# Global Information Assurance Certification Paper

# Built From Scratch – Creating an Audit Program for a Nonprofit Organization

*GIAC (GSNA) Gold Certification*

Author: Christopher Jarko, csjarko@yahoo.com
Advisor: Rick Wanner
Accepted: March 9, 2017

Abstract

Corporations and government entities are not the only enterprises in need of IT security audit programs. Nonprofit organizations are also exposed to risk, and can also use audit to monitor compliance and ensure system vulnerabilities are mitigated. While most nonprofits are often thought of as small organizations, some have extensive compliance requirements, enterprise-scale network architectures, and robust audit programs. Smaller nonprofit organizations often lack an audit program, and may not even factor risk management into their decision-making process. This paper will document the tailoring of enterprise audit processes to align with the realities of small nonprofit organizations, with the intent to provide a means for measuring and reporting risk that will not exceed the capacity of the organization's IT department, and in order to provide a repeatable framework so that other organizations are able to accomplish the same outcomes in attempting to secure their networks.

# 1. Introduction

Network audit assesses the effectiveness of an organization's security controls and identifies and documents risks to information security (Hoelzer, D.; Enclave Forensics, 2016). Building and sustaining an audit program requires an organization to invest time, labor, and money, yet the financial return on investment is very difficult to quantify. The enterprise world and large nonprofit organizations (NPOs) often make the investment in audit because it is required by regulation. On the other hand, small NPOs without such a requirement typically lack audit programs altogether (Gelbstein, 2015).

The absence of audit in small NPOs impedes their ability to manage risk and efficiently remediate existing security problems. NPOs in general often fail to make risk management a priority. According to one survey of nonprofits, only 22 percent of the respondents had a dedicated risk management position (O'Rourke, 2013). Furthermore, small NPOs typically have limited IT staffs, leading them to believe that audit is beyond their capacity.

To be fair, building an audit program from scratch can be a significant undertaking. Audit is usually conducted within the context of a risk management framework. Many of these frameworks can appear overwhelming, which could contribute to an NPO's reluctance to initiate an audit program. One such framework comes from the U.S. government's National Institute of Standards and Technology (NIST) (National Institute of Standards and Technology, 2017), another from the International Organization for Standardization (ISO) (International Organization for Standardization, 2017). Each of these frameworks is comprised of multiple volumes and hundreds of pages. While comprehensive, their size and complexity make them unsuitable for most small NPOs. There is a third option, managed by the Center for Internet Security (CIS). Consisting of twenty prioritized security controls (CSCs), the CIS framework is still extensive but much more concise, and therefore has potential for use by a small NPO.

Ultimately, the belief that a small NPO cannot sustain an audit program is understandable but mistaken. Conducting small audits using a repeatable framework, a clearly defined subset of the CSCs, and open source security tools, a small NPO's IT staff

can baseline their network, and subsequently audit against that baseline. In many small NPOs, the IT staff might not know how to accomplish this, but an information security professional acting as a volunteer can help the NPO build a self-sustaining audit program. This paper will provide a usable framework for creating such a program at a small NPO that does not already have a regulatory requirement to audit their networks.

# 2. Background

## 2.1. Information Security and Nonprofit Organizations (NPOs)

Nonprofit Organizations (NPOs) vary greatly in size and diversity of activity. At one end of the spectrum, Boys Town is a Nebraska-based NPO which operates two hospitals, multiple homes for at-risk youth, schools, a police department (Boys Town Village is a municipality), and other "affiliate corporations" (Boys Town, 2017). Many of the sub-organizations within Boys Town have enterprise-like compliance and regulatory requirements and correspondingly mature information security programs. Interestingly, however, Boys Town only recently created an office to centrally coordinate information security risk management efforts (Stewart, 2016).

At the opposite end of the spectrum are small NPOs, including local branches of organizations designed to provide after-school programs, such as Girls Incorporated (Girls Incorporated, 2017). These NPOs are relatively small, with few employees and a comparatively small budget. They still process sensitive information, but the need for information security governance and subsequent audit requirements might not be as evident to the NPO management or IT staff. This oversight can contribute to a mindset among NPO leadership where determination of risk is not even considered in their planning and operations (Stewart, 2016), seemingly confirming the results of the previously cited survey of NPOs. When risk is not considered, and governance is not obvious, the existence of an IT audit program is unlikely.

## 2.2. Audit at Small NPOs

### 2.2.1. Benefits

An audit program can provide the same benefits to a small NPO as it does to a larger organization. First and foremost, an audit program helps quantify risk, which in turn can be used to prioritize limited IT resources. An audit program can help an organization understand its information environment by facilitating an inventory of IT hardware and software. Auditing can serve as a means to validate whether or not the NPO is following industry best practices (IT Policy Compliance Group, 2009). Finally, if the organization's operations are subject to a regulatory framework, auditing is necessary to verify compliance.

A successful audit encounter with an NPO helps the community, furthers a cause the volunteer auditor believes in, and provides an opportunity for both the auditor and the NPO's IT staff to grow professionally. The auditor can use an NPO audit as an opportunity to gain experience, practice audit techniques, or work with different network architectures, all in a low-stress environment. The NPO IT staff can increase their knowledge of network security principles, see firsthand how implementing security affects network operations, and learn about security from the auditor's past experiences. Finally, a volunteer audit increases the security of the NPO's networks without the added cost of hiring an additional IT staff member.

### 2.2.2. Challenges

Although audit benefits organizations regardless of size, a small NPO is inherently limited in capacity. An enterprise IT organization can dedicate the resources necessary to make an audit program robust and successful, whereas an NPO with one or two IT professionals on staff would be hard-pressed to sustain an enterprise-level audit program. An enterprise audit lasts days and can take a team of 2 – 3 auditors anywhere from 40 – 500 hours on the aggregate, with much of that time involving the sysadmins as well (Fish, E-mail from Warren Fish, Manager of IT Audit, ACI Worldwide, Inc. (Subject: Audit Timelines), 2017). If the NPO has a two-person IT staff, this means they will be unavailable to perform their routine duties for the duration of an audit performed in this manner.

