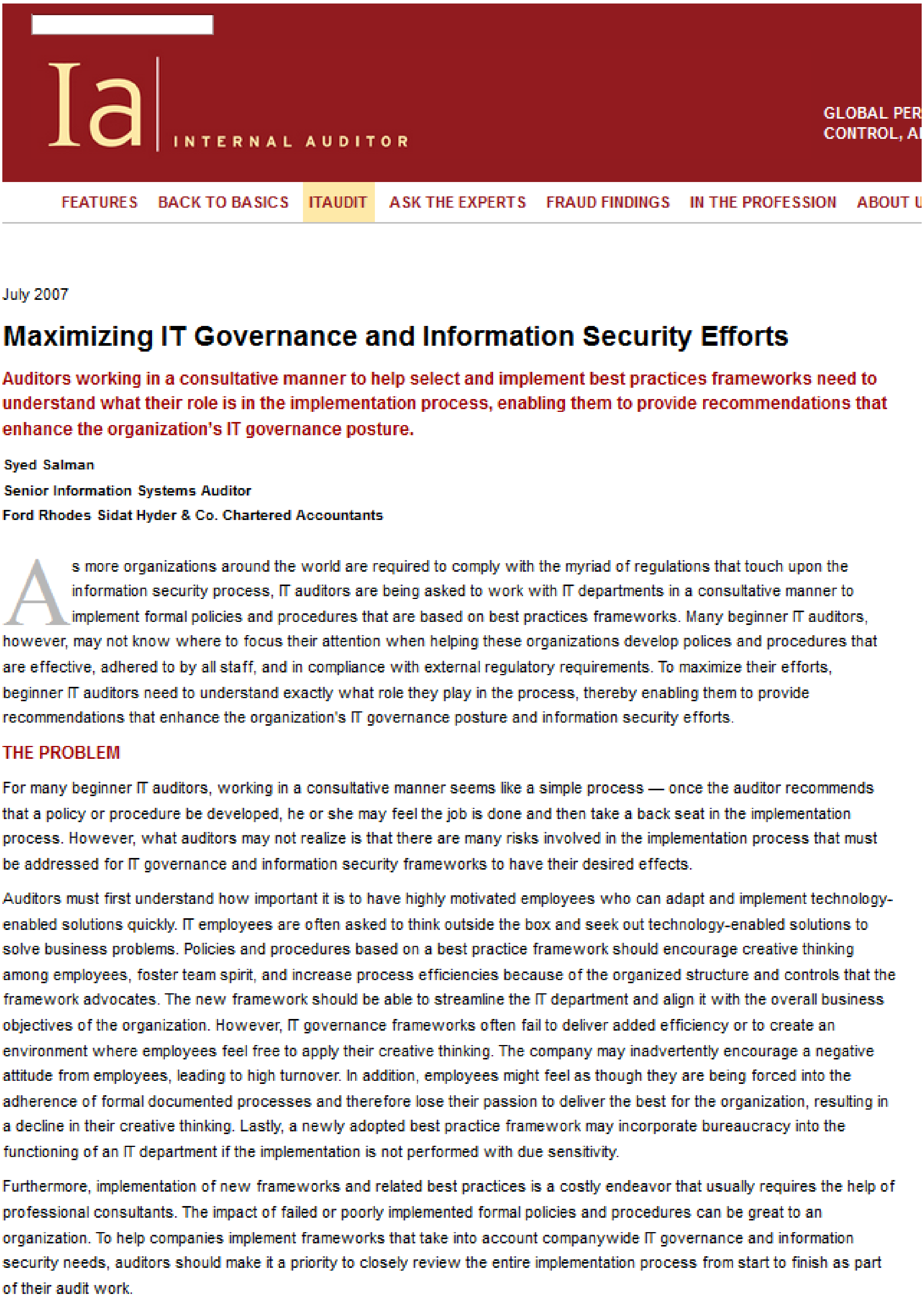


July 2007

# Maximizing IT Governance and Information Security Efforts

**Auditors working in a consultative manner to help select and implement best practices frameworks need to understand what their role is in the implementation process, enabling them to provide recommendations that enhance the organization's IT governance posture.**

**Syed Salman**
**Senior Information Systems Auditor**
**Ford Rhodes Sidat Hyder & Co. Chartered Accountants**

As more organizations around the world are required to comply with the myriad of regulations that touch upon the information security process, IT auditors are being asked to work with IT departments in a consultative manner to implement formal policies and procedures that are based on best practices frameworks. Many beginner IT auditors, however, may not know where to focus their attention when helping these organizations develop polices and procedures that are effective, adhered to by all staff, and in compliance with external regulatory requirements. To maximize their efforts, beginner IT auditors need to understand exactly what role they play in the process, thereby enabling them to provide recommendations that enhance the organization's IT governance posture and information security efforts.

