Whitepaper: IT Audit Readiness – The Federal Agency Journey

Cecil Dildine, PMP, CISM, CSM/CSPO, ITIL, ZT

Introduction

Both U.S. defense and civilian agencies must undergo independent audits to demonstrate compliance with federal information technology (IT) audit controls contained in guidelines such as Federal Information System Controls Audit Manual (FISCAM), Federal Information Security Modernization Act (FISMA), Statement on Standards for Attestation Engagements (SSAE), Financial Improvement and Readiness Guidance (FIAR), and National Institute of Standards and Technology (NIST) guidance as well as other federal audit and general federal IT controls. Agencies often struggle to achieve a state of readiness for these audits as a means of minimizing IT findings, improving FIAR compliance, and gaining an understanding of options for remediation of IT findings resulting from the audit.

Achieving an unopinionated (i.e., "clean") audit is a long journey for any organization, and progress can only be made at a pace the organization can absorb and accept. Most organizations start with reactive tactical remediation of deficiencies found by the external auditor and ultimately will reach maturity when they are proactively self-identifying and robustly implementing sustainable solutions as part of normal business operations.

A recent article sums up the benefits of auditing thusly:

> Financial auditability helps … to not only comply with laws, but also helps improve business processes, increase data reliability, make better use of resources, and enhance public trust to drive operational readiness. Financial statement audits aim to reduce risk from waste, fraud, and abuse by identifying improvements to internal controls, by validating that processes are operating as intended.

Background

IT audits trace their origins to circa 1970 when technology became an integral part of the workplace. The conduct of IT audits and the skill requirements of IT auditors have grown in sophistication since their early origins. Today, IT audit objectives are threefold. First, verify that IT systems, related infrastructure, and organizational policies and procedures comply with legal and regulatory requirements. Second, ensure that data is secure and that employees comply with security protocols. Third, perform vulnerability assessments and recommend means of mitigating risks.

Specialists, known as IT auditors, perform the assessments of an organization's IT infrastructure guided by the three objectives above. Frequently, the specialized auditors who perform these reviews are employees of Independent Public Accounting (IPA) firms.

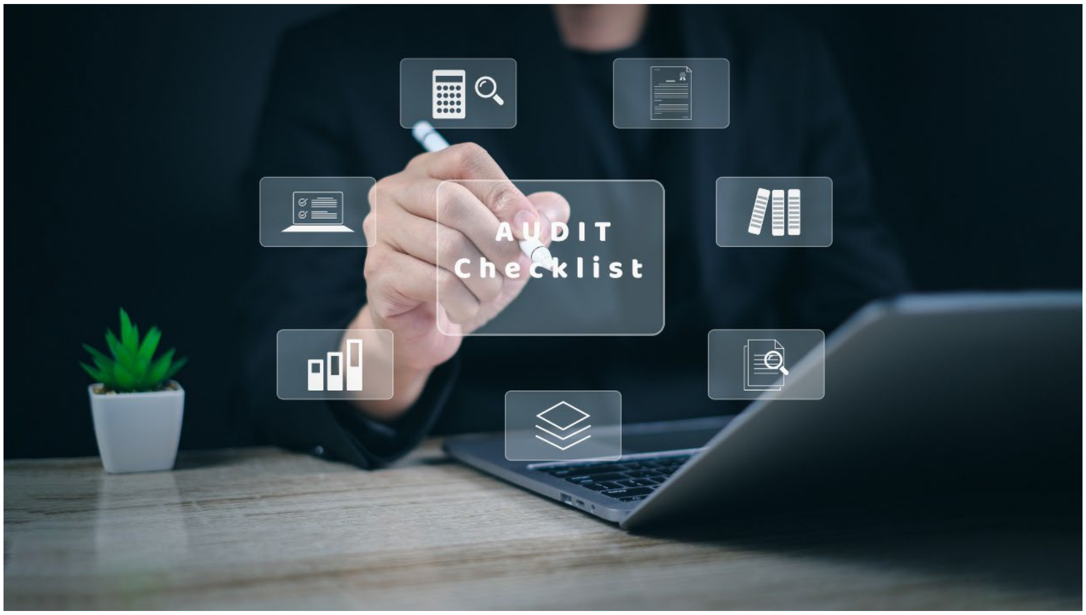
Compliance audits compare actual practice to governing criteria, identify gaps, and offer recommendations. Conversely, program effectiveness or performance audits seek to determine whether a program actually achieves the objectives for which it was created. More and more, this distinction is diminishing, and IT auditing seeks to incorporate both elements.

As if the sheer number of governing documents – and IT audit controls specified within – were not enough, the areas where IT governance is demanded is equally diverse. Agencies must address issues associated with cybersecurity, cloud migration and operation, and technology resilience, among many others.

Federal Agency Challenges

Federal agencies encounter three main challenges when facing the prospect of undergoing an IT audit:

1. Readiness for IT audit.
2. Resolution of IT audit findings and/or deficiencies in a timely and comprehensive fashion.
3. IT audit posture, specifically transitioning from a reactive to a proactive stance when it comes to deficiency identification and resolution.