Audit also requires skills a small NPO's sysadmin may not possess. Much of audit is security-focused, but security is not the same as administration. Some audit tools will probably be familiar to most admins, but others may be new.

A third factor makes audit difficult for a small IT staff. Audit is more effective when conducted within the context of a risk management framework. There are several frameworks available, such as ISO 31000 (International Organization for Standardization, 2017) and NIST SP 800-39 (National Institute of Standards and Technology, 2011). Both the ISO and NIST frameworks are very complex, which could be intimidating to a small IT staff.

## 2.3. Scoping the overall effort

SANS teaches audit as a 6-step process (audit planning, entrance conference, fieldwork, preparing the report, exit conference, report to management) (Hoelzer, D.; Enclave Forensics, 2016). This process is thorough, but can still be feasible at a small NPO. Following SANS' six steps on a smaller scale, the IT staff can conduct multiple smaller audits, each seeking to achieve *limited* objectives. The keys to this "lightweight" approach are identifying which parts of each step are relevant to the NPO, and modular scheduling over an extended period, perhaps six to nine months. Doing these things increases the IT staff's availability while still allowing them to achieve a significant end state – possession of a baseline against which to conduct future recurring audits.

### 2.3.1. Tailoring the six-step process


**Figure 1 - The SANS Six-Step Audit Process**

Some parts of the SANS process are still required, regardless of the size of the organization or objectives of the audit. It is hard to imagine conducting an audit without planning it first. Fieldwork refers to the actual tests and reviews that make up an audit. Following fieldwork, a report must be prepared and delivered; otherwise the organization will have nothing on which to base risk management decisions. Entrance and exit conferences *could* be omitted in the case of a small NPO, but there are still reasons to conduct them, as will be shown later. Instead of completely cutting out one or more steps, a better way to streamline the audit process is to scope each step in consideration of several factors such as fiscal and manpower constraints, the skill level of the IT staff, and the security culture at the NPO.

### 2.3.2. Modular Scheduling

In addition to tailoring the process to fit the NPO, the auditor and IT staff must scope each audit. In doing so, the auditor should realize that not every audit needs to be a comprehensive review of the network's security. Moreover, the first audit of any organization is likely to produce so many findings that the IT staff could be overwhelmed, leading to the perception that there are too many problems to remediate.

As a result, NPO might only attempt to fix a very small subset (perhaps as few as the top five or ten findings). The Australian Signals Directorate noted this phenomenon, leading to the creation of their "Top 4 Mitigation Strategies" (Misenar & Conrad, 2016, 2nd Quarter). The remaining findings may *never* be fixed; once briefed to management, the risk for these findings is accepted, and they are therefore "out of scope" for future audits (Fish, Interview with Warren Fish, Manager of IT Audit, ACI Worldwide, Incorporated, 2016). In contrast, using a modular approach will help keep the number of findings to a manageable level. The scope of the individual audits is at the discretion of the IT staff, provided that each audit accomplishes a smaller part of the overall goal. The key to making this approach work is to have the entire process mapped out before the first audit. This "map" may change in light of findings made during the course of the smaller audits, but the auditor and IT staff must document the changes.

And yet the audits themselves are only part of the scheduling equation. Hardening a network takes time; risks need to be mitigated or remediated through the implementation of security controls. Until those controls are implemented, an audit may accomplish little more than identifying known shortfalls. On the other hand, if the IT staff is given the opportunity to select and implement the controls first, then an audit can serve to validate the effectiveness of the controls and the manner in which they were implemented. Therefore, choosing and implementing security controls prior to the first audit is a more effective approach.

Preselecting security controls raises the issue of which controls to implement. The NPO IT staff could select controls based on their budget, threat trends reported in open source publications, the auditor's advice, or other factors. A better basis for selection is to use a consolidated risk management approach. Fortunately, several such approaches exist.

## 2.4. Choosing a Risk Management Approach

### 2.4.1. Comprehensive approaches - National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO)

One such approach is published by the U.S. Department of Commerce's NIST and is available free of charge at the NIST website (www.nist.gov/publications). The NIST approach centers around Special Publication 800-39 (NIST SP 800-39) *Managing Information Security Risk: Organization, Mission, and Information System View* (National Institute of Standards and Technology, 2011). NIST SP 800-39 is supported by several more Special Publications, totaling hundreds of pages.

Another comprehensive approach comes from the Switzerland-based ISO. ISO 31000 provides the overall framework for managing information security risk and is supported by another standard, ISO 31010. In addition to being complex, ISO standards are not free. As of February 2017, ISO 31000 and 31010 sold for approximately USD $118 and $320, respectively (International Organization for Standardization (ISO), 2017). Given the NIST and ISO standards' length and complexity (not to mention the cost of the ISO standards), these approaches are not feasible for a small NPO.

### 2.4.2. Center for Internet Security (CIS)

An alternate option is the Center for Internet Security Critical Security Controls for Effective Cyber Defense, also known as the CIS Controls, or CSCs. The CSCs serve as an excellent roadmap to improve information security and reduce risk, and are available free of charge for non-commercial use at the CIS website (www.cisecurity.org). They are less of a formalized overall approach to risk management than NIST SP 800-39 or ISO 31000, but instead represent a prioritized collection of security best practices. While not nearly as exhaustive as the listing of security controls found in the NIST or ISO frameworks, implementing all 20 CSCs is most likely beyond the capacity of a small NPO. According to the CIS website, "Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent" (Center for Internet Security, 2017).

