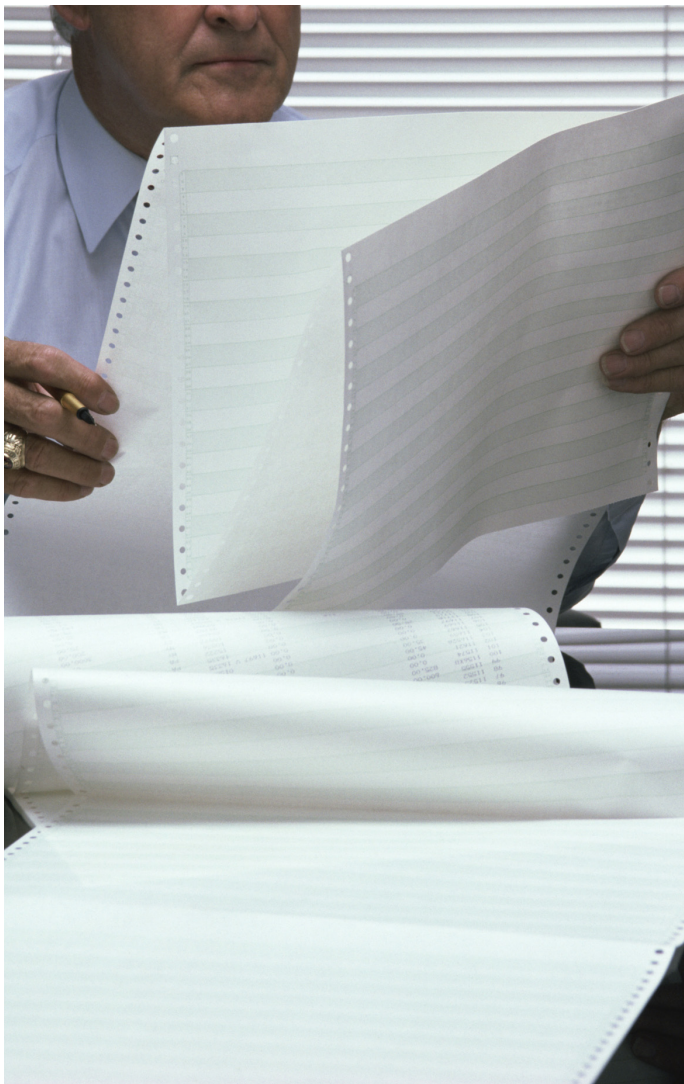


Risk Management: The other big shared services benefit



Shared services organizations (SSOs) have long enjoyed a well-deserved reputation for helping large companies to cut administrative costs. Now, in a world full of regulations and intense public scrutiny of corporate financial practices, another, less obvious shared services benefit is beginning to share the limelight: the ability to better manage risk. Done well, adopting shared services can help companies not only significantly reduce the risk of financial misstatements and fraud, but also increase audit and compliance efficiency. Here's how.

How shared services works

An SSO is an in-house organization that consolidates business processes from multiple divisions, subsidiaries, or locations into one or several "shared" organizations to eliminate redundant processes, systems, and organizations. Most SSOs include finance processes such as accounts payable, fixed assets, and general accounting, many of which generate the raw data used for a company's financial reporting and compliance activities. SSOs can also house information technology (IT) processes such as server management, data center operations, and security and controls. Typically, an IT SSO hosts the essential data (including financial data) and IT infrastructure used to run the business, providing data and applications to the operating units from a central location. Other processes often placed in an SSO include HR processes such as payroll, pension/benefit administration, and hiring and on-boarding; procurement processes such as purchase order processing, invoice entry, payment, spend analysis, and sometimes even knowledge-based functions such as research and development, legal, and marketing.

Regardless of what processes they house, all SSOs strive for certain characteristics in order to deliver their cost-saving benefits. An SSO usually operates out of one or, at most, a few low-cost locations, resulting in a physical relocation of both people and processes from the business units. SSO processes are standardized and automated for efficiency, and SSO personnel and the SSO's business-unit "customers" are expected to follow consistent procedures. Finally, SSOs find that using a single IT platform, especially if the same platform also supports the rest of the business, can improve their performance.

