A Cooperative Model for Security, Audit, and Risk:

A Collaborative Approach to Risk-based Audits

By Jack Freund

The author presents a perspective of security, audit, and risk over time beginning with the founding of the Electronic Data Processing Auditors Association (EDPAA). The article concludes with a practical approach to auditing with collaborative assistance to be provided by the risk management function of an organization.

Abstract

In this article, the author presents a perspective of security, audit, and risk over time beginning with the founding of the Electronic Data Processing Auditors Association (EDPAA). Given recent advances in the science and capability of risk management, the author argues that moving these professions forward will require an analysis of the job practices each is expected to perform, and to eliminate redundancies. A review of risk-based auditing opportunities and potential pitfalls is provided. The article concludes with a practical approach to auditing with collaborative assistance to be provided by the risk management function of an organization.

Information technology audit is a relatively recent addition to the professional world of auditing. A review of the history of IT audit leads one back to the Electronic Data Processing Auditors Association (EDPAA), which is the forerunner of what would eventually become the Information Systems Audit and Control Association (ISACA).[1] Although EDPAA published control objectives in the 1970s, what would eventually become ISACA's flagship publication, *Control Objectives for IT* (COBIT), was published in 1996. In large part, this publication defines controls for IT systems but is grounded in the definitions of controls codified by The Committee of Sponsoring Organizations of the Treadway Commission Internal Control-Integrated Framework (COSO).[2] Clearly, IT auditing was happening before these organizations codified the practice as reliance upon IT systems was identified as critical to organizational success. Indeed, the authors of the original COBIT document identify their impetus for creation thusly:

> "In recent years, it has become increasingly evident to regulators, lawmakers, users, and service providers that there is a need for a reference framework for security and control in information technology (IT)."[3]

In many ways this is a landmark in the cumulative history of information security, audit, and eventually risk. Utilizing reference frameworks for auditing is exactly what one expects from their audit function. Put another way, what we want from our audit functions is a gap analysis: here is what we said we were going to do compared to what the auditors found. Fanciful interpretations of this mandate are where problems begin to arise between security, audit, and risk.

Clearly, when management is presented with a list of findings after an audit, there is desire to prioritize the findings into actionable units to improve operations. Any talk of prioritization necessarily involves risk-based decisions and tradeoffs. Here is where the trouble begins. In the world of 1996's COBIT, there were not well-developed IT risk functions in many organizations. They likely existed, but not in sufficient quantity to call them a bone-fide profession. Enterprise risk management existed for a lot of organizations, but probably had their hands full with the larger operations of the business to worry about what was at the time a relatively small part of the business (i.e., IT). So where would management turn to get a sense of prioritization of control deficiency findings? The obvious answer was the trusted audit function across the table presenting the results in the first place. Put much more

[1] Friedman, H., 2012. ISACA's 1973-4 president: Nearly four decades later, some things remain the same. Retrieved from http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d-9997-4b62-96a4-a36fb7e171af&ID=203.

[2] COSO. (2004). Enterprise Risk Management - Integrated Framework. Retrieved from http://www.coso.org/ERM-IntegratedFramework.htm.

[3] COBIT Control Objectives. (1996). Rolling Meadows, IL: ISACA.

graciously, IT audit did IT risk management because the security function was too immature to know how to help with risk prioritization. However, the organizational and professional landscape has since changed and not entirely for the better.

Analysis of current job practices

Let's analyze an organizational model for risk audit and security that is broadly deployed. In many organizations one can find groups that go by the following names:

- Internal Audit (IT focused)
- IT Compliance
- IT Security
- IT Risk Management

Let's analyze the above groups in terms of the nature of the following professional activities: control design, control assessment, and risk assessments (what is largely considered basic security activities – see, for instance, CRISC, CISM, CISA job practice areas). In large part, control design is the task of a security engineer, architect, or analyst. These professionals would evaluate the technological facets of the system and suggest or evaluate controls designed to reduce risk. A security and/or control assessment could be conducted by either Internal Audit or IT Compliance. This task involves evaluating the performance of controls (inclusive of adherence to policy). One difference between the two functions is that external auditors can rely on materials gathered by Internal Audit, but not compliance functions. Lastly, risk management advises the business as to the priority of security and audit findings and initiatives. This modern version of security job functions is predicated on the maturity of each function. However, there was a time when this was not the case, particularly with regards to risk management.

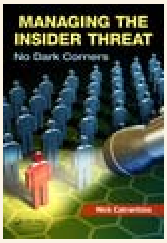
Mature risk management must focus on quantification[4] and this point is key: if the risk management function focuses on qualitative assessments and control-based activities, then they are at best duplicating the efforts of Internal Audit and IT Compliance and wasting resources, and at worse misinforming management on the state of risk. At a practical level, the distinction between the functions of risk and security is severely limited if the risk management activities duplicate security. If the leaders of such organizations wish to continue the two functions without changing the risk management focus, then they are paying twice for the same benefit.