Rather than attempting to implement all the CSCs at once, a small NPO could implement the first *three* CSCs sequentially: CSC 1 (*Inventory of Authorized and Unauthorized Devices*), CSC 2 (*Inventory of Authorized and Unauthorized Software*), and CSC 3 (*Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*). By implementing just these three controls, the NPO will gain awareness of what connects to or operates on their network as well as configuration management and change control processes to prevent deviation from what is authorized. Once CSCs 1 – 3 are implemented, the NPO will have a baseline against which to conduct future audits on a recurring basis. Later, as the NPO's security program matures (perhaps over a two year period), the IT staff could consider adding CSC 4 (*Continuous Vulnerability Assessment and Remediation*).

Implementing CSCs 1 – 3 and getting to the point where the NPO has a usable baseline will take time, effort, and resources, but it is an achievable goal. Using audit to validate the effectiveness of this implementation will also take time, effort, and resources, but is achievable if done within the audit framework proposed below.

# 3. Execution

## 3.1. A Repeatable Framework

To create a repeatable process for auditors to establish programs at NPOs, perform the following steps (corresponding SANS step in italics):

- Initial contact – approach the NPO to propose the audit (*Audit Planning*)
    - Introduction and explanation of intent
    - Explain the audit process and determine audit objectives and end states
    - If NPO is interested, arrange subsequent face-to-face meeting
- Scheduling meeting (*Audit Planning*)
    - Offer assistance to the NPO
    - Discuss CSCs 1 – 3, if IT staff is not familiar with them
    - Gather technical and policy information about NPO network:
        - Identify the network architecture

        - Identify sensitive information transmitted over or stored on network
        - Written security policy
        - Identify "normal" network use
    - Plan which controls will be implemented to achieve CSCs
    - Build timeline
    - Schedule first technical meeting
- Technical meetings (iterative, one for each audit) (*Audit Planning*)
    - Review audit objective and end state
    - Scope the audit; identify the following:
        - "No scan" systems, applications, directories, or files and quantity of each to include "in scope"
        - Tests and scans to be performed
        - Tools to be used to conduct the tests
        - Documentation to be reviewed
        - Date and time the audit will take place
        - Entrance and exit conference attendance and additional presentation requirements
- Create the audit plan (*Audit Planning*)
    - Document the technical meeting and submit the audit plan to the NPO for approval
    - Provide an opportunity for the NPO to ask questions or make changes
    - Draft a "Get out of Jail letter" (Indemnification/Hold Harmless agreement)
- Conduct research for the audit as required (*Audit Planning*)
    - Vulnerability research
    - Research on tools
- Conduct entrance conference (*Entrance Conference*)
- Conduct audit fieldwork (*Fieldwork*)
- Prepare the audit report (*Report Preparation*)
    - Findings
    - Recommendations

  - Action plan
- Conduct the exit conference (*Exit Conference*)
- Report to management, if applicable (*Report to Management*)
- Follow up with NPO (*Audit Planning*)
  - Mitigation of audit findings
  - IT Staff's lessons learned
  - Auditor's lessons learned
  - Schedule next audit

## 3.2. Initial Contact – Approaching the NPO to Propose the Audit

### 3.2.1. Introduction and explanation of intent

Depending upon whether or not the auditor has a pre-existing relationship with the NPO, the method of first contact could vary. If the auditor is already involved with the NPO in another capacity (e.g., as a volunteer), then the auditor can request an introduction to the IT staff from their contacts at the NPO. If the auditor is not yet affiliated with the NPO, they will need to make initial contact in the form of a "cold call." The auditor's first contact with IT should include their information security credentials and experience, as well as a brief but concise explanation of why the NPO may want to allow an audit (to identify risk and help the secure its networks). The auditor can make this contact in person, through a phone call, or by an introductory email with a resume attached.

Regardless of whom the auditor knows at the NPO, the best choice for proposing an audit is the IT staff rather than the NPO management. At first, bypassing the NPO management to talk directly with the IT staff may seem counter-intuitive. Management buy-in helps the audit go more smoothly and helps overcome resistance (Hoelzer, D.; Enclave Forensics, 2016). In the case of an NPO without an existing audit program, the IT staff has no reason to accept the volunteer auditor's proposal. Downward direction from NPO management could easily cause resentment between the IT staff and the auditor, making teamwork difficult and casting serious doubts on the success or sustainability of an audit program at the NPO.

Another potential hurdle for the volunteer auditor is mistrust of the auditor's motives by the IT staff. To be fair, this is not totally unreasonable. After all, a stranger calling out of the blue and asking for detailed information on network architecture and security controls is certainly a valid reason for concern. While an auditor's actions do not directly increase network security, the volunteer auditor genuinely wants to use his skills to help harden the network. Still, a malicious social engineer could use the same cold call tactic to gain unauthorized access and cause harm to the NPO. To help ease the IT staff's concerns, the auditor should offer to sign a non-disclosure agreement (NDA) prohibiting the auditor from revealing audit findings or information about the NPO's network. Also, the auditor should explain how the audit can be scoped to minimize exposure of sensitive information.

A third source of potential resistance from the IT staff may be fear, either of being made to look foolish or getting fired. Audits generate reports. Should the controls used to secure the NPO's networks be found lacking, and the report find its way to the NPO's leadership, the IT staff could be held personally accountable. This would be a horrible outcome from an audit the IT staff did not request in the first place. While this fear is understandable from the IT staff's perspective, the auditor's role is not to judge anyone's job performance, and this must be taken into account when preparing the audit report (Hoelzer, D.; Enclave Forensics, 2016).

The IT staff may also fear the audit will lead to a significant increase in their workload, as well as a strain on their limited IT budget. Fear of being stretched too thin could be particularly unappealing for the IT staff; again, this audit was not their idea, and their time and budget may very well be fully utilized when the auditor makes first contact. For that matter, the IT staff may feel the extra work is outside the normal scope of their duties.

To gain the IT staff's trust, overcome their fears, and help secure the NPO's networks, the volunteer auditor should consider making a formal presentation to the IT staff at the technical meeting, not only to explain their proposed audit methodology but also to cover the following topics:

***The auditor will practice transparency in all aspects of the audit.*** Nothing builds trust faster than trustworthiness. As with any audit, there should be no surprises. The auditor will work with the IT staff to scope the audit and will review findings with the IT staff before finalizing the report.