Shared services and risk management

The same factors that make shared services effective in lowering costs – consolidation, standardization, and streamlining – can also help companies improve the quality and reduce the cost of risk management. In fact, many organizations have already recognized the value of shared services in this area. In a 2007 Deloitte survey of shared services leaders, respondents reported that the benefit of improved controls due to shared services was nearly as important to their organizations as reduced operating costs.¹ These improved controls, moreover, can help companies save money: 53 percent of the survey respondents reported that their SSOs made compliance with the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) less expensive than it would have been without shared services.²

Improving risk management quality and reducing its cost are two key goals of Risk Intelligence, an enterprise-wide approach to risk that, among other things, helps an organization to more effectively manage risk across organizational silos, use standardized risk management processes and metrics, and consider risk management an organization-wide responsibility.³ Shared services can help organizations pursue a Risk Intelligent approach in a number of ways. Among the most important:

- **Process standardization.** Standardizing processes as part of a shared services implementation can improve enterprise-wide control effectiveness in two ways. First, standardizing SSO training programs and customizing the training to be specific to the SSO's processes and systems allows all SSO personnel to be trained to follow the same procedures in the same way. This can help maintain common business processes, which are easier to monitor than disparate business processes. Second, when implementing an SSO, a company can evaluate the controls in place over each process at the business units, decide which controls are most effective, and implement the most effective practices at the SSO, bringing the entire SSO's control effectiveness up to the standard formerly achieved by only the most effective business unit.
- **Technology standardization.** Standardized technology can improve information quality and reduce the probability of errors. If an SSO uses a single technology platform – especially if the business units also use that same platform – information can be processed more effectively than if data had to be converted to be compatible with different systems and applications or if it were manually managed using spreadsheets.
- **Personnel consolidation.** Centralizing the people doing the work – for example, the programmers responsible for maintaining a company's IT environment – into a single location makes them easier to supervise, reducing the risk of fraud.

Case study: Shared payroll process reduces risk of errors, unethical behavior

One large manufacturer's shared payroll process illustrates several ways that using an SSO can help manage the risk of errors and unethical behavior. All of the company's U.S. locations must enter the number of either hours or dollars to be paid into a central mainframe system, which compares the entries to the location's labor (time and attendance) system data to verify that the amounts requested by payroll equal the number of employee hours captured through the time and attendance process. Once a location's payroll entries match the labor data, the SSO processes the location's payroll, initiates direct deposits, and prints and mails all checks from the SSO's central facility. The SSO is also responsible for processing all third-party payments (such as withholding taxes and union dues) as well as for sending a direct deposit file to the company's bank.

Because the corporate locations do not have access to check stock, they cannot process manual payments to employees, reducing the risk of unauthorized payroll payments. In addition, the SSO team analyzes various aspects of payroll, including payroll accruals, reconciliations, garnishments, and benefits, to verify the validity and accuracy of payroll entries. These analyses are performed by employees who are not able to process payrolls, reducing the possibility that the same person could create inappropriate payroll entries and cover them up during the verification process.

The SSO also uses its bank's positive pay service to help prevent invalid or fraudulent checks from clearing. The fact that the bank receives the entire U.S. company's paycheck information from a single point of contact in the SSO – as opposed to collecting that information from multiple locations – streamlines and strengthens control over the positive pay process. Finally, the SSO's system security is configured to limit SSO staff access to payroll-related functions, reducing the risk that SSO employees will be able to tamper with the process.

- **Segregation of duties.** At companies whose SSOs employ more people than were employed in back-office functions at any one business unit, the scale of the SSO may make it easier to maintain separation between key financial and IT-related responsibilities. The SSO's size can allow the company to assign different parts of a sensitive task to different SSO staff, whereas a business unit may not have enough people to always do so.

- **Separation from the business units.** Separating certain processes from the business units can help companies implement checks and balances aimed at reducing fraud. For example, requiring an SSO to approve and process a purchase order submitted by a business unit can reduce the ability of a business-unit employee, acting on his or her own, to make fraudulent purchases.
- **Process consolidation.** Consolidating processes in the same physical location can improve audit efficiency by streamlining the testing of processes and controls required by Sarbanes-Oxley and other regulations. Instead of testing processes and controls at each business unit, the company's internal and external auditors can perform the bulk of their testing on the consolidated processes and controls at the SSO, then give each business unit a certificate of the results (often referred to as a clearance memorandum) to support further compliance needs at the business-unit level.
- **Automated controls.** Automating controls as part of an SSO implementation – for example, enabling automated, systematic matching of accounts payable invoices to purchase orders and receivers – reduces opportunities for human error and fraud. In addition, automated application controls within an SSO's standard software applications often need much less testing than manual controls, further reducing the effort needed for Sarbanes-Oxley compliance and internal audit. We have seen automation and process consolidation drive tremendous savings – savings that are typically not captured in the initial shared services business case – at companies that implement regional SSOs that take ownership of key internal controls, removing the burden and cost from each historical business unit audit.

