NEW PERSPECTIVES
on Healthcare Risk Management, Control and Governance


Data Analysis Challenges:
Try Proven Strategies for More Success
page 11

Anticipate IRS Audits:
How to Mitigate Human Resource Risks
page 7

System Development and Implementation Projects:
Internal Audit’s Guide
page 46

Assessing IT Governance:
Considerations for Internal Audit
page 54
Executive Summary

In the healthcare industry, Information Technology’s (IT) evolution from support function to “top table” contributor has been unfolding at a much slower pace than in other business sectors. Regulatory pressures and the need to embrace new technology to increase efficiencies are now setting a faster pace. These changes and the consideration of The IIA’s Standard 2110.A2 have many internal auditors re-evaluating their roles and responsibilities in the area of IT governance.

Well-designed IT governance helps empower management and enable value across a healthcare organization. Internal audit can play a leading role in helping align the facility’s IT decision-making and execution with business strategy through better communication and effective processes.

Internal audit can help to assess whether established business processes and existing organizational structures are being leveraged effectively. Audit teams also can “slice” IT governance assessments to focus on specific areas and high-profile initiatives, instead of conducting labor-intensive, enterprise-level reviews.

Most leading businesses no longer view their information technology (IT) function strictly as a back-office utility or low-value information service provider. Instead, they see its potential as a process optimizer and an enabler of new services and products for the enterprise.1 Senior management in healthcare organizations increasingly is consulting with IT leadership on how to use technology strategically to increase profit and competitive advantage, while improving efficiency and reducing costs.

Among healthcare providers, IT’s evolution from support function to “top table” contributor has been unfolding at a much slower pace than in other industries—but that’s quickly changing. The healthcare industry has been historically slow to embrace new technologies and deployment of IT systems. This is due to a number of challenges, including resource constraints and information privacy concerns.

Now, intensifying regulatory pressure—from the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Patient Protection and Affordable Care Act (PPACA), for example—is hastening the need for healthcare organizations to work more closely with IT. They need to make smart technology decisions not only to meet compliance demands, but also to improve patient safety, quality of care and operational efficiency.

Another compliance measure, Standard 2110.A2, has made it more important for internal audit departments to work with management to ensure IT investments align with business goals. Issued by The Institute of Internal Auditors (The IIA) as part of its International Standards for the Professional Practice of Internal Auditing, Standard 2110.A2 instructs internal audit to assess whether an organization’s “IT governance” sustains and supports the business’s strategies and objectives.

This standard is not new, nor is the concept of IT governance. Yet a recent survey conducted by Protiviti found that in nearly 70 percent of North American companies, the internal audit team has not completed an evaluation and assessment of the organization’s IT governance, as required by The IIA Standards.2

While more firms are integrating IT further into their operations and decision-making processes, most are not formally examining their IT governance risks. As a result, they are increasing the likelihood that they are ineffective in managing their IT risks, opportunities and investments.

This is not a wise—or sustainable—position, particularly for a healthcare provider. An increasingly large portion of critical clinical and business functions, essential to employee collaboration and productivity, depends on IT. IT more often

---


now plays a central role in a company’s ability to innovate and compete.

Organizations that are “IT-empowered”—where IT spends less and is better positioned to help enable growth—commonly have an IT strategy and organization that fully support key business objectives.3

Understanding IT governance

To assess IT governance effectively, you must understand that its purpose is to provide a single integrated view across IT—from demand management, to service management, to process activities (such as security), to architecture, including databases and operating systems.

IT governance provides a means for a healthcare enterprise to validate that IT-related decisions are aligned strategically with where the business wants to go. It is not a stand-alone process, but a set of integrated practices and structures that enable oversight for all IT activity. By this definition, IT governance must be embedded in everything the IT function does.

Many healthcare organizations delay instituting formalized IT governance practices and assessments because they do not understand where the responsibility for IT governance should reside in the enterprise.