More and more, federal contractors with expertise in these requirements are helping agencies meet these challenges. Electrosoft's experience demonstrates three key lessons learned:

1. Agencies need to embrace IT audits as an integral part of their normal operations.

2. An audit readiness Project Management Office (PMO) is a necessity. The PMO should possess authority for and accountability over setting standards, policies, and procedures; creating standard templates; training staff; and creating a single, authoritative, centralized solution reporting progress ("one version of the truth") for audit readiness, response, and reporting. In so doing, agency leaders are able to track progress, ask targeted questions, and make informed decisions.
3. Action officers with distinct responsibility for specific internal controls must be assigned and held accountable.

Relative to #1, audits are not a "one and done" event. Audit frequency is determined by law (e.g., financial statement audits are annual events) and regulation. Staff may ask: "We just did this last year, why are we doing it again?" That is why it's important for leaders to communicate to staff the ongoing nature of IT audits and the need for them to be knowledgeable of and compliant with external and internal requirements and processes.

In the final analysis, auditing is a risk management function that seeks to reduce agency jeopardy by assuring that effective controls are in place. Further, agencies operate in a dynamic environment, especially regarding changing guidance. Vigilance is imperative, especially when cybersecurity is at issue.

IT Audit Readiness

One of the key tasks relating to IT audit readiness involves possessing the requisite documentation and gathering it for auditor use. IT auditors require access to the full range of documents in order to evaluate the effectiveness and efficiency of IT controls and compliance with them.

The central tenet of an IT audit is: trust and verify. Auditors must "see" something to believe it exists. They also need to document evidence. Without being able to compare what they "see" against documented processes, procedures, and criteria, they cannot establish that controls are being consistently and correctly applied.

There are four categories of documentation that federal agencies must compile in preparation for an IT audit:

1. An inventory of all the certified and accredited systems (and data) that are part of the agency's business process.
2. Applicable laws, regulations, and other requirements, including general and application controls, risk assessments, manuals, standard operating procedures, memoranda of understanding, service-level agreements, cycle understandings, roles and responsibilities, flowcharts, system diagrams, audit trails, reports, and any other IT-related artifacts that are considered part of the system business process.
3. Agency-specific policies and procedures implementing the applicable laws and regulations in #2 as well as other necessary internal controls.
4. IT control documentation. FIAR guidance, for example, recommends IT control documentation that specifies each control, who performs the control, the frequency of review and approval, and evidence substantiating that the control was performed in accordance with written policies and procedures.

Compiling the above-listed documents can be cumbersome – and problematic in agencies where they don't already exist. An experienced federal contractor can assist agencies in establishing baselines, developing procedures, and creating material to ensure best practices and compliance with relevant guidelines in FISCAM, FISMA, SSAE, FIAR, NIST guidance, OMB A-123 Internal Controls, and other federal IT controls. Likewise, experienced contractors can review evidential matter (EM) for accuracy, completeness, and effectiveness concerning the specific IT control it seeks to satisfy. Beyond this aspect, contractor review can evaluate whether the EM package is written in such a way that an IT auditor can readily understand the material and apply it. If not, the contractor can be invaluable in coordinating the changes needed to make the EM intelligible.

Remediation

In the course of auditing and post-audit, the IPA will issue a Notice of Findings and Recommendations (NFR). This document details audit-identified issues and recommended corrective measures. The NFR can communicate issues related to business processes, access control/user access, configuration management, security management/contingency planning, software development, and segregation of duties. Agency management, in response, is expected to develop a Corrective Action Plan (CAP) that delineates the actions it plans to implement to comprehensively address and correct the identified issues and instances of noncompliance or underperformance.

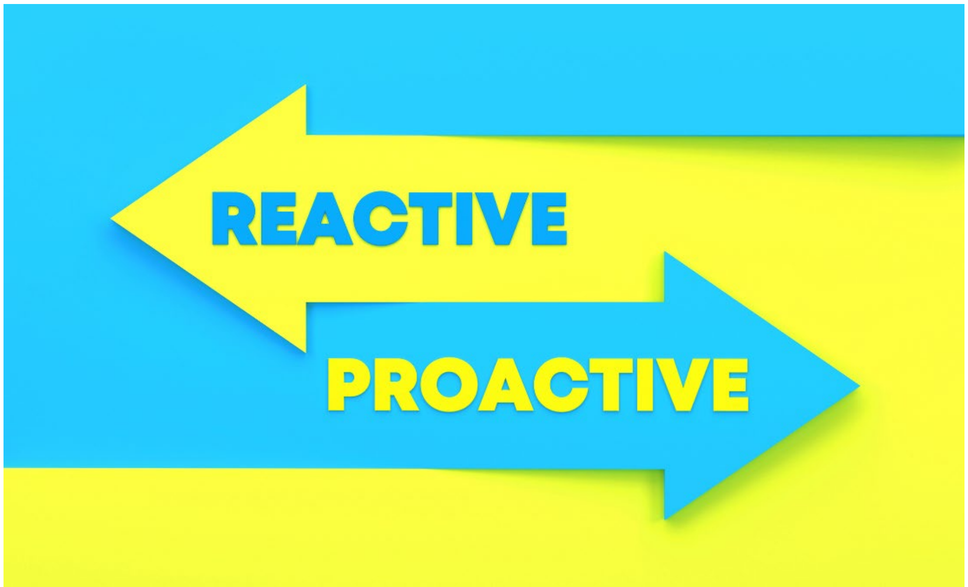
Here, a federal contractor can assist CAP development via root cause analyses that discern the contributing factors underlying the identified deficiencies. Contractor expertise often yields an unparalleled understanding of how best to address specific control scenarios. For example, based on experience, contractors are frequently aware of common high-profile risks that many federal agencies share. This knowledge facilitates advance identification of risks and development of strategies to mitigate them. In the process, an experienced federal contractor might even discern ways to prevent future deficiencies.