Reaping the benefits

With benefits like these, why don't more people appreciate shared services' potential role in improving risk management? Partly, it may be because the risk-management benefits simply aren't as obvious, or as easily quantifiable, as the cost-saving benefits. But it may also be because the risk-management benefits – like the cost-saving benefits – aren't necessarily easy to achieve.

Ineffective execution of the shared services model can sabotage risk management efficiency and effectiveness in a variety of ways. For instance, if financial processes continue to take place in the business units as well as at the SSO, a company will not be able to take full advantage of the SSO's ability to improve audit efficiency through process consolidation. Similarly, if an SSO lacks effective automation, or if it operates on several different technology platforms, the company will have difficulty realizing its potential technology-enabled benefits in both risk and cost reduction. And if a business unit generates a large number of exceptions to a standardized process, the complexity of the work increases along with the probability of error, especially since exceptions may not be as tightly controlled as the standardized process.

Case study: IT SSO helps combat fraud, improve internal control

At one large U.S. bank, an IT SSO plays a key role in helping maintain control and reduce the risk of fraud. All IT applications for the organization are developed and upgraded by the SSO in collaboration with a central office in charge of processes and controls for each of the bank's products. Once the software is developed, the central office pushes it out to a representative in each of the branches, who is responsible for installing it into the local IT environment with the involvement of local IT resources and for managing processes and controls at the local user level.

This service model helps combat fraud in a number of ways. The use of the IT SSO allows the bank to separate the software developers from the software implementers and users at each district. Because the same people are not both developing and using the software, no single programmer on either end has enough knowledge to either write or use the software to commit fraud. In addition, the design of the process prevents any local programmer involvement in the deployment to the production environment. The local offices, as they cannot change the applications once they have been finalized by the central office and the IT SSO, do not have the opportunity to commit fraud by tampering with the software.

A key to reaping the rewards of an SSO's risk-management benefits is getting the SSO to work effectively. A high degree of standardization is important, as is compliance with the SSO's policies and procedures. The following strategies can improve the odds:

- Maintain a strong tone at the top. Mandate use of the SSO if you can, and encourage it as forcefully as possible if an official mandate isn't feasible.
- Understand the local business environment well enough to anticipate and counter business-unit objections to SSO use based on country-specific factors. National works councils, privacy and security regulations, and other such factors may be cited for a country's inability to participate in a shared services model. Carefully investigate all such claims to determine if they're legitimate.
- Establish business-unit accountability for complying with the SSO's processes. Use individual performance management tactics to drive compliance – evaluate and reward people based on how well they work with the SSO.
- Keep all parties engaged and working together. Set up a number of explicitly defined governance mechanisms with clearly defined roles and responsibilities to encourage productive communication and collaboration among the SSO, the business units, and corporate headquarters.

The business case for shared services based on cost reduction is typically compelling. But the potential for shared services to improve a company's ability to manage risk more effectively adds even more weight to the shared services value proposition. Companies seeking to increase risk management efficiency and effectiveness would do well to explore shared services as a powerful tool.

Contacts

Kyle Cheney

Deloitte & Touche LLP
216-589-1387
kcheney@deloitte.com

Jeffrey Pierce

Deloitte & Touche LLP
216-589-5469
jepierce@deloitte.com

Susan Hogan

Deloitte Consulting LLP
404-631-2166
shogan@deloitte.com

David Hodgson

Deloitte & Touche LLP
973-602-6869
dhodgson@deloitte.com

About this publication

This publication contains general information only and Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, and Deloitte Financial Advisory Services LLP are not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, Deloitte Financial Advisory Services LLP, their affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication

References

- 1 *Shared Services Comes of Age: Pursuing broader business value on a global scale*, Deloitte Development LLC, 2007.
- 2 *Shared Services Comes of Age*, Deloitte Development LLC, 2007.
- 3 *The Risk Intelligent Enterprise: ERM Done Right*, Deloitte Development LLC, 2006.