***The audit will assess the controls, not the people.*** It is neither appropriate nor fair for an auditor to judge job performance. This is especially true when the auditor is not a member of the NPO's staff and does not have the full context in which the controls were implemented. It is absolutely essential to provide assurances to the IT staff that the focus of both the audit and the audit report will be the *identification of risk* to enable informed decision making on prioritizing security efforts.

***The audit will serve as an opportunity for the exchange of knowledge between the auditor and the IT staff.*** This knowledge will increase both parties' skill and value to their respective organizations.

***The auditor will do their best to understand the nature of the organization being audited and its limitations, especially in terms of budget and manpower. Also, the auditor understands that others will have to pay the bill for any recommended changes.*** A $2,000 Palo Alto Firewall and a fully staffed Security Operations Center are almost certainly out of reach for a small NPO. An auditor who makes recommendations that cannot be implemented is neither helping the NPO secure its network nor protect its sensitive information. Also, the auditor may have significantly more information security training and experience than the IT staff of a small NPO. An administrator who lacks security training and experience through no fault of their own should not be made to feel as though the auditor is trying to "stump" them. An open dialogue between the auditor and the IT staff will build mutual respect and trust, especially if the auditor can educate without condescension.

***The auditor understands the NPO has no obligation to allow access to their networks, let alone heed any recommendations.*** In audit, the auditor identifies risk, and the success, failure, or absence of efforts to mitigate those risks is up to the enterprise (Fish, Interview with Warren Fish, Manager of IT Audit, ACI Worldwide, Incorporated, 2016). An NPO that does not employ an auditor on its paid staff may not see a reason to

allow an outsider to look at their networks. In this case, the auditor must show the value added to the NPO by the audit. Still, the auditor must accept the fact that they may have to walk away without conducting the audit, or that it may take a very long time to set up.

### 3.2.2. Explain the audit process and propose audit objectives and end state

An administrator who has never worked in enterprise IT may be completely unfamiliar with what the audit process. In this situation, the auditor should take the time to explain the process carefully, perhaps by including the audit process in the formal presentation mentioned earlier. However the auditor chooses to cover the topic, they should provide the IT staff an opportunity to ask questions.

Once the IT staff is comfortable with the audit process, the next task is to propose the audit objectives and end state. Ultimately, these are for the IT staff to choose, not the auditor. That being said, an IT staff that only minutes prior learned what an audit entails may not know what constitutes a realistic objective or end state. As discussed earlier, achieving CSCs 1 – 3 is an achievable overall objective. Once the IT staff achieves first three CSCs, they can consider expanding their program to include CSC 4, *Continuous Vulnerability Assessment and Remediation.*

In addition to achieving certain Critical Security Controls, another valuable and achievable objective is to teach the IT staff how to conduct an audit. The length of time required for this could vary considerably based on many factors, such as the IT staff's technical proficiency, knowledge of security concepts, and familiarity with auditing tools. Of course, the auditor's ability to pass their knowledge and experience to others, as well as the IT staff's willingness and ability to learn new skills will also affect the outcome. In any case, train the IT staff by steadily shifting the balance of effort away from himself over the course of several audits, transitioning from conducting the first audit as he would for an enterprise customer to eventually acting as a consultant while the IT staff performs all aspects of the audit (including audit planning, report preparation, and presenting the results to management).

Audit objectives lead to end states, or conditions that exist when the objectives are successfully completed. Based on the objective of achieving CSCs 1 - 3, the end state would be that the IT staff will possess a network baseline. A baseline is a snapshot of the

network in a "known good" state. Subsequent audits measure deviation from that baseline (Hoelzer, D.; Enclave Forensics, 2016).

With regards to the objective of teaching the IT staff how to conduct an audit, the corresponding end state would be self-sufficiency in auditing their networks. Self-sufficiency increases the sustainability of the audit program and relieves the auditor from an open-ended commitment of time and resources. Self-sufficiency also empowers the IT staff to validate the effectiveness of their security controls in the event of a change in their network architecture or security posture.

### 3.2.3. Request a face-to-face meeting

The auditor should conclude the initial contact with a request for a face-to-face meeting to further discuss the proposal, and if the IT staff is interested, to schedule technical meetings and audits. As with any professional encounter, regardless of the outcome, the auditor should thank the IT staff for their time, and send a follow-up e-mail within 24 hours, recapping the discussion. If the IT staff agreed to a technical meeting, confirm the meeting time and date. If they declined the audit proposal, extend an offer to revisit the matter should they later reconsider.

## 3.3. Scheduling Meeting – Building the Overarching Plan

The scheduling meeting is a one-time event that is best conducted face-to-face, as it may require more time than is practical for a telephone call or email exchange. The scheduling meeting provides an opportunity to discuss CSCs 1 – 3 in more detail, gain an understanding of the NPO's information environment (network architecture, sensitive information, "normal" use, and written security policy), plan which controls the IT staff will use to achieve the CSCs, and build the timeline. The scheduling meeting is also an opportunity for the auditor to offer assistance to the IT staff not directly related to audit.

### 3.3.1. Offering assistance

The scheduling meeting will cover many topics, and the IT staff may reveal challenges or shortfalls in any of a number of areas. The auditor might be in a position to help the NPO overcome these challenges, whether directly (e.g., by providing security policy templates and assisting in their revision to fit the NPO's needs), or indirectly (e.g.,

referring the IT staff to training materials that are available online for free). Regardless of the need, the auditor should take advantage of the opportunity to help the NPO. Doing so not only builds trust and goodwill between the two parties, it provides another way for the auditor to help a cause or organization in which they believe. The auditor should keep this in mind as the scheduling meeting unfolds, but the first order of business is to ensure the IT staff understands the CSCs it will attempt to achieve.

