White Paper

The Benefits of Incorporating Internal Auditing Consultants into Information Technology and Cybersecurity

Striving for an Audit-Ready Environment

January 12th, 2022

Amanda Higley, CISA, Sec+
Security Compliance and Policy Analyst

Company: M Powered Strategies
Socio-Economic Status: Small Business (under $15 Million); HUBZone Certified
Years in Business: 19 Years

Contents

Introduction

Executives of organizations, both private and public, are striving to make their IT environments more connected for customers and partners, while also balancing security needs. At the same time, almost every day there's a news story about a new vulnerability being exploited or another well-known company getting breached. Most of these organizations are aware of the several available security frameworks (i.e., the Federal Information Security Management Act (FISMA), and the Federal Risk and Authorization Management Program (FedRAMP), etc.,) that strive to steer them to a mature future state and prevent such security events. However, these frameworks require layering with other frameworks to guide effective risk management, cybersecurity implementation, and security controls. The challenge is further compounded by the flexibility and interpretability of many frameworks that allows them to adapt to varying IT and operational models. Flexibility is certainly a boon for any organization to have, but it does create a challenge of ensuring that each framework they use are in sync and work flawlessly together.

Combining the challenge of multiple frameworks with additional requirements for regulatory organizations (i.e., healthcare, government, and finance, etc.,) to participate in regular third-party IT audits, and the environment can become downright chaotic. Third-party auditing firms come in and out of your place of business for months at a time, bringing to light flaws within every facet of the business' critical programs, documentation and processes. Several audits may be going on at any given point within the fiscal year, and staff are continuously stretched to the max trying to manage those responsibilities, while also maintaining daily operational tasks needed to run effectively and compliantly.

To make matters more frustrating, some third-party audit firms are behind the curve of incorporating security expertise into their staff's repertoire, leading to an inability to understand and review the current security implementation effectively. Other firms may have the experience, point out the flaws that exist, but provide no insight as to how to address those flaws. It's no wonder then that the organizational staff begin to feel frustrated and stressed out when the same issues are consistently pointed out over and over again, resulting in fraying relationships between IT security and audit personnel and audit findings piling up for months or even years into the future. Ironically, it seems, the more audits, the less secure organizations become over time.

All of the above are common issues that MPS has seen first-hand. We have found that such issues can be addressed with the continuous inclusion of personnel who are well-versed in cybersecurity and IT Internal Audit. When such personnel are incorporated into the everyday business environment at any given frequency, expertise is on-hand to ensure the alignment of business processes with management and IT security goals, but also with the regulatory compliance standards such organizations must answer to.

Internal Audit – Are they Partners or Just More "Police"

In theory, the relationship between Internal IT Audit and IT security professionals should be complementary in that both Internal and External IT Auditors would be there to provide the appropriate testing IT Security needs to continuously ensure programs and processes are consistently working effectively and at the peak levels of maturity. IT Security focuses on designing and implementing the security plan and the internal IT Audit effectively tests that plan continuously so that the kinks are worked out. However, the relationship between these two groups can become less than harmonious for a variety of reasons, most of which stem from the perception that internal auditors are simply there to act as the "police officers" of compliance who would simply turn the environment upside down instead of effectively helping to make the environment more secure. The discord can be heightened when an organization begins to face an array of cybersecurity reviews in a short time frame that result in multiple findings for the same items consistently being identified. The policing is then perceived as redundant and excessive. Over time, this type of acrimonious relationship can inhibit the organizations' goals to have secure programs implemented and instead leads to remediation efforts that simply "check the box."

However, the perception of Internal Audit is improved significantly when IT Security viewed the Internal Auditing staff as partners in ensuring that security improvements were gained (Steinbart, Raschke and Gal, Internal Audit's Contribution to the Effectiveness of Information Security, Part 1 - Perceptions of Information Security Professionals). The problem to be solved then, is how to get IT audit professionals to be seen as partners with the IT security staff? The solution comes when IT Security Professionals understand the benefits that Internal Auditing personnel can provide when incorporated into the organization's day-to-day operational environment. This white paper explains the key benefits that occur when Internal Audit is incorporated into an organization's environment and how the partnership can grow to provide value and maturity to the IT environments' programs and processes.

The Benefits of Internal Audit

To assist in assessing the IT Security's and Internal Audit's perception of value, the Information Systems Audit and Control Association (ISACA) comprised a 3-year interview and survey period where both IT Security Professionals and Internal Auditors were asked about their views on their relationship with each other and what factors each viewed as being a main factor for their viewpoints. The survey flagged 2-key components supporting the argument for an Internal Audit program:

- There was an increased perception of improved value that occurred when Internal Auditors had technical expertise themselves; and,
- An increased perception of maturity benefits to organizational programs and processes when Internal Audits were conducted regularly

On the whole, both groups validated the belief that incorporating Internal Audit activities into an organization's cybersecurity activities provided tremendous benefit over the course of program development and implementation. Those benefits were expressed to be found across all levels of an organization; from the managerial and Board member level, all the way through the supportive personnel responsible for implementing those mission and business critical processes.