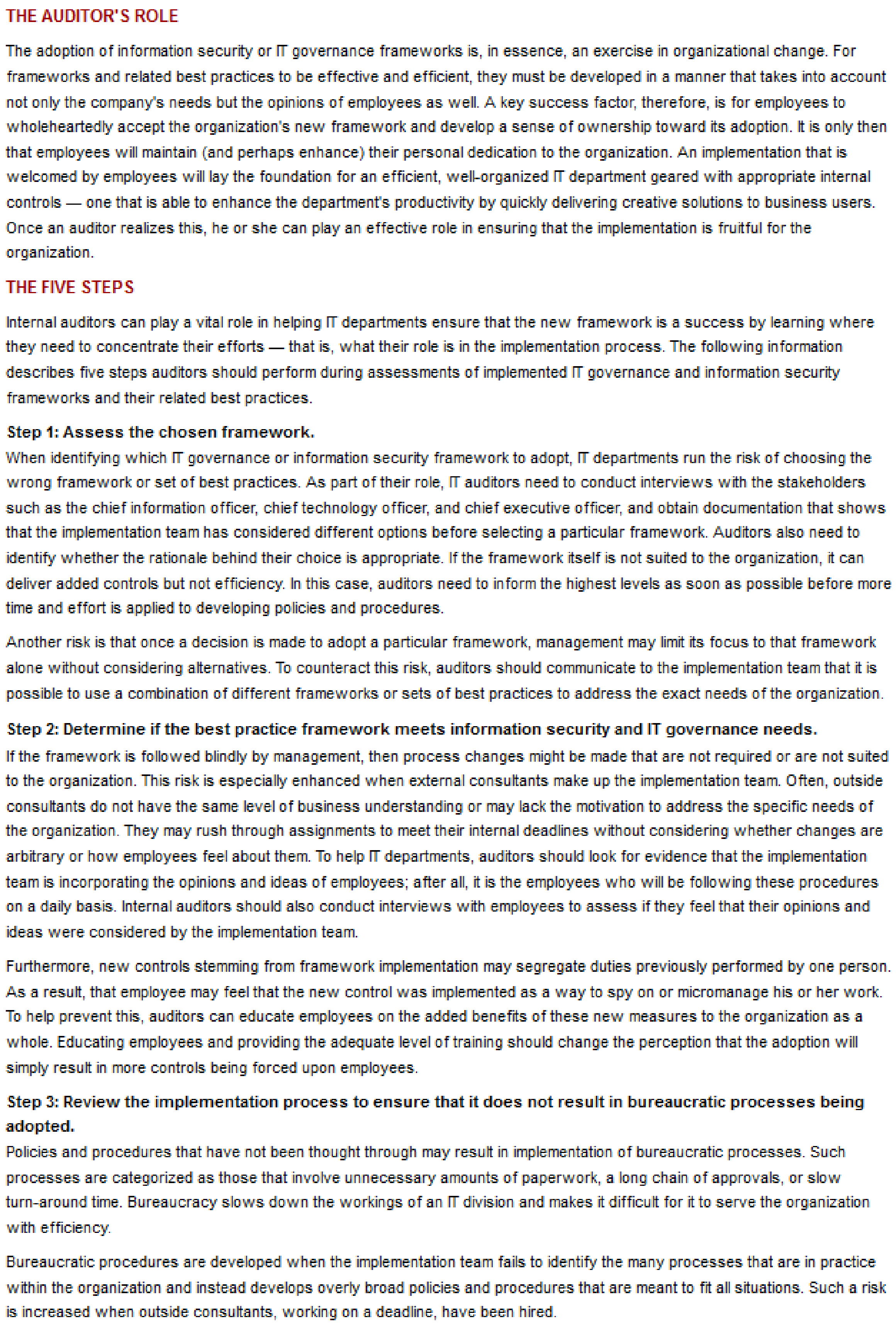
## THE PROBLEM

For many beginner IT auditors, working in a consultative manner seems like a simple process — once the auditor recommends that a policy or procedure be developed, he or she may feel the job is done and then take a back seat in the implementation process. However, what auditors may not realize is that there are many risks involved in the implementation process that must be addressed for IT governance and information security frameworks to have their desired effects.