### 3.3.2. Discussing CSCs 1 – 3

If the IT staff is unfamiliar with the CSCs, the scheduling meeting allows the auditor to describe them in detail and explain how each one contributes to network security. This understanding will be beneficial later in the meeting in helping select specific security controls, and also illustrates how achieving the CSCs can ultimately make the IT staff's job easier. For example, CSC 1 (*Inventory of Authorized and Unauthorized Devices*) calls for the use of both active and passive automated asset inventory discovery tools. As more organizations adopt Bring Your Own Device (BYOD) policies, accurate hardware inventories are increasingly difficult to maintain. Deploying a passive asset discovery tool as recommended by CSC 1 helps the IT staff maintain continuous situational awareness of what is connected to their network.

### 3.3.3. Understanding the network architecture

To plan an audit, the auditor needs to understand the network, both logically and physically. The network architecture will help inform what tests and tools to use during the audit. A network that is run entirely over Ethernet does not require an assessment of wireless encryption standards, although it would still be wise to test for unauthorized ("rogue") wireless access points. The architecture also can impact *how* an audit is conducted; assessing security in a virtualized environment is not the same as in a traditional physical network (Dharmalingam, Smalov, Shivashankarappa, & Neelamegham, 2013).

Network architecture can provide a layer of defense in the form of segmentation, but only if the architecture is informed by how the NPO's sensitive information is processed and stored. Understanding how the NPO processes sensitive information requires an understanding of what information they consider sensitive.

### 3.3.4. Identifying sensitive information

The auditor and the IT staff must come to a shared understanding of what information is considered sensitive, where that information resides, and how it transits the network. Any organization with paid employees will handle PII at some level. Social Security numbers, contact information, and bank account information are needed to ensure staff members get paid. Other information, such as employees' spouse's names and perhaps even their children's names and schools may be processed on site, and can be used against the organization in a spear phishing campaign.

Once the NPO identifies its sensitive information, they can bin it within a data classification standard. This standard does not need to be overly complex. Data can be classified by type, or as simply "Sensitive" and "Routine." The advantage of applying a data standard is that it can help the IT staff segregate the network more efficiently and allow them to focus security controls where they are needed most.

### 3.3.5. Written security policy

To help protect its sensitive information, the NPO may have already implemented written security policies. If so, the auditor should include compliance with these policies within the scope of the audit. Written policies (an administrative control) are as essential to security as a firewall (a technical control) and may be effective or ineffective depending upon the manner in which they are implemented and enforced (Northcutt, 2009). In the complete absence of written policy, the IT staff may not know which policies might be most useful. In general, an Acceptable Use Policy (AUP), a Mobile Device Policy, a Bring Your Own Device (BYOD) Policy, and a policy for handling sensitive information are a good start. The SANS Security Policy Project (http://www.sans.org/security-resources/policies) has templates that the NPO can then customize to fit their needs.

### 3.3.6. Determine "normal" network use and activity

Understanding what constitutes "normal" network use is valuable to both the auditor and the network owner. Knowing what is normal helps identify what software the NPO needs to conduct its business. Unnecessary software should be deleted (if possible) or at least disabled, and the remainder will form the basis of the application

whitelist needed to achieve CSC 2 (*Inventory of Authorized and Unauthorized Software*) (Center for Internet Security, 2016).

### 3.3.7. Selecting appropriate security controls

Once the auditor and IT staff agree upon objectives and understand the information security environment, the IT staff can decide what security controls need to be implemented to achieve the CSCs. Two important caveats need to be made here: First, the IT staff may already have some of the required controls in place. For example, they may already require the use of client certificates (CSC 1). Second, and perhaps more importantly, the NPO may not have the means to implement all parts of a given control, or it might simply be too impractical for them to do so. For instance, in a BYOD environment, it is reasonable to assume that operating systems could change without notice. A constantly changing operating environment makes it very challenging to establish standard secure configurations for every OS and software application in accordance with CSC 3 (Center for Internet Security, 2016). In this example, the auditor may need to work with the IT staff to devise creative ways to mitigate the risk of not implementing this part of the CSC, perhaps through the use of virtual private networks in conjunction with careful network segmentation. Ultimately, the auditor must keep in mind that it is the NPO management's decision whether or not to accept risk.

Note that any control requiring a purchase may result in potential delays if the IT staff needs to request authorization. This is another reason to consider open source solutions whenever possible. After deciding which controls to implement, the auditor and IT staff should be able to begin putting together a timeline.

### 3.3.8. Building the timeline

The auditor and IT staff should not attempt to build the timeline with much fidelity beyond completing the current CSC. In other words, the CSCs are to be achieved sequentially; when the audit process starts, the IT staff will be working to achieve CSC 1. Each CSC will require time to implement the necessary controls, conduct an audit to validate their effectiveness (and identify residual risk), with retests as required. Each CSC may require multiple iterations of this process, especially if the NPO's budget prevents the IT staff from implementing all of the required sub-controls at once. Since

there is no way of knowing how many iterations it will take to achieve each CSC, the timeline should consist of "best estimate" placeholders for later CSCs. As the process matures, the auditor and IT staff will likely develop a more accurate sense of the time required to achieve each CSC. Once the auditor and IT staff build the timeline, planning for the next audit can begin. The first step for each audit is to conduct a technical meeting.

## 3.4. Technical Meetings

The technical meetings, held between the auditor and the NPO's IT staff, are used to plan individual audits down to specific "tactical" details. Holding separate technical meetings for each audit facilitates the modular approach, allows both the auditor and IT staff to frequently review the short-term objectives, which helps ensure continued progress towards the overall goal. Multiple technical meetings also help in keeping all parties focused on the requirements of the immediate task at hand. Finally, by including a separate technical meeting for each audit, the IT staff has more examples of how audit planning fits holistically into the audit process.

