.

To touch on a previous point, you should also make sure you're reviewing logs for unexplained failed authentication attempts. In some cases, this may indicate that an account within the organization has been compromised. Additionally, be thoughtful about who has permissions to certain accounts and disable accounts when they are not actively being used. Audit this regularly.

Lastly, use the principle of least privilege to restrict unnecessary privileges. This requires that you identify the most high-risk devices across your organization and minimize the access people have to them. When working with a vendor, make sure they apply this principle to your network environments.

Segregate and Control Internal Data and Networks

As an organization, it's important that you understand your environment and segregate your networks. By doing this, you'll be able to isolate critical business systems and apply network security controls to reduce risk across the organization.

It is recommended that organizations verify their connections between internal systems, their MSPs' systems, and other strategic advisors and supplier networks they communicate with. Virtual private networks (VPNs) or alternative secure access solutions should be used when connecting to MSP infrastructure, and all traffic should be limited to that one dedicated, secure connection.

Your organization should also ask and validate that any third-party vendor you are working with uses different admin credentials for each customer (i.e., they won't use the same credentials they use to log in to your organization that they use for other customers). If any of those vendors' customers are breached, those same credentials could be used to compromise other organizations, including yours.

With vendors and other trusted advisors having access to an organization's network, it becomes increasingly important to limit network access. Limiting access of advisors to only the solutions or applications they require helps improve security hygiene. Over the past few years, ransomware actors have increasingly started to target business advisors to gain access to other organizations by abusing trusted access and a lack of segregation controls. Threat actors continue to have success by leveraging a lack of controls limiting user privileges and access to data.

Apply the Principle of Least Privilege

Use of tiering models is recommended for administrative accounts to provide layered permissions that don't create unnecessary access or privileges. Full privileged accounts should only be used when absolutely necessary and should be time based to further restrict risk. Identifying high-risk devices, applications and users can help minimize access and associated risks.

As an organization, you should require that the vendors you work with apply this least privilege principle across your environment as well as their own. Additionally, they should only have access to the services and resources needed to deliver the agreed-upon scope of work.

Building on least privilege is the zero-trust model. While not quite interchangeable but tightly coupled, zero trust means every organization, by default, should put zero trust in every user, endpoint, device, etc. From internal to external users, mobile devices to laptops, network components to network connections, every endpoint should be considered untrusted until authenticated and authorized.

Apply Updates Regularly and Adhere to All Recommendations

To be fully secure and compliant, don't just apply routine updates. Go the extra mile and address that all aspects of patches are adhered to. When working with a vendor, use their recommendations and experiences to help ensure you're getting the most out of updates. For example, organizations should prioritize patching vulnerabilities included in CISA's catalog of known exploited vulnerabilities (KEV) versus only those with high Common Vulnerability Scoring System (CVSS) scores that have not been exploited (and may never be exploited).

Back Up All Systems and Data Routinely

Equally as important as routine updates are routine backups. Regularly backing up your critical data and systems is an important cybersecurity best practice. Data from business-critical systems should be backed up, with the frequency of backups being informed by the type of data and business requirements. Backups should be stored remotely, encrypted and, ideally, have different retention spans as a best practice.

Further, keep backups separate and isolate them from network connections that could promote the spread of ransomware. Most ransomware variants attempt to find and encrypt/delete accessible backups. Isolating them will allow for the restoration of systems/data to their previous state.

Another important aspect of disaster recovery is frequent backup and restoration process testing. You must confirm that your process works; the time of a disaster is not the appropriate time for these tests! They should be planned, scheduled and tested at a regular cadence. Then, process and procedure documentation should be updated based on results.

Create and Implement an Incident Response and Recovery Plan

Often the best way to shore up a security program is to improve internal operational procedures. Make sure your computer emergency response team and crisis plans are tuned to the digital age. Don't be caught flat-footed in terms of privacy, reputation or other impacts.

An incident response and recovery plan should outline the roles and responsibilities of all stakeholders in the organization in the event of a disaster. Make sure you keep updated, hard copies of this plan on hand to help ensure the plan is accessible even if networks are inaccessible. Additionally, to be extra prepared, you should test your plan often.

Understand Supply Chain Risk and Manage It

Vendors bring a certain level of expertise and valuable experiences to the table; however, with those connections comes increased risk. Integration of the digital supply chain creates massive conveniences but provides an increasing number of new opportunities for threat actors. Even within the secure and trusted connection of your most important digital vendors, threats can thrive with persistence and cause widespread damage.