Auditors must first understand how important it is to have highly motivated employees who can adapt and implement technology-enabled solutions quickly. IT employees are often asked to think outside the box and seek out technology-enabled solutions to solve business problems. Policies and procedures based on a best practice framework should encourage creative thinking among employees, foster team spirit, and increase process efficiencies because of the organized structure and controls that the framework advocates. The new framework should be able to streamline the IT department and align it with the overall business objectives of the organization. However, IT governance frameworks often fail to deliver added efficiency or to create an environment where employees feel free to apply their creative thinking. The company may inadvertently encourage a negative attitude from employees, leading to high turnover. In addition, employees might feel as though they are being forced into the adherence of formal documented processes and therefore lose their passion to deliver the best for the organization, resulting in a decline in their creative thinking. Lastly, a newly adopted best practice framework may incorporate bureaucracy into the functioning of an IT department if the implementation is not performed with due sensitivity.

Furthermore, implementation of new frameworks and related best practices is a costly endeavor that usually requires the help of professional consultants. The impact of failed or poorly implemented formal policies and procedures can be great to an organization. To help companies implement frameworks that take into account companywide IT governance and information security needs, auditors should make it a priority to closely review the entire implementation process from start to finish as part of their audit work.

Continued…



## THE AUDITOR'S ROLE

The adoption of information security or IT governance frameworks is, in essence, an exercise in organizational change. For frameworks and related best practices to be effective and efficient, they must be developed in a manner that takes into account not only the company's needs but the opinions of employees as well. A key success factor, therefore, is for employees to wholeheartedly accept the organization's new framework and develop a sense of ownership toward its adoption. It is only then that employees will maintain (and perhaps enhance) their personal dedication to the organization. An implementation that is welcomed by employees will lay the foundation for an efficient, well-organized IT department geared with appropriate internal controls — one that is able to enhance the department's productivity by quickly delivering creative solutions to business users. Once an auditor realizes this, he or she can play an effective role in ensuring that the implementation is fruitful for the organization.

## THE FIVE STEPS

Internal auditors can play a vital role in helping IT departments ensure that the new framework is a success by learning where they need to concentrate their efforts — that is, what their role is in the implementation process. The following information describes five steps auditors should perform during assessments of implemented IT governance and information security frameworks and their related best practices.

**Step 1: Assess the chosen framework.**

When identifying which IT governance or information security framework to adopt, IT departments run the risk of choosing the wrong framework or set of best practices. As part of their role, IT auditors need to conduct interviews with the stakeholders such as the chief information officer, chief technology officer, and chief executive officer, and obtain documentation that shows that the implementation team has considered different options before selecting a particular framework. Auditors also need to identify whether the rationale behind their choice is appropriate. If the framework itself is not suited to the organization, it can deliver added controls but not efficiency. In this case, auditors need to inform the highest levels as soon as possible before more time and effort is applied to developing policies and procedures.

Another risk is that once a decision is made to adopt a particular framework, management may limit its focus to that framework alone without considering alternatives. To counteract this risk, auditors should communicate to the implementation team that it is possible to use a combination of different frameworks or sets of best practices to address the exact needs of the organization.

**Step 2: Determine if the best practice framework meets information security and IT governance needs.**

If the framework is followed blindly by management, then process changes might be made that are not required or are not suited to the organization. This risk is especially enhanced when external consultants make up the implementation team. Often, outside consultants do not have the same level of business understanding or may lack the motivation to address the specific needs of the organization. They may rush through assignments to meet their internal deadlines without considering whether changes are arbitrary or how employees feel about them. To help IT departments, auditors should look for evidence that the implementation team is incorporating the opinions and ideas of employees; after all, it is the employees who will be following these procedures on a daily basis. Internal auditors should also conduct interviews with employees to assess if they feel that their opinions and ideas were considered by the implementation team.