### 3.4.1. Review the audit objective and end state

Since each audit is intended to accomplish a limited objective in support of the overall objectives of accomplishing CSCs 1 – 3, each technical meeting should begin with a review of the specific objective for the audit in question, and its resulting end state. For instance, the first audit will be conducted after the IT staff has implemented at least some part of the security controls used to achieve CSC 1. Assuming the IT staff has deployed an automated asset inventory tool and used it to build a preliminary inventory of systems connected to the network, the audit objective could be to validate that inventory. The end state from this objective would be that the IT staff is using an adequate asset discovery tool, possesses an accurate hardware inventory list, and most importantly, can be certain no unauthorized devices are connected to the network. The hardware inventory list can then be used to produce an accurate network map.

### 3.4.2. Identify "no scan" systems, directories, and files

After reviewing the audit's objectives and end state, the next step is to identify which parts of the network the auditor cannot interact with, i.e., "no scan" areas. There

are many reasons to declare a "no scan" area. There may be directories or files containing sensitive information that the auditor has no legitimate need to access. Audit duration may be a factor; some scans can be very time consuming and may take more time than the auditor or IT staff can spare. Operational risk can also drive "no scan" decisions; certain hosts may be declared "off limits" due to fear that a scan may cause a critical system or service to crash. Ultimately, exclusion decisions belong to the NPO IT staff, since it is their network.

In reality, these exclusions should not pose a significant problem to the auditor. While it may be ideal to test every inch of the network and data, it is often unnecessary, and in many cases impractical, especially for a single auditor. If the network is made up of a variety of operating systems, tests can be run on just a representative sample of each OS, the size of the sample being agreed upon in advance by the auditor and the IT staff. Relying on a sample to provide a representative "snapshot" assumes desktop and server configuration control is consistently applied by the IT staff and cannot be subverted by the users. Should the end users be able to install unauthorized applications, the auditor and IT staff will need to reassess the number of desktops they need to examine. (In fact, configuration control is a large part of CSC 3 and will need to be evaluated separately (Center for Internet Security, 2016).)

### 3.4.3. Determine which tests and scans will be run

After establishing the physical and logical boundaries for the audit, the auditor and IT staff must agree upon which tests will take place on the network. With regards to the objective of validating the preliminary asset inventory, an independent test needs to be conducted to assess the security control used to produce the inventory. Discrepancies could be resolved with a walk-around of the facility to perform a physical inventory, so long as the computers on the inventory are all located within the same facility.

Conducting a walk-around raises another, often overlooked aspect of security: physical security. Physical security controls are a key part of network security (National Institute of Standards and Technology, 2015). Physical security tests may range from social engineering to attempting to bypass physical security devices (e.g., picking locks). If the NPO's physical security controls are to be audited, it is essential that the auditor

and the NPO explicitly document the scope of the physical security tests. Also, if the auditor is going to conduct the physical security tests outside the presence of the NPO IT staff, an Indemnification Agreement (also known as a "Hold Harmless Agreement" or "get out of jail free letter") should be considered mandatory. An Indemnification Agreement protects the auditor from liability in the event their actions cause damage and should be signed (at a minimum) by the IT lead. The term "get out of jail free" comes from the Agreement's ability to help the auditor in situations where they are caught trying to "break into" the NPO facilities by law enforcement or other staff members who are unaware that the auditor has the NPO's consent. If the auditor has an example from their employer, it can be used as a template for the NPO audit. If the auditor does not have an example letter, there are templates available at sites on the Internet. Some sites, such as Lawdepot.com, offer free customizable templates (Sequiter, Incorporated, 2017). As with any written agreement, legal review is strongly advised.

### 3.4.4. Gain approval for assessment tools

Following agreement on which tests and scans to conduct during the audit, the next question is which tools will be used to conduct them. Refer once again to the asset inventory validated through the use of an independent test. The test is independent if it is conducted under the auditor's observation using a different inventory tool than the one that produced the initial inventory. The reason for using a different tool is to validate the effectiveness of the security control chosen by the IT staff to accomplish the inventory (in this case, an automated inventory tool). Using the same tool twice to get identical results merely shows that the IT staff performed the test the same way twice, perhaps doing so incorrectly both times.

In more general terms, choosing the "right" or "best" tool depends on many factors, such as familiarity with how the tool operates, tool cost, and risk to the network. This last factor is significant. Many security tools are capable of injecting a substantial amount of network traffic, potentially causing a denial of service or even crashing the network altogether. Tenable Network Security's Nessus vulnerability scanner even comes with a "safe checks" setting designed to avoid crashes, but enabling this feature is not a guarantee against adverse effects (Tenable Network Security, 2017).

After selecting the tools, the auditor should include the tool list in the audit plan documentation. Documentation holds both the auditor and the IT staff accountable for using only approved tools during the audit.

### 3.4.5. Determine what documentation to review

If the audit is to include a documentation review, the auditor and IT staff will need to agree upon which documents the auditor will be allowed to access. System and firewall logs, printed copies of security configuration files, procedural compilations ("run books"), and other security test documentation such as hardening guides can help paint a more accurate picture of the network's security posture. All documentation must be recent enough to reflect the current network configuration.

### 3.4.6. Schedule the audit

Once the auditor and IT staff have hammered out the details on the nature and scope of the audit, the only remaining questions are when the audit will take place and how long it is expected to last. Unlike an audit in an enterprise environment, the timing of the audit may require more flexibility. Since the audit is not a normal part of the IT staff's duties, it represents an increase in their workload. This is not just a matter of convenience; in some cases, there is a limit to the number of hours the IT staff is allowed to work every week (Henderson, 2016). If the administrator is already busy, the audit will have to wait. Also, the issue of risk to the network is again a factor. The IT staff may want to run network scans outside of normal business hours to lessen the impact of adverse effects. Finally, the auditor's availability must also be considered.