Value of Auditor's Technical Expertise on Audit Remediation Efficacy

Organizations gain tremendous value from audits when they are conducted by professionals who understand the IT Security implementations sufficiently enough to audit them properly (Steinbart, Raschke and Gal, Internal Audit's Contribution to the Effectiveness of Information Security, Part 1 - Perceptions of Information Security Professionals). Identifying problems, (i.e., "findings") is the focus of standard audits, but developing effective remediation plans that resolve security issues is the overall goal. In order for this effort to be effective, auditors must thoroughly understand the issues that were found and the root causes of those findings, then effectively. Failure to document findings clearly can plague the IT Security Personnel's efforts to define remediation efforts, resulting in frustrating and contentious meetings, longer remediation timelines, and/or remediation packages that are rejected numerous times by auditing teams.

Alternatively, having Internal Auditory staff with IT Security expertise allows for a better "translational" activity to occur: third-party audit findings can be digested by an organization's staff in a more palpable way. Findings can be thoroughly researched from the audit's perspective, cross-checked with other audits that might overlap with the subject matter and then the synopsis of those findings can be communicated more effectively to the IT Security Personnel using the same language and terminology. This decreases the number of possible misunderstandings during the remediation efforts. The "cross-checking" and improved communication allows projects to be thoroughly planned out to not just incorporate the updates that were necessary for business operational value, but to also address any past audit issues at the same time. These audit personnel can also consult throughout these projects to ensure that the new solution addresses those findings effectively.

Internal Audit at any Frequency Improves Cyber Maturity Gains

The secondary benefit discovered during ISACA's 3-year survey period stemmed from questions IT Security Professionals were asked about the perceived value add of audit at varying frequencies. The data showed that there was a higher perception of value add when Internal Audits were conducted, in general. But the value was further increased when audits occurred at an increased frequency as referenced in the questions IT Security Professionals responded to on the subject. They stated that it was believed that in such cases when Internal Auditing occurred at higher frequencies, improvements were made continuously throughout the cybersecurity environment at all levels of the programs' lifecycle (i.e. planning, development, implementation, etc.) (Steinbart, Raschke and Gal, Internal Audit's Contribution to the Effectiveness of Information Security, Part 1 - Perceptions of Information Security Professionals). In doing so, organizations found that having compliance baked in at earlier stages demonstrated higher maturity scores when external auditors came to call (Protivti Knowledge Leader).

MPS has observed that Internal Audit activities at any frequency can also assist the organizations past year audit remediation efforts, although incorporating continuous Internal Auditing is the more favored option. The value to the organization grows enormously when Internal Audit occurs continuously, and proper gap analysis occurs continuously *within all facets of the organization's processes*. security and audit staff members approach leadership with insights as to the commonality across findings and determine the most effective path for remediation while ensuring that all projects are consistently incorporating future audit concerns and progressing toward a future state.

Programs and Processes are made "Audit Ready"

The benefits of Internal Auditing personnel can also be found when they assist the organization from an "audit readiness" point of view. There are numerous frameworks that are used as guideposts – some of which were mentioned in the introduction of this paper (i.e., FISMA, FedRAMP, etc.). Typically, these frameworks are to guide organizations through the process of building of their programs with the incorporation of minimum security controls needed to accomplish business processes. However, incorporating third-party audit requirements of proving implementation and efficacy of those controls are not typically at the forefront of managerial considerations.

With this in mind, Internal Auditors who are involved at every facet of an organization's program-building process can apply their consulting services early on by informing them on what their clients need to be audit-ready, not just to ensure efficient operability of the business itself. This ensures that the organization is already aware of how a given process' implementation must be documented effectively at all stages of the program/process' development. This preparation flows into the audits itself, in that organizations already have the necessary documentation and proof of implementation in hand and ready for third-party auditors, thus ensuring a less-contentious, more efficient audit period.

MPS' Approach to Internal Audit and Audit Management

The Internal Audit and Audit Management capability at MPS allows our staff to be in the trenches with our clients, ensuring effective support for all functions of program management from an integrated cybersecurity and audit readiness approach. We strive to ensure regulatory organizations create programs and processes that not only incorporate the best cybersecurity techniques, but also support the organization's desire to incorporate an audit-ready functionality. This approach ensures that all applicable regulatory frameworks are thoroughly assessed, analyzed, communicated and incorporated into programs and processes at every stage of development. Communication with the client's management and key security personnel are maintained at every stage of program development as well so that solutions are nimble and flexible enough to change without much overhead, while still maintaining the key regulatory compliance requirements needed to maintain maturity scores.