Furthermore, new controls stemming from framework implementation may segregate duties previously performed by one person. As a result, that employee may feel that the new control was implemented as a way to spy on or micromanage his or her work. To help prevent this, auditors can educate employees on the added benefits of these new measures to the organization as a whole. Educating employees and providing the adequate level of training should change the perception that the adoption will simply result in more controls being forced upon employees.

**Step 3: Review the implementation process to ensure that it does not result in bureaucratic processes being adopted.**

Policies and procedures that have not been thought through may result in implementation of bureaucratic processes. Such processes are categorized as those that involve unnecessary amounts of paperwork, a long chain of approvals, or slow turn-around time. Bureaucracy slows down the workings of an IT division and makes it difficult for it to serve the organization with efficiency.

Bureaucratic procedures are developed when the implementation team fails to identify the many processes that are in practice within the organization and instead develops overly broad policies and procedures that are meant to fit all situations. Such a risk is increased when outside consultants, working on a deadline, have been hired.

Continued…

A good example is the software development life cycle. Procedures that define the entire software development life cycle should require a methodology, approvals, feasibility studies, and consultations with executives across the organization. However, this procedure is suited to large scale development projects but is impractical for small projects. Therefore, procedures relating to software development should include provisions for smaller projects whereby extensive and meaningless documentation or approvals are bypassed.

Internal auditors should ensure that the implementation process incorporates the means to identify all of the processes that the organization faces and hence develop practical policies and procedures with which to address them. One way is to hold brainstorming sessions with employees specifically to identify all processes in place in the organization. This step could help ensure that policies and procedures are practical and will not result in the development of bureaucracy.

**Step 4: Review the approval process.**

Although the U.S. Sarbanes-Oxley Act of 2002 and other regulations have changed the way most executive boards approve the implementation of IT best practices and frameworks, many boards still approve implementation without assessing if the framework meets the organization's needs. The board may feel that they are not in a position to comment on IT-related issues or they do not understand these issues. Internal auditors should assess whether the implementation team is making an effort to ensure that executive boards completely understand the IT governance or information security framework.

Auditors should also recommend that the implementation team achieve this understanding by giving detailed, clear, and non-technical presentations to the board that explain the framework's policies and procedures. During these presentations, the board should be made to feel comfortable with and understand the documentation, the processes and technical solutions to be implemented, the organizational structure to be adopted, and the procedural measures to be incorporated. The implementation team should be available to answer any questions or queries the board might have.

**Step 5: Evaluating post-framework implementation.**

Once the documentation is completed, technical methods are applied, procedural measures are established, and organizational structures are put in place according to the newly adopted framework, end users will often request changes. If management is too rigid and does not incorporate reasonable demands, end users may feel disgruntled. To help IT departments prevent the presence of unhappy employees, auditors should determine whether sufficient avenues to discuss the framework have been established with employees and whether senior management is making an effort to obtain and validate their opinions. Furthermore, they should gain an understanding of how end users feel regarding the newly adopted framework by focusing on signs of dissatisfaction or views that the new framework is not maximizing company processes. Views from different business users of the organization should be taken by internal auditors to see how they feel the IT department is operating with the newly adopted IT governance framework.

**Framework Choices**

Popular framework choices and best practices for IT governance and information security include the UK's Office of Government Commerce IT Infrastructure Library, ISACA's Control Objectives for Information and Related Technology, and the International Organization for Standardization's 27001: 2005 Standard, *Specification for an Information Security Management System.*

## BECOMING AN ACTIVE PLAYER

When auditors understand their role in assuring that the implementation team is considering the organization's needs and the opinions of employees, they can greatly improve the organization's implementation of a framework.

**Syed M. Salman** is a senior information systems auditor for Ford Rhodes Sidat Hyder & Co. Chartered Accountants, an Ernst & Young International member firm in Pakistan. Previously, he worked for Deloitte in Karachi, Pakistan. Salman has conducted reviews of general computer controls in companies where computer processing environments play a dominant role in business operations in Pakistan and the Middle East. He has been a part of business continuity planning efforts at major financial institutions.