IT Strategic Audit Plan

Marc Ackerman
Beth Rucker
Anecia Wells
Joseph Wilson
Randy Wittmann

Jacksonville University

Abstract

IT Governance and Strategy are critical to a successful enterprise. Corporate executives must formulate governance plans and strategies, as well as accompanying policies and procedures, to concurrently enable the company to achieve its strategic vision, support audit requirements, manage risk, and exhibit responsible financial management (Swanson & Brewer, 2007). Formal audit processes are utilized to determine if IT governance and strategy are functioning as intended. This research paper will summarize key components of an IT strategic audit plan, including why the processes and components are important. It will conclude with a mock audit designed to demonstrate the types of findings that might result from an audit of an organization's IT strategy. The mock audit is based on an actual company. The company name has been withheld based on confidentiality requirements.

Keywords: strategic audit, strategy, IT, information technology, audit plan

IT Audit Plan Process

Understand the Business
1. Identify the organization's strategies and business objectives 2. Recognize the risk profile for the organization 3. Assess how the organization structures its business operations 4. Comprehend the IT service support model
Define the IT Universe
5. Analyze the business fundamentals 6. Isolate significant applications that sustain the business operations 7. Distinguish critical infrastructure for the significant applications 8. Appreciate the role of supporting technologies 9. Categorize major projects and initiatives
Perform Risk Assessment
10. Evaluate business and IT processes to identify risk 11. Assess risks and rank audit subjects using IT risk factors 12. Assess risks and rank audit subjects using business risk factors
Formalize Audit Plan
13. Choose audit subjects and group into distinct audit actions 14. Establish audit cycle and frequency 15. Attach appropriate actions based on management requests or opportunities for consulting 16. Confirm the plan with management

Figure 1.

Process Overview

An IT strategic audit should be conducted with the view that the primary purpose of an organization's technological resources is to support their business objectives and these technologies should be considered a risk to the organization if their failure thwarts attainment of those objectives. The first step in planning and then conducting an IT strategic audit is to define and evaluate an organization's objectives, strategies, underlying business model, and the role of technology in the support of that business. Once this is accomplished, a risk assessment can take place. That is to say, each technology employed can be evaluated in terms of the risk that it poses to the organization achieving its specific business objectives.

Overall, this outlines the basis for developing an IT audit that aligns with business direction and strategic goals. Therefore, it is imperative that an audit design incorporates a definitive structure allowing for assessment of the functional relationship of IT and core business objectives. Chronologically, an IT strategic audit should first assess the understanding of business objectives. Secondly, the IT Universe must be assessed to determine the level of IT support for the business, including, operations, production (if applicable), marketing and development. Thirdly, risk assessments must be performed to ensure representation of precise understanding of business goals and culture. Lastly, based on these prerequisite steps, formulation of a successful IT strategic audit plan incorporating the fundamentals of the business model, IT and risk is achievable.

IT is the fundamental backbone of any business that allows for potential growth and development in desired markets. It is crucial to realize whether IT governance represents the core business goals as resource allocation generating revenue growth versus declining trends maximizing business opportunity. The following sections provide additional details on how this Strategic Audit design optimizes the value of the results and benefit to business growth.

Understanding the Business

Since each organization is unique, the IT strategic audit plan should be defined by an organization's underlying business model. Once the business model is understood, the auditor will have a better sense of how technology is being utilized to meet business objectives. The following internal resources provide detailed information pertaining to an organization's goals and objectives:

1. Mission, vision and value statements
2. Strategic plans
3. Annual business plans
4. Management performance scorecards
5. Stockholder annual reports
6. Regulatory filings (SEC)

Once an organization's strategic objectives are determined, it is possible to identify the key business processes that are essential for meeting those objectives. A business process is considered key if its failure inhibits the organization from arriving at the strategic objective it is linked to. Operating units such as manufacturing, sales, and distribution should be examined at the process level. Supporting functions of management should also be examined, such as governance, compliance, finance, and human resources. As soon as the key processes are identified, the audit plan must outline the important applications and critical IT infrastructure that supports these applications. The IT processes that underlie these applications are systems development life cycle, change management, operations, and security procedures.