### 3.4.7. Determine the audience for the entrance and exit conferences and the final report

In audits conducted for enterprise IT, entrance and exit conferences attendees typically include the auditor, the system administrators, and the members of the business unit involved in the audit. The purpose of the entrance conference is to establish expectations for the audit, show management support, and gain buy-in from those responsible for the network segments being audited. The exit conference allows frank discussion of the audit findings in a group setting prior to the auditor's report to management (Hoelzer, D.; Enclave Forensics, 2016). In an audit of a small NPO,

business unit members may or may not want to attend either conference, and management participation is unlikely if the auditor did not engage them from the beginning of the process. Formal entrance and exit conferences seem awkward if only two or three people are in attendance, including the auditor. Still, it is a good idea to meet, even if the setting is not formally designated as a "conference." A scheduled meeting serves as a milestone in the audit process, which helps make the process repeatable.

## 3.5. Document the Scheduling and Technical Meetings and Get Approval for the Audit Plan

Following the technical meeting, the auditor should document his understanding of the agreed upon audit scope, including tests to be conducted and tools to be used. The auditor should also include any follow-on questions that arise after the meeting ends. This document should then be sent to the IT staff for their approval, providing them an opportunity to clear up any misunderstandings. Also, the auditor should provide a copy of the Indemnity Agreement for their signature. Once all questions have been resolved and the scope of the audit has been agreed upon in writing, the auditor has a plan he can use to perform the audit.

## 3.6. Conduct Research for the Audit

Research is done prior to many audits. Assuming the auditor does not work at the NPO, they might need to conduct more research than they would for an audit of their employer's enterprise. There are a variety of reasons to conduct pre-audit research.

### 3.6.1. Vulnerability research based on hardware and software

A small NPO may have vastly different network architecture than a large enterprise. An auditor for a large financial firm whose primary duties consist of performing audits on UNIX servers and enterprise-grade routers may need to do research to gain a better understanding of what to do when faced with a Windows Active Domain environment stitched together with routers and switches designed for Small Office-Home Office (SOHO) or consumer-grade deployments.

### 3.6.2. Research on tools needed to conduct audit

A large organization with a robust, mature audit program will more likely be better able to afford expensive enterprise-grade security tools than a small community service NPO. Using open source tools whenever possible will help keep costs down, making it easier for the NPO to sustain an audit program. As a result, the audit may be conducted using security tools the auditor has never used before. Regardless of the choice of tools, it is essential for the auditor to know how to use them, if for no other reason than to instruct the IT staff for their use in follow-on audits.

## 3.7. Conduct the Entrance Conference

As stated earlier, an entrance conference serves to formalize the audit process and make it more repeatable. The auditor should discuss how the audit will flow and review individual responsibilities with regards to the tests being performed. The meeting also provides a final opportunity for the IT staff to ask questions prior to the start of the audit.

## 3.8. Conduct Fieldwork

The audit fieldwork should be conducted as a "team effort" with the IT staff, regardless of who is physically sending commands over the network. As with an audit in an enterprise environment, discuss variations from standards or best practices with the administrator. Perhaps most importantly, the auditor should document all commands issued and the responses received from the network; this will form the basis for the audit report and will also serve as a template for future audits.

## 3.9. Preparing the Report

After fieldwork is complete, the auditor must write the report. The auditor should treat the report for the NPO as seriously as any report they would produce for their employer. The report should include findings (to include positive observations), along with recommendations to remediate the findings. The audit report will become an enduring "snapshot" of the network security posture at that point in time. It will demonstrate the potential value added by an audit program, acting as a template for future audits. Finally, it can serve as an action plan for the IT staff, giving them written justification from an objective source to ask for additional resources for network security.

## 3.10. Conduct the Exit Conference

Meeting with the IT staff to discuss the audit findings is beneficial in that it gives the opportunity for the IT staff to see potential security weaknesses in the context of the whole. For example, an audit where there are no Earth-shattering findings may leave the IT staff with the sense that the network is secure. That sense of security may be false if the audit report contains page after page of "minor" findings. To allow the IT staff time to digest the findings and prepare questions, the auditor should provide a copy of the report prior to the meeting (Hoelzer, D.; Enclave Forensics, 2016).

## 3.11. Reporting to Management

Unless the audit was originally requested by the NPO's management, the auditor has no mandate to provide a report to them. This may be particularly true for an initial audit, where the IT staff does not yet know how "bad" things are. (Still, the IT staff may have a better chance of getting management's support for security improvements if the auditor (an objective outsider) makes the report.) If the IT staff chooses, the auditor may be invited to give a report to the NPO management. When presenting to management, limit the report to an "Executive Summary" style presentation to avoid burying them in technical details.

## 3.12. Follow-up

Documenting risk is of no benefit if the audit report is ignored. As stated earlier, it is ultimately up to the NPO whether or not to accept or mitigate risk. Any decision not to fix a reported security deficiency represents a conscious decision to accept the identified risk. Any remediated audit findings should be retested to ensure efficacy. Once all findings have been accepted or remediated, the auditor and IT staff can begin the next iteration in the process, whether it be to take further action on the same CSC or move on to the next. To maintain momentum, the auditor should schedule the technical meeting for the next audit as soon as practicable after the IT staff is ready to proceed.

## 3.13. Lessons Learned

Conducting an audit presumes the IT staff (and possibly the NPO management) will come away from the event with lessons learned. This is certainly a desirable end

state after any audit, but the auditor should consider what *he* learned from the encounter. Perhaps his pre-audit research taught him the intricacies of a new security tool or piece of network equipment, or perhaps he will feel more confident the next time he is asked to perform an audit on a virtualized architecture. If nothing else, maybe the auditor learned something new about the NPO and its operations, and now has a greater appreciation for the organization he set out to help in the first place.

After the entire series of audits is complete, the NPO will have achieved CSCs 1 – 3, and the IT staff should be competent in performing audits without the auditor's assistance. This is a very real achievement for the auditor and IT staff, but there is one final measure of success: whether or not the newly-developed baseline is used to start a recurring audit program. If the program takes hold, the auditor should recommend periodic recurring audits either annually or after any significant change to the network architecture.

