Deloitte.

Business Integrity in Service Delivery

Doing the right things the reliable way

Growth is generally perceived to be good in a business context. Whether it is about entering new markets, expanding business capabilities, or acquiring other businesses, companies are increasingly