Organizations should validate that their contractual agreements with third parties meet specific security requirements and that their contract specifies whether the third party or the customer owns specific responsibilities, such as hardening, detection and incident response.

Your organization must understand the risk of working with third-party vendors and subcontractors. When working with third-party vendors, make your security expectations very clear from the get-go and make sure that you understand and audit the level of access they have.

Partner With Those Who Believe in Transparency

Last but certainly not least, remember that more transparency leads to enhanced security. When working with external vendors, make sure you clearly understand what security services are being provided. Address anything you feel your business needs but that may fall outside of the scope of the contract.

Check to make sure your vendor clearly outlines how they will notify you in the case of an incident affecting your environment. As their customer, a vendor should want you to have as much information about your cybersecurity program as possible. Being transparent will only benefit both of you in the long run, as it can enable better results and a more secure business environment.

• • • •

Written by Matt Cromwell, Sam Thompson, David Clark, Jackie Bernal, Matthew Becker and Cathryn McAleavey. Copyright © 2022 BDO USA, LLP. All rights reserved. www.bdo.com

How Technology & Culture Support Sustainability

By Matthew Becker and Cathryn McAleavey

Embracing technology, outsourcing key operations to specialists and improving organizational culture can all be a part of a nonprofit's plan for sustainability. While it's important to make plans, recent years have demonstrated how easily even the best-laid plans can go awry.

The following four key steps can provide direction.

1. Embrace Technology to Enhance Efficiency and Increase Transparency

Technology can help nonprofits optimize processes to seize opportunities for fundraising and overcome a variety of current challenges, including rising cybersecurity risk and staffing shortages.

Organizations are increasingly leveraging artificial intelligence (AI) technology to take a deep dive into donor pools. Tech-enabled data analysis can help nonprofits determine who is most likely to give, identify their most involved donors, and uncover the best ways to engage them.

Nonprofits that adopt technology are also better prepared to mitigate current threats and challenges. The pandemic sparked a shift to remote work environments and online operations, creating new opportunities for cybercrime. Nonprofits that switch to digital payments and concentrate cash in a global pool via automation can benefit from more transparent tracking. Additionally, as the labor shortage continues, nonprofits that automate their job application and hiring processes are well equipped to fill empty positions with minimal interruption.

Tech-enabled data analysis can help nonprofits determine who is most likely to give, identify their most involved donors, and uncover the best ways to engage them.

2. Reassess Organizational Culture to Retain and Attract Talent

Streamlined application and onboarding ensure that positions are filled, but a strong organizational culture increases the likelihood that new hires are motivated to remain at and grow with the nonprofit. Shifting employee expectations and stiff competition for labor provide ample incentive for nonprofits to reassess their practices, policies and offerings.

It's a worker's job market, where employees are leaving employers for jobs that offer them greater work-life balance, mission alignment and other benefits. Nonprofits should explore their benefit packages and ensure they have competitive and equitable offerings, including paid time off, mental health benefits and other programs. It is also crucial that nonprofits looking to retain employees offer opportunities for career advancement. Professional development initiatives allow trusted staff to acquire valuable skills and apply them to furthering the nonprofit's mission.

Organizational culture also encompasses the intangible. Decisions should be made with the goal of caring for employee mental health and avoiding burnout. Nonprofits should consider whether employee feedback is sought and implemented, whether collaboration among colleagues is valued over competition, and whether their practices and policies are equitable, and then adjust accordingly.

3. Consider Outsourcing Operations to Multiple Vendors

Nonprofits looking to support and retain employees might want to consider outsourcing key responsibilities and functions to multiple vendors. Outsourcing to specialists in human resources, marketing and other work not directly related to the nonprofit's mission can help boost staff morale and return on investment (ROI).

Some nonprofits with limited resources try to handle as many tasks as possible in-house. This practice can have the unintended result of overwhelming employees and distracting them from the mission related work that initially drew them to the role. Others outsource all work not directly related to the mission to one vendor. While less time-consuming than performing these functions internally, outsourcing to a one-size-fits-all operation might not be the most cost-effective or efficient option.

Nonprofits should consider whether employee feedback is sought and implemented, whether collaboration among colleagues is valued over competition, and whether their practices and policies are equitable, and then adjust accordingly.