Simply developing corrective actions responsive to identified deficiencies is only half of the equation. Tracking timely and complete implementation is yet another challenge confronting agencies. As stated previously, a PMO or similar agency entity must create a single, authoritative, centralized progress-reporting solution that encompasses audit readiness, remediation, and reporting.

The bottom line is this: auditors rarely reach findings that are unknown to an agency. It's important for the agency to demonstrate awareness. Being able to say "We know the issue exists from our testing, we've reviewed it, and we're managing it" can go a long way toward preventing audit findings. Most important, it indicates an important step toward agency maturation relative to IT audits.

Transition to a Proactive Posture

The ultimate goal of every federal agency subject to IT auditing is to eventually receive clean/unqualified audit opinions. Achieving this objective on a consistent basis requires a fundamental agency shift from being reactive to proactive in its posture toward IT audits. While such a journey is replete with challenges, an experienced federal contractor like Electrosoft is an able Sherpa on the pathway to IT audit readiness and beyond.



Such a transition first demands standardized audit life cycle operating procedures developed in collaboration with stakeholders. Further, stakeholder implementation cannot be left to chance. A rigorous program incorporating staff training, monitoring, accountability, and regular reporting is necessary, supplemented by high-level root cause analysis and CAP processes. Again, an experienced federal contractor can be invaluable in designing and implementing such programs.

Here again, the use of a centralized performance tracking and reporting solution is essential to the transition. So, too, is the development of a Risk Control Matrix that includes all relevant IT General Controls and Business Process Application Controls. Notably, matrix development supports best practices delineated in OMB Circular No. A-123 and other key documents.

Targeted performance metrics play an essential role in driving continuous improvement. By reporting metrics to agency officials on an ongoing basis, they gain the ability to make the adjustments needed to achieve improvements and limit/eliminate audit findings.

Another big challenge is moving at a pace the organization can accept. Sometimes, the impulse is to move as fast as possible but, like Kübler-Ross' five stages of grief, agencies must move through the five stages of change. At first there will be denial and anger, then negotiating and depression, and finally acceptance. Incorporating standardized audit readiness processes and procedures ahead of time is beneficial as it affords the opportunity to train staff. It's also important to remember that every agency has a mission and it's not to do audits. The agency must remain effective in discharging its mission while moving toward IT audit readiness.

The most important objective of all is achieving culture change within the agency, especially at the leadership level. Having a performance database (i.e., one that tracks how many open CAPs there are, how many open findings there are, and how long they've been open) can be meaningless unless the agency culture demands attention be focused on resolving findings in a timely manner. Leaders must help the organization mature its automation and build processes and procedures to a point where continuous testing, control management, and risk management become part of the organization's DNA.

Electrosoft as an Industry Leader in IT Audit Readiness and Beyond

For nearly a decade, Electrosoft has successfully supported federal agencies in efforts related to IT system audits, specifically audit readiness. Our reputation has made Electrosoft the contractor of choice to support other audit processes including the Annual Statement of Assurance risk assessment, quarterly system reviews, and preparatory efforts for financial statement audits. Electrosoft also has expanded its focus to include support of enterprise Segregation of Duties auditing for applications as well as internal audit requirements.

Contact Us

To learn more information about Electrosoft and our capabilities, contact us at info@electrosoft-inc.com.

About Electrosoft

Electrosoft delivers comprehensive technology-based solutions and services that propel mission success for federal government customers. Specializing in cybersecurity, Electrosoft supports civilian and defense organizations in advancing cybersecurity postures, achieving digital transformation, and adopting agile approaches to improve operational efficiency and security. Recognized for deep domain knowledge and mature management practices, the company is rated at Maturity Level 3 for CMMI-DEV and CMMI-SVC and is certified under ISO 9001, ISO 20000-1, and ISO 27001. The company is headquartered in Reston, Virginia. www.electrosoft-inc.com.