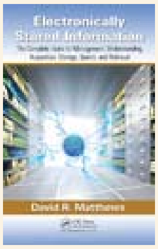
A cooperative model based on job practices

When ISACA published its standard, codifying what was years of professional practice in the industry, IT risk management (if it existed at all) was not capable of evaluating the priority of audit findings to management. The state of practice at the time could be summed up as, "lack of control equals high risk." Risk management practices today are more mature.[5] A mature risk management function should bear the responsibility of informing decision makers on the severity of audit findings. In this paradigm, the following things are required from the audit function. They should identify:

1. Variances from agreed-upon policies and standards
2. The degree and frequency of deviations (one-time, systemic, etc.)
3. How critical the deviations are to the operation of the overall system

Continued on page 36





[4] Hubbard, D., Evans, D. 2010. Problems with Scoring Methods and Ordinal Scales in Risk Assessment. *IBM Journal of Research and Development.*

[5] Lowder, J., December, 2010. Is Risk-Based Security a Failed Concept? *ISSA Journal.*

monitoring via your RSS feed reader. For those of you defending Internet-facing SharePoint implementations, you'll definitely want to check out the SharePoint Diggity Hacking Project too.

Enjoy this tool arsenal from Stach & Liu's Dynamic Duo; they'd love to hear from you with kudos, constructive criticism, and feature requests via diggity at stachliu.com.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Francis Brown and Rob Ragan, Managing Partners, Stach & Liu, Google Hacking Diggity project leads.

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.

A Cooperative Model for Security, Audit, and Risk

continued from page 32

The first element is a part of the classical definition of audit responsibilities. In this regard, audit should focus on critical operations and functions in the organization, and focus on areas where failure to abide by internal policies and standards would endanger those operations. This is a critical part of the process. Many modern versions of IT audit functions employ what is termed a risk-based-audit. According to Griffiths, a risk-based audit focuses on those areas of the organization that are the most important.[6] Although one would be hard-pressed to justify an audit of unimportant areas, the author indicates that this approach represents the future of Internal Audit. It is described as being a horizontal approach that focuses on areas that correspond to high-risk business activities along with the application of best-practices.

This approach has the opportunity to be beneficial to the organization, as it substitutes the auditor's priority-making for that of the businesses (i.e., focusing on the areas that the business already identifies as being critical). However, where this approach will not improve decision-making is in the application of standards for which the business has not agreed to adhere. For instance, strictly auditing an organization by ISO/IEC 27001:2005 that has not committed to follow it would not help inform management of their organization's compliance with that standard. An ISO auditor would ask for the Statement of Applicability or evidence of management commitment and the result would immediately halt the audit. As a result, a key takeaway is to ensure that any perceived best practices inform the decision making of those who are writing the policies and standards of the organization, or those who have the authority to commit an organization to adhere to them.

Whereas the first audit requirement attempts to have the auditors identify where variances are occurring, items two and three seek to add some details to that variance. In particular, item three allows auditors to apply their knowledge of the business and IT operations to the audit finding. Audit reports and closeout meetings should include risk ratings from the IT Risk Management function. If there is concern about impartiality, then the risk report can be separate from the audit results presentation and documentation. The executives will be expecting a sense of priority from the audit closeout report, so collaborating with risk management will bring validity to the results by ensuring that the audit findings are grounded in the risk appetite of the organization.

Conclusion

The goal of all information security and risk management functions should be to align operations to a tolerance level decided by the leadership of the organization. In order to accomplish this goal, someone has to communicate risk posture to that leadership such as to inform good decision making. There is a growing body of evidence that IT risk management is increasingly able to accomplish this goal by focusing on solid risk practices developed over time by risk professionals in other industries. Adopting this modern approach to risk management will mean reevaluating the role of the other functions in your organization. It simply is not cost-effective to have up to four different groups in your companies doing the same task, namely control-based assessments. The proliferation of audit fatigue in our organizations demands resolution, and aligning our security, audit, and risk professions to the jobs they do best is a great place to start reducing this strain on our businesses.

About the Author

Dr. Jack Freund is a senior information risk professional specializing in analyzing and communicating complex IT risk scenarios in plain language to business executives. Jack blogs at riskdr.com. He can be reached at jfreund@ieee.org.

[6] Griffiths, P., 2005. R*isk-Based Auditing*. Farnham, Surrey, United Kingdom: Gower Publishing Ltd.