Exhibit 1 – Responsibility for IT governance

This does not mean assessing IT governance—and evaluating its effectiveness—must be a complex and resource-intensive undertaking.

The generally accepted guidance on ownership comes from the IT Governance Institute (ITGI): “IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.”

Exhibit 1 illustrates how responsibility for IT governance is centered within the IT management layer. This layer includes the IT leader, usually the chief information officer (CIO), IT managers and business leadership that includes IT oversight functions such as the IT steering committee.

See the sidebar for more detail on the five key elements of IT governance, depicted in the middle of the pyramid: strategic alignment, risk management, resource management, performance management and value delivery.

IT governance includes clearly defining the chain of command that runs through the business’s IT-related decision-making process: Who provides input on decisions, who makes decisions, who executes decisions and who measures results?

Most organizations, including those in the healthcare industry, do not have their IT decision-making roles and authority levels clearly defined. A significant number of healthcare enterprises are only just starting to take a more strategic view of IT. Many IT decisions have been made in response to immediate technology needs of specific groups or initiatives, and not to support broader business objectives.

Fully understanding the decision-making process for IT and assigning accountability for decisions are critical to ensuring strategic alignment. Business strategy can only be enabled through well-considered decisions that are discussed, made and carried out by the appropriate people in the organization.

The goal is to develop a decision-making model that provides a framework for the types of decisions a healthcare organization’s IT function needs to make, and/or what decisions the business needs to make around IT. The desired level of input and action around those decisions by relevant parties should also be outlined.

Exhibit 2 shows the entities tasked with each type of IT-related decision process and activity, and how often they are expected to perform those responsibilities.

**Approaches to assessing IT governance**

Many healthcare organizations delay assessing their IT governance because there is no one-size-fits-all approach. Additionally, the scale of an enterprise assessment of IT governance can be taxing for an internal audit team—especially if auditors don’t know how or where to begin their work.

Because IT governance requirements will vary based on organizational needs, healthcare facilities need to design an approach that is most appropriate for ensuring technology decisions align with their specific business objectives.

However, this does not mean assessing IT governance—and evaluating its effectiveness—must be a complex and resource-intensive undertaking. In fact, these organizations and their internal audit functions will be well-served to leverage established business processes to integrate IT governance effectively. This will also help them to ensure the selected approach is compatible with existing corporate governance structures and practices.

Still, some healthcare organizations may decide they want to dig deep, at least initially, to determine the current state of their IT governance. They will conduct an enterprise-level governance review to examine all five areas of the IT governance model across the entire IT organization (see the “Five Key Elements” sidebar).

This top-down approach, while thorough, can be time-consuming and expensive. It is a full, in-depth review that can easily overwhelm audit departments, even large ones. This is because IT-specific auditing resources are often limited—or nonexistent—in a large percentage of internal audit teams.

Resource constraints are a key reason why it is important for audit departments in healthcare facilities to leverage existing research, frameworks and previous audit efforts whenever possible. You may have more to work with than you think. There is a good chance many things that should be evaluated as part of an IT governance assessment were evaluated for other audits within the recent past.

For example, in for-profit entities, Sarbanes-Oxley compliance assessments can provide insight into the risks and controls related to the organization’s financial systems. Work should not be redone for the sake of checking a box; instead, you should build upon results and avoid wasting time validating basics already in place.

Another way to simplify the approach to assessing IT governance is to “slice” internal audit’s review process so that only a specific function, service area or process area within IT is examined. Depending on a healthcare organization’s IT activities and strategic objectives, this may be all that is necessary to identify governance risk areas.

For example, with a service/process area review, your focus could be strictly on how a hospital is governing the software life cycle. Through this bottom-up approach, internal audit can determine how the focus area is integrated with other key IT services/processes and how well it is aligned with the hospital’s IT objectives and managing its resources and risks.