Defining the IT Universe

According to the Global Technology Audit Guide (GTAG) published by The Institute of Internal Auditors (2001), there are eight IT environment factors that are essential to understanding an organization's IT universe. First, the degree of system and geographic centralization should be examined. Whether or not an organization maintains a centralized or decentralized organizational structure will influence decision-making and allocation of IT resources. The second factor is what types of technologies have been installed. There may be great diversity in any level of the IT stack, warranting investigation in a specific application's program code, database, operating system, and network infrastructure. The third factor is the degree of customization. Some business processes may have required customization of off-the-shelf software, thus creating more reliance on in-house technical support versus the original vendor(s). The fourth factor is the degree of formalized company policies and standards that define IT governance. According to Peter Weill, IT governance is specifying the decision rights and accountability framework that encourages desirable behavior in the use of IT (Weill & Ross, 2004). The fifth factor is the degree of regulation and compliance in a particular industry. An organization's regulatory requirements must be considered in the risk profile and IT audit

universe. Any organization registered with the Securities and Exchange Commission is required by the Sarbanes-Oxley Act to report on the effectiveness of their internal policies for financial reporting. The sixth factor essential to understanding an organization's IT universe is the degree and method of IT outsourcing. Although outsourcing IT may bring significant cost savings, it carries with it additional levels of risk that may be country-specific. The seventh factor is the degree of operational standardization. This will impact the reliability and integrity of the IT infrastructure and related processes. The eighth factor influencing an auditor's understanding of an organization's IT universe is the level of reliance on technology in that organization. The more an organization relies on the availability and functionality of different technologies in the IT universe in day-to-day business operations, the more the potential risk increases (Rehage, Hunt, & Nikitin, 2008).

Performing the Risk Assessment

One of the primary goals of the risk assessment process is to understand the strategic goals and objectives of the business and what role IT plays in support of or assisting in the achievement of said goals. Practice Advisory 2110-1 issued by the IIA identifies five key objectives of the risk management process (Institute of Internal Auditors, 2001):

1. Mission, vision and value statements.
2. Identification of business strategy risk, and prioritization of associated activities.
3. Determination by management and the board of the acceptable risk level, including signoff on risks associated with accomplishing the company's strategic plans.
4. Design and implementation of risk mitigation activities to reduce or otherwise manage risk to levels that management and the board deem acceptable.
5. Creation of ongoing monitoring activities to periodically reassess risk, and the effectiveness of risk management controls.
6. Creation of periodic risk management metrics for management and board review, as well as timely periodic stakeholder communications regarding risk, risk strategies, and risk controls.

Key to the risk assessment process is breaking down the IT Universe into smaller more manageable sub-components. Typically, the IT sub-components are defined as infrastructure, computer operations and applications. Contained within the infrastructure sub-component are servers, routers, communications, desktops, etc. This hardware controls the flow and processing of information throughout the organization. Computer operations deal with the maintenance of the computing environment. These controls consist of security applications, disaster recovery plans, and service level agreements (SLAs). The third sub-component is applications. This is the software used to record and store business transactions. Examples would be database, enterprise resource planning, or business intelligence software.

In the development of the risk assessment, there will need to be some form of rating for each risk identified. IT audit usually classifies this as ranking risk. The table in Figure 2 is how the GTAG suggests risk be ranked.

H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Figure 2.

Three types of risk factors are continually in use: Subjective, objective or historical, and calculated. *Assessing Risk* (McNamee, 2004) defines each of these factors as follows:

- Subjective – Measuring risk and its impact requires a combination of expertise, skills, imagination, and creativity. The emphasis on subjective measurements is borne out in practice; many auditable units change so much between audits that prior audit history is of little use. Therefore, an experienced practitioner's sound subjective judgment is just as valid.
- Objective or Historical – Measuring risk factor trends can be useful in organizations with stable operations. In all cases, current objective information is helpful in measuring risk.
- Calculated – A subset of objective risk factor data, this is the class of factors calculated from historical or objective information. These are often the weakest of all factors to use because they are derivative factors of risk that is further upstream.

Formalizing the Audit Plan

Once the risk assessment is complete, the IT Audit Plan can be prepared. At its core, the IT audit plan is the execution of evaluating the risks identified in the organization. The key in the IT audit plan is deciding what frequency to audit what risks and how to allocate resources to those risks. According to *Brinks' Modern Internal Auditing*, auditors can employ two strategies to arrive at the ideal frequency of planned audit activities (Moeller & Witt, 2005).