This approach is specifically designed to ensure that organizational management and Board members can worry less about upcoming auditory requirements as more programs incorporate this approach simply because they can be assured that audit frameworks (i.e., FISMA, FedRAMP, etc.,) have already been incorporated into the program's foundation. Previous years' audit findings are also assessed and incorporated into ongoing project improvements so that those efforts can be remediated efficiently. Once programs/processes are ready to be approved by management, our MPS' audit experts give it a thorough review so that only the most effective programs and processes are provided for managerial review and approval for implementation. Over time, this approach drives the continuous decrease of previous audit years' auditory noise while ensuring that more efforts are put into the preparation for upcoming audits. Third-party audit findings, therefore, become more focused on confirming the remediation of issues that the organization is already aware of and reviewing the provided proof of its efforts to address those issues.

How does MPS maintain this audit-ready mindset? Our experts maintain their focus on ensuring that compliance is at the forefront of creating mature programs and processes. We are constantly attuned to audit framework changes so that the most up-to-date information is used, communicated, and incorporated into our clients' deliverables before external auditors come in to assess. We also ensure that we maintain strong relationships with our client's leadership and IT Security experts so that all deliverables are in alignment with the business' mission, business, and security requirements. Processes for the maintenance of these deliverables are also built into each program so that updates can be incorporated quickly and efficiently as needed. This entire effort ensures continuous compliance with the audit frameworks of the day while steering the development of strong, implementable cybersecurity deliverables into the client's environment.

Over the course of a 3 year period, a staff member with cybersecurity and auditing expertise was incorporated into a client's IT Operational environment. That individual, was able to inject several Internal Audit activities into the client's environment, ranging from Contingency Planning and Business Continuity, Risk Management, and FISMA-facing Policy and Procedure creation. This effort assisted the organization in accomplishing the desired maturity gains across several internal self-assessments. That preparation allowed the organization to ensure major achievements during the FY2020 and FY2021 FISMA Audit periods. During this period, the client's FISMA domain scorings increased from Levels 2 "Defined" and Level 3 "Consistently Implemented" to FISMA domain scores of Level 4 "Managed and Measurable" for 7 out of 8 domains. The final domain was also well on its way to receiving a domain score of Level 3 "Consistently Implemented" in its upcoming FISMA audit period. In order to ensure the organization continued on that path, MPS provided them with more detailed activity plans that would ensure the client's domain would join the other 7 domains at the Level 4 "Managed and Measurable" status in future audit years.

Within Audit Management, MPS was able to assist the client throughout each step of their external audit finding remediation efforts, from the creation and management of the activities detailed in approved Corrective Action Plans, to the creation of the audit remediation package itself, all while ensuring effective communication occurred throughout the process. This improved communication and process facilitation allowed for greater understanding of the changes that needed to occur, the reasons for those changes, and the most effective way of completing those changes. As a result, the organization's audit finding closure increased rate by 70% over the course of that single year. Imagine what MPS' audit experts could do for your organization!

About M. Powered Strategies

M Powered Strategies (MPS), a HUBZone Small Business, is a management consulting firm focused on planning and executing mission-driven organizational change and driving organizational effectiveness. Our agile, highly collaborative approach empowers clients to articulate their strategic vision, build their organization to support the mission, align program objectives to measurable outcomes, and improve business processes. MPS serves clients by producing lasting tools, processes, and deliverables that provide value to our clients and their stakeholder organizations over time.

MPS has served as trusted advisors via long-term program management support to high-profile change initiatives within the Departments of Veterans Affairs (VA), Health and Human Services (HHS), Agriculture (USDA), Energy (DOE), Commerce, and the Federal Retirement Thrift Investment Board (FRTIB) over the past 15 years. Our company looks forward to empowering your organization with your Program Management and/or Internal Audit and Audit Management Servicing needs.

Delivering Excellence to Our Clients

- **Continuous Improvement:** We design sustainable solutions for our clients through iterative improvement to leave lasting impact.
- **Service-Oriented Approach:** We have specialized expertise in facilitating groups and enabling organizational change through effective communication and stakeholder engagement.
- **Proven Success:** We have applied our frameworks in support of high-visibility projects at various Federal Agencies.
- **High Quality Delivery:** Our QMS processes are ISO-9001 Certified**.**
- **Dedication to Public Service:** Our delivery teams bring passion and energy to work with our clients to solve their most challenging problems and to build and develop their organizations.

References

Protivti Knowledge Leader. *KnowledgeLeader*. 9 June 2017. 29 November 2021. <https://info.knowledgeleader.com/what-is-internal-audits-role-in-cyber-security>.

Steinbart, Paul John, et al. "Internal Audit's Contribution to the Effectiveness of Information Security Part 2 - Perceptions of Internal Auditors." *ISACA Journal* (2014).

—. "Internal Audit's Contribution to the Effectiveness of Information Security, Part 1 - Perceptions of Information Security Professionals." *ISACA Journal* (2014).