Whether applying either an enterprise-level or a service/process-level approach, areas that are commonly examined as part of internal audit’s review of IT governance include:

1. Strategy definition and planning
2. IT oversight functions (e.g., steering committee)
3. Program, project and portfolio management
4. Risk management and compliance

---

Exhibit 2 – Sample IT governance model

[Diagram showing various governance committees and processes, including:
- Executive Management Committee
- IT Steering Committee
- IT Service Management Team
- IT Architecture Committee
- IT Demand / Portfolio Working Group

Key activities include:
- Track metrics across ALL IT and review / projects (monthly)
- Determine standards for technology; Monitor compliance with standards (quarterly)
- Re-engineer IT processes and functions to fit evolving service requirements (continuous)
- Broad IT strategy and investment decisions (quarterly)
- Tracking IT investments vs. budget; scenario/ “What If?” planning (quarterly)
The Five Key Elements of IT Governance

When audit teams are analyzing an organization’s IT governance, they should take the five focus areas below into consideration.* Each element on this list has relevance to all IT process areas and presents a distinct value proposition for the enterprise:

1. **Strategic alignment** – Maximize opportunities for the business use of IT while providing transparency and assurance that IT objectives are being achieved. This includes defining the IT value proposition, determining the linkage between business and IT plans and increasing managerial effectiveness.

2. **Risk management** – Address legal and regulatory compliance needs and understand and manage key operation risks. This includes determining risk appetite and tolerance, assessing IT risk awareness and identifying risk exposures.

3. **Resource management** – Appropriately align IT capabilities with business needs, including optimizing IT resources, optimizing knowledge and aligning capabilities.

4. **Performance measurement** – Utilize real-time data to continuously improve IT delivery. Approaches include measuring strategy implementation, reporting and the application of operational and strategic metrics.

5. **Value delivery** – Optimize return on IT investments by executing on the IT value proposition, meeting business requirements and verifying the integrity and accuracy of information.

*Based on the IT Process Institute’s five areas of IT governance.

5. Management information and reporting

6. IT operational processes (e.g., security, continuity)

“Slicing” the IT governance review process can be taken even further to refine the focus on:

- **Outsourced service providers** – This includes examination of the governance approach for a particular outsourced IT service provider. Questions internal audit may consider as part of their assessment include: How are the service provider’s internal processes executing against our organization’s governance? Are we effectively governing the service provider’s activities? Is there good alignment between our management and the service provider? This type of review also focuses on the enterprise’s mechanisms for managing relationships with service providers and measuring/managing results.

- **Strategic initiatives** – With this approach, governance for a particular IT program area or project, such as an enterprise resource planning (ERP) system implementation, is examined. This review focuses on the oversight structures for the specific IT initiative, and can include examination of the design of requirements and execution of the life cycle for a particular program. The enterprise-level IT governance approach in the context of the project or program is also taken into consideration.

  • **Decision-making and strategy alignment** – Using this quick-hit type of assessment, internal audit takes a basic look at IT decision-making and strategic alignment to identify key risks. Special focus is given to the IT management layer to assess the tone at the top, the level of oversight and the state of management across the board. IT’s business demands, its input and decision mechanisms, its management structure and how the function coordinates itself to align with the business are also considered.

**Defining the alignment model**

Of the five elements of IT governance that internal audit should consider in their assessment, strategic alignment is often the most difficult. This is because it is an abstract concept.

Defining the IT function’s alignment model is vital to successful IT governance. Through this process, a healthcare enterprise can identify what type of IT organization is currently in place, and how (or if) the function needs to evolve to meet business objectives.

According to the IT Process Institute’s 2008 IT Strategic Alignment Performance Study, IT organizations correspond to one of three specific alignment models:

- **Utility providers** – This type of IT function is not actively engaged with the business. Its primary focus is to provide shared information management functions in support of basic information and transaction management.

- **Process optimizers** – This type of IT organization is more responsive to the business. Process optimizers split their focus between information management functions and optimization of key business processes.