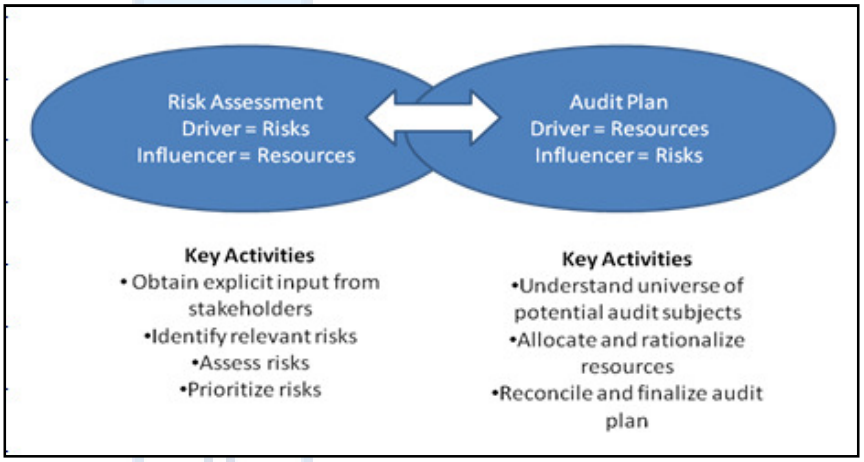

Figure 3.

- The audit frequency is established in an initial risk assessment to take place every three to five years and is proportional to the risk level.
- The audit plan is based on a continuous risk assessment without a predefined audit frequency. Some organizations use this approach, which is especially appropriate within the context of the IT audit plan, given the higher rate of IT change as compared to non-IT activities.

Deployment of resources is always challenging. As in most situations, there are virtually unlimited tasks and limited resources. It is for this very reason that it is critical to rely on the risk assessment for resource deployment. During the assessment phase, risks have been identified, likelihoods of occurrence have been established, and priorities have been created. Sourcing of resources is also critical in the audit planning stage. Sources can be all internal, all outsourced, or some combination of the two. It is important to be cost beneficial as well as effective so value is conveyed to the stakeholder.

Role of IT Governance and Strategic Alignment

The role of IT governance and strategic alignment within an organization is imperative to overall business success. Implementation of an integrated IT governance program that aligns with business planning and strategy is the fundamental key to IT governance supporting business growth and stability. Moreover, focus on strategic alignment in IT governance results in creation of cross functional teams with participation from executive level leadership including the CIO. These teams help ensure the alignment of the business and IT strategy, establish the IT architecture and ensure the proper allocation of IT resources. These teams are charged to manage IT utilizing an "all in involved" approach. For example, projects are chosen based on weighted risk: strengthening global market position, value and return (Gallegos, 2003).

Industry experts continue to reiterate the importance of IT being aligned to business strategy. According to research conducted by Richard Nolan of Harvard Business School, companies with effective IT Governance Committees tend to keep their costly projects under control, which ultimately leads to gains in competitive advantage. His research included large companies such Home Depot, Wal-Mart, FedEx, Mellon Financial, Novell, and Procter & Gamble (Nolan, 2005). Chris Potts made a very bold statement in a *CIO Magazine* article, indicating that IT-centric strategies have become impossible to execute against. He attributes this shift to two factors: 1) The change from mainframe technologies to client server technologies that were more understood by business professionals, and 2) the Year 2000 and dotcom colapse that left business professionals disenchanted with IT and its techno-babble. Potts posits that these events were the start of IT decisions shifting to the executives responsible for the business, as opposed to those responsible for the technology (Potts, 2007).

IT governance programs that are properly aligned with business goals provide opportunity for appropriate business reorganization to sustain growth in global markets as competition increases. In successful IT governance programs using CobiT domains in activity mapping, four key factors are maintained: 1) planning and organization, 2) acquisition and implementation, 3) delivery and support, and 4) monitoring (Ramos, 2001). While the framework of the IT department supports this, the audit survey can often identify a divide between the execution of the company's core business strategies, the direction, and the IT governance. Furthermore, the focus on IT organizational structure, IT infrastructure, and IT project oversight is vital to IT governance aligning with business objectives.