## 4. Conclusion

The size of the network and nature of the organization may inform the scope of an audit, but they do not have an impact on whether or not an audit program helps the network's security posture. In particular, a small NPO can derive the same benefit as a large enterprise, but small NPOs often lack the resources to establish an audit program. Rather than attempt to force an enterprise IT audit construct onto a small NPO, limited objectives and a more streamlined approach are necessary. The limited objectives are the achievement of CIS Critical Security Controls 1 – 3, which are sufficient to provide the NPO with a baseline to conduct future recurring audits, ideally without external assistance. The streamlined approach is taken from the SANS six-step audit process. All six steps are still used, but are tailored to what is relevant to the NPO.

This paper has taken these limited objectives and streamlined approach and built them into a repeatable framework for auditors to use in helping an NPO build a sustainable program to strengthen their network's security posture. The framework walks through the audit process: initial contact, planning the audit through discovery of the NPO's information environment, scoping the audit, conducting fieldwork, and finally reporting and follow-up. This framework is made feasible for small NPOs through the

use of modular scheduling. Rather than attempting a single, comprehensive audit, multiple smaller audits are conducted over an extended period. Using this approach, a volunteer with the right knowledge can give back to their community or serve a cause in a way that perhaps they never expected – by helping protect sensitive data from would-be hackers.

# References

Boys Town. (2017, January 1). *About Boys Town*. Retrieved from Boys Town Web site: http://www.boystown.org/about/Pages/default.aspx

Center for Internet Security. (2016, August 31). *Center for Internet Security Critical Security Controls for Effective Cyber Defense (Version 6.1)*. East Greenbush, New York: Center for Internet Security.

Center for Internet Security. (2017, January 19). *Welcome to the CIS Controls*. Retrieved from Center for Internet Security Web site: https://www.cisecurity.org/critical-controls.cfm

Dharmalingam, R., Smalov, L., Shivashankarappa, A., & Neelamegham, A. (2013, April). Information Security Audit in Virtual Environment. (A. Daoud, Ed.) *The Research Bulletin of Jordan ACM, II*(III), pp. 132-136. Retrieved February 25, 2017, from http://ijj.acm.org/volumes/volume2/issue3/ijjvol2no36.pdf

Fish, W. (2016, December 15). Interview with Warren Fish, Manager of IT Audit, ACI Worldwide, Incorporated. (C. Jarko, Interviewer)

Fish, W. (2017, February 13). E-mail from Warren Fish, Manager of IT Audit, ACI Worldwide, Inc. (Subject: Audit Timelines). (C. Jarko, Interviewer)

Gelbstein, E. (2015). *IS Audit Basics: Auditing Small IS/IT Organizations: When is an IS/IT Organization small?* Retrieved from ISACA Web site: http://www.isaca.org/Journal/archives/2015/Volume-4/Pages/auditing-small-is-it-organizations-when-is-an-is-it-organization-small.aspx

Girls Incorporated. (2017, February 4). *About Girls Inc.* Retrieved from Girls Incorporated Web site: http://www.girlsinc.org/about/about-girls-inc.html

Henderson, L. (2016, December 5). Interview with LaVelle Henderson, Chief Information Officer, Boys and Girls Clubs of the Midlands. (C. Jarko, Interviewer) Omaha, Nebraska.

Hoelzer, D.; Enclave Forensics. (2016, 2nd Quarter). 507.1 - Effective Auditing, Risk Assessment, and Reporting. *SANS AUD507 - Auditing & Monitoring Networks, Perimeters, and Systems*. Bethesda, Maryland: The SANS Institute.

Christopher Jarko, csjarko@yahoo.com

International Organization for Standardization. (2017, February 16). *ISO 31000 - Risk Management*. Retrieved from ISO Standards: http://www.iso.org/iso/home/standards/iso31000.htm

International Organization for Standardization. (2017, March 1). Standards Catalogue. Retrieved from ISO Standards: http://www.iso.org/standards-catalogue/browse-by-ics/htm

IT Policy Compliance Group. (2009). *Guidance for Best Practices in Information Security and IT Audit.* Cleveland: IT Policy Compliance Group.

Misenar, S., & Conrad, E. (2016, 2nd Quarter). 511.5 - Automation and Continuous Security Monitoring. *SEC511 - Continuous Monitoring and Security Operations*. Bethesda, Maryland: The SANS Institute.

National Institute of Standards and Technology. (2011, March). *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information Systems View.* Retrieved from NIST Publications Web site: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Institute of Standards and Technology. (2015, January 22). *NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved from NIST Computer Security Resource Center: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology. (2017, February 15). *NIST Computer Security Publications*. Retrieved from NIST Web site: http://csrc.nist.gov/publications/PubsSPs.html#800-53

Northcutt, S. (2009, September 1). *Security Controls*. Retrieved from SANS Technology Institute Security Laboratory Web site: https://www.sans.edu/cyber-research/security-laboratory/article/security-controls

O'Rourke, M. (2013, August 1). *The Challenges of Nonprofit Risk Management*. Retrieved February 26, 2017, from Risk Management Monitor: http://www.rmmagazine.com/2013/08/01/the-challenges-of-nonprofit-risk-management/

Sequiter, Incorporated. (2017, February 4). *Free Hold-Harmless (Indemnity) Agreement*. Retrieved from Law Depot Web site: http://www.lawdepot.com/contracts/hold-

harmless-agreement/?loc=US&pid=googleppc-indemn_us-indemnityT1_t1-ggkey_indemnification%20sample&gclid=CMLzrPLK99ECFQ6paQodGnEKFA#.WJfqF39K3Bm

Stewart, K. (2016, November 10). Interview with Keelan Stewart, Information Security Analyst at Boys Town. (C. Jarko, Interviewer)

Tenable Network Security. (2017, January 19). *Understanding the Nessus "Safe Checks" Option*. Retrieved from Tenable Network Security Web site: https://www.tenable.com/blog/understanding-the-nessus-safe-checks-option