Nonprofits might maximize ROI by placing select responsibilities in the hands of specialists. Nonprofits that choose this route benefit from expert help in essential areas and have a greater ability to customize their outsourcing plan to meet their needs as they scale and navigate economic uncertainty. As they diversify their network of vendors, nonprofits are encouraged to do their due diligence. In addition to key considerations like cost and scope of services, nonprofits will want to ensure vendors' values align with their mission. They will also want to make sure vendors follow cybersecurity best practices.

4. Develop a Plan for Sustainability

Nonprofits that engage in scenario planning can prepare for the worst as they strive for the best. Scenario planning involves organizations thinking through their best- and worst-case financial scenarios to determine what steps they would take in each situation. What expenses would be reduced in a worst-case scenario? Alternatively, what investments would be made in a best-case scenario?

Nonprofits are also encouraged to develop multiyear models to help them look beyond the annual budgeting cycle and understand what financial resources are needed to meet their goals over the next three to five years. It is crucial that nonprofits engage their boards in multiyear planning.

Organizations that leverage technology for key insights and efficiency, prioritize improving organizational culture, diversify their network of vendors and devise a detailed sustainability plan today are more likely to seize tomorrow's opportunities and mitigate challenges.

• • • •

Written by Matthew Becker and Cathryn McAleavey. Copyright © 2022 BDO USA, LLP. All rights reserved. www.bdo.com

Other Items to Note

Shuttered Venue Operators Grant (SVOG) Updates

The Small Business Administration (SBA) has updated the SVOG Post-Application Guidance and the Post-Award Frequently Asked Questions. These documents apply to both non-federal entity recipients (these include nonprofit entities, state and local governments and Native American tribes, and institutions of higher education) and for-profit recipients. Included in the updates made by SBA to these documents are updates to questions related to the audit requirements.

Federal Audit Clearinghouse (FAC) Transition From Census to GSA

The FAC plans to transition from the U.S. Census Bureau to the General Services Administration (GSA) on Oct. 1, 2023. This is a one-year delay from the original plan.

The Census FAC will continue to accept fiscal year 2021 single audits as they have been doing historically. The Census FAC will begin accepting fiscal year 2022 single audits on Oct. 1, 2022. The 2022 fiscal year-end single audits cannot be submitted until a formal update to the Data Collection Form (DCF) is completed to permit its use for the 2022 audits. Census is currently working on updating the DCF. Some of the expected updates to the form include replacing the entity's DUNS number with the new entity Unique Employer Identification (UEI) number and changes to permit the FAC to eventually accept the alternative compliance examination engagement for certain recipients of the Coronavirus State and Local Fiscal Recovery Funds (CSLFRF). (See the Other Items to Note section in the Summer 2022 Nonprofit Standard for more information on the CSLFRF issue.)

The Office of Management and Budget has stated that the provision described in Appendix VII of the Compliance Supplement that temporarily suspends the 30-day aspect of the single audit submission deadline continues to apply even though this was originally put into place due to the change in the FAC from Census to GSA. As a reminder, under the Uniform Guidance the DCF must be submitted within the earlier of 30 days from the audit report date or nine months after the fiscal year-end. As a result, if it is not possible to meet the 30-day aspect of the single audit submission deadline due to the delay in the ability for the Census FAC to accept 2022 fiscal year end single audits, those audits will not be considered late if they are submitted within nine months after the end of the audit period.

Coronavirus State and Local Fiscal Recovery Funds Guidance

On Aug. 11, 2022, the U.S. Department of the Treasury (Treasury) issued a document titled, Alternative Compliance Examination Engagement Report User Guide (User Guide). It provides information for eligible recipients to submit the CSLFRF alternative compliance examination engagements through a Treasury portal. This is likely a temporary measure until the Census FAC can accept these in the future as discussed above. However, until Treasury states otherwise, these engagements should be submitted by recipients to Treasury as described in the User Guide.

• • • •

baldwin
CPAs

For additional information regarding any article, please contact Chris Hatcher or Myron Fisher via email or at 1.866.287.9604.

OFFICE LOCATIONS

114 N. Main Cross St., Flemingsburg, KY 41041
1019 Majestic Dr., Suite 370, Lexington, KY 40513
116 Sutton St., Maysville, KY 41056

713 W. Main St., Richmond, KY 40475
10180 Linn Station Rd., Suite A200
Louisville, KY 40223