Mission, vision, value statement, strategic plans, annual business plans, management performance scorecards, stockholder annual reports, regulator and filings with the SEC are all crucial components, but just as important are the company's employees. For an IT strategic audit to be effective, it must be performed by personnel who are well versed in strategy and governance disciplines. In addition, successful remediation of the audit's findings is directly dependent upon the personnel allocated to carry out the improvements. Infrastructure and technology assets are typically utilized in the remediation; however, the people are what make the IT Strategic Audit process a success.

References

Gallegos, F. (2003, January). IT governance: IT audit role. *Information Systems Control Journal, 4*, 25. Retrieved October 8, 2008, from ProQuest Central database.

Institute of Internal Auditors, The (2001). Practice advisory 2110-1: Assessing the adequacy of risk management processes. Retrieved October 11, 2008.

McNamee, D. (2004). Assessing risk, 2nd Edition. The IIA Research Foundation.

Moeller, R. & Witt, H. (2005). *Brinks' modern internal auditing,* 6th edition, p292, Wiley Publishing.

Nolan, R. (2005, October). Information Technology and the board of directors. *Harvard Business Review*. Retrieved September 16, 2008.

Potts, C. (2007, September). Let the business drive IT strategy, CIO Magazine. Retrieved October 15, 2008.

Ramos, D. (2001, January). The auditor's role in IT governance. *Information Systems Control Journal, 5*, 23-24. Retrieved October 8, 2008.

Rehage, K., Hunt, S., & Nikitin, F. (2008, July). Global technology audit guide: Developing the IT audit plan. The Institute of Internal Auditors. Retrieved October 6, 2008.

Swanson, D. & Brewer, C. (2007, April). IT governance and strategy, p*ractical guidance for managers on how to prepare for successful audits*. IT Compliance Institute, www.itcinstitute.com. Retrieved October 15, 2008.

Weill, P. & Ross, J. (2004). IT governance: How top performers manage IT decision rights for superior results, Harvard Business School Press, Boston, MA.

Appendix A – Mock IT Strategy Audit.

ABC Company
IT Strategy Audit

Audit Objective

The objective of this IT Strategy Audit is to evaluate ABC Company's (ABC) overall IT strategy. The audit will specifically target IT's performance related to the following areas: Alignment with ABC's business strategy, IT organizational structure, IT infrastructure, IT security, and IT project oversight. The resulting report will include recommendations for improvements where deficiencies are noted.

Executive Summary

ABC's Information Technology division has taken very positive steps in the development of an IT Strategy that is aligned with the overall ABC business strategy, especially considering ABC Company performed a considerable reorganization of its Executive Management team, including naming a new CIO, less than six months ago. The new CIO significantly reorganized the IT leadership team and quickly moved into developing its forward looking strategic plan. Although the plan is not yet complete, it is trending in the right direction and is being based upon solid methodologies.

The recommendations resulting from this audit are as follows:

- IT Security – ABC should form a more formalized Security Council, comprised of empowered delegates from each business segment, to closely manage the company's security initiatives. This Council should also be chartered to foster collaboration and consistency across the enterprise.
- IT Infrastructure – ABC should continue forward with its stated plans to implement recently proposed infrastructure strategies for its network, data centers, and email systems. These initiatives will mitigate many operational and security risks inherent to the existence of disparate networks and production processing locations and will enable enhanced intra-company communications and integration.
- IT Architecture – ABC should continue leveraging a cross-organizational team to devise a set of architectural standards that will be utilized for ongoing development of existing and new products. These standards should include key components such as processing platforms, database standards, consistent use of agreed upon technology stacks, and security standards.
- IT Project Management – ABC should continue development of processes that ensure alignment of IT projects to business sponsorship and prioritization. This will result in maximized business benefit being derived from IT initiatives.
-

Overview of the Business

ABC Company is comprised of many different business entities that provide business process services to the financial services industry. ABC is comprised of fifteen Operating Segments, representing forty-two Business Segments. Many of these segments have evolved

from different points of origin (e.g. via acquisition, via entrepreneurial startup, via prior reorganizations); therefore, many continue to operate in a somewhat autonomous fashion, both from a business perspective and from a technology perspective.

In the six months since the corporate level reorganizations, great strides have been made to align the business units and to bring clarity to ABC's overall strategy and vision. The new Executive Management team is very clear in their sponsorship of bringing end to end solutions to their customers, which will result in increased market penetration and increased overall revenues. This sponsorship encompasses not only the business aspect, but also the technology aspect.