- **Revenue enablers** – This IT function is well integrated into the business. Its focus is on three key areas: shared information management, business process optimization and technology-enabled products and services.
Identifying the appropriate alignment model will help the business answer questions such as: Where should we be in terms of our strategy alignment? What do we want IT to be? How are we currently governing IT? Issues that are inhibiting effective IT governance also will come to light.

For instance, the organization may want IT to help the business improve its processes and profits, but it is currently treating the function as a utility provider. This means there is a significant communication—and governance—problem to address.

Adapting to change through IT governance

A growing number of businesses, including healthcare organizations, want to use their IT functions more strategically, but fewer than 40 percent of enterprises feel they have effective IT governance, according to ITGI. In other words, more than 60 percent of enterprises are failing to realize opportunities for enhanced business success and value.

There is clearly an opportunity for internal audit—and more specifically, IT auditors—to help the enterprise work more effectively with IT. IT governance is all about being conscious of how IT decisions are made in the enterprise, and evaluating whether those decisions are resulting in the desired value. But IT governance is not something business leadership often thinks about. This is especially true in the healthcare industry. Until recently, most healthcare firms viewed their IT functions almost exclusively as utility providers.

Effective IT governance begins by setting the appropriate tone at the top, as Exhibit 1 underscores. Therefore, a good starting place for formalizing IT governance in a healthcare organization is to improve communication among key decision-makers in the business and in IT.

To make IT governance a top-table topic, internal audit should invite these groups to a workshop or to one-on-one interviews. Ask them to define what they think alignment should look like and how IT decision-making is currently being handled. If an inconsistent picture develops, a governance problem in the enterprise may be the cause. An organization that wants to get more value from its IT function must start treating it like a value center instead of a cost center. To put this issue in IT terms: If you only request dial-up service, don’t expect to receive high-speed internet access.

Conclusion

IT governance helps healthcare organizations keep strategic objectives in focus, while ensuring balanced and predictable IT delivery for the enterprise. An organization’s approach to IT governance will be shaped by its unique set of business, compliance and IT needs.

But assessing IT governance and evaluating its effectiveness do not need to be complex and resource-intensive undertakings. Healthcare providers and their internal audit functions can leverage established business processes to integrate IT governance effectively, and slice assessments to focus attention solely on specific areas and high-profile initiatives.

Businesses in the healthcare field and their IT leadership, with guidance from internal audit, need to adjust their IT governance approach continuously to ensure IT decisions made in the enterprise are generating the desired business value.

IT governance—like any risk and opportunity assessment—is by no means a “set it and forget it” endeavor. Technology is dynamic and always evolving; so, too, are healthcare organizations, their operations and their strategies. But having an effective IT governance approach in place can help you adapt to changing technology and business demands in the healthcare field with greater speed and confidence.

Measuring IT Governance Maturity

Because there is no one-size-fits-all approach to IT governance, audit teams will want to consider several potential states of IT governance maturity and seek to:

- Understand the current state
- Identify an appropriate target state
- Identify steps to improvement (to move from current state to future state)

Maturity modeling measures IT governance progression from the initial state (ad hoc/chaotic) to the optimized state (continuous improvement). It is important to note that many, if not most, healthcare organizations will not need to reach an optimized state in their IT governance, as it is neither necessary nor cost-effective.

Instead, they should work toward defining their appropriate target level of maturity for each of the five key elements of IT governance. Determining the current state of IT governance maturity is important, but so too is identifying the appropriate target state—without idealizing. Maturity modeling can help with benchmarking the current state of the IT function.

A standard by which process effectiveness can be appraised is the Capability Maturity Model, developed by Carnegie Mellon University.

Authors

Susan Haseley is a managing director with Protiviti, a global business consulting and internal audit firm. Susan leads the firm’s national healthcare practice. You can reach Susan by telephone at (469) 374-2435 and by email at Susan.Haseley@protiviti.com.

Jason Brucker is an associate director with Protiviti, a global business consulting and internal audit firm. Jason can be reached by telephone at (415) 402-6937 and by email at Jason.Bruker@protiviti.com.