The IT Universe

Just as much of ABC's business is decentralized in multiple business segments, many of ABC's technology assets and services are also decentralized. This is the result of each business segment, and their respective supporting technology organizations, coming from unique origins.

Currently, ABC provides production processing for its clients from fifteen different data centers. Four of these data centers have been deemed strategic; the other eleven are leased facilities that are tactical and targeted for consolidation into the four strategic data centers over the next eighteen months. The technology infrastructure that supports ABC's lines of business is complicated by the large number of acquisitions that have occurred in the past several years. As an example, although the networks are fairly standardized on Cisco equipment, several different networks are interconnected utilizing various telecommunications technologies (e.g. VPN, MPLS, frame relay, etc.). Many of the networks remain independent of one another. Similarly, although email is standardized on Microsoft Exchange, several different Exchange organizations are interconnected, complicating activities such as directory synchronization and mail routing. ABC has recognized that these situations are not favorable to their ongoing growth objectives, and has approved technology investments to remediate these situations, with the end result being comprehensive network and messaging solutions that will be deployed across the organization. These initiatives, combined with the data center consolidation, will position ABC very well for future growth and for consistent technology oversight and governance at the infrastructure level.

Since the corporate level reorganization, many changes have taken place within the Information Technology area to better align technology with the business. ABC's new CIO has clearly been empowered to systematically begin restructuring the decentralized IT organization into centralized shared services where it makes sense, and to improve cross-company collaboration within the decentralized areas that are logical to leave decentralized. The CIO has also taken a very firm stance that IT will no longer independently sponsor technology initiatives without business involvement. IT will make recommendations to the appropriate levels of business line management, seeking their concurrence that the recommended initiatives align with overall business strategy. Technology initiatives will only proceed if this concurrence and associated sponsorship is obtained.

Risk Assessment and Strategic Recommendations

Finding / Recommendation 1. From a technology perspective, one of the largest areas of IT risk is the number of different IT security risk mitigation tools and processes deployed across the data centers. The number of variants closely correlates to the number of geographically dispersed data centers, in that most have functioned autonomously in the past. Although each is

likely to be adequate when viewed in singularity, the duplication in support effort is counterproductive to the company's overall expense management objectives and the variations in tools and processes leave the door open for ABC's customers and auditors to be confused when they receive different insights from different segments. Several areas are currently being evaluated for centralized management, or at least central governance, including risk assessment methodology, vulnerability management, intrusion detection, penetration testing, encryption standards, and logging standards. A more formalized Security Council, comprised of empowered delegates from each business segment, should be formed to closely manage these initiatives and to foster collaboration and consistency across the enterprise.

Finding / Recommendation 2. ABC's core infrastructure continues to be heavily fragmented in disconnected segments. Although this situation is understandable given the pace of recent acquisitions, it is imperative that ABC move forward with its stated plans to implement approved enterprise infrastructure initiatives. These initiatives will mitigate many operational and security risks inherent to the existence of disparate networks and production processing locations and will enable enhanced intra-company communications and product integration.

Finding / Recommendation 3. Another area of technology risk is related to architectural strategy, and alignment of that strategy to ABC's overall business strategy. A key component of ABC's business strategy is to continue integrating the full suite of products, which will in turn lead to increased market penetration. Given each product category has matured somewhat in isolation from the others, it is critically important that IT across the company begin aligning on specific standards for ongoing development and architectural enhancements. ABC should continue leveraging a cross-organizational team to devise a set of architectural standards that will be utilized for ongoing development of existing and new products. These standards should include key components such as processing platforms, database standards, consistent use of agreed upon technology stacks, and security standards.

Finding / Recommendation 4. Existing project management processes are not currently robust enough to sustain ABC's objective of business and IT alignment. As previously mentioned, the CIO has taken a firm stance to align all IT projects to the business strategy; however, the processes to facilitate this alignment are still being formulated. Additionally, IT project management remains decentralized, with several Project Management Offices co-existing across the organization. This leads to different project management methodologies, tools and processes; it also complicates workload management when multiple initiatives draw on the same centralized resources. ABC should continue development of processes that ensure alignment of IT projects to business sponsorship and prioritization. This will result in maximized business benefit being derived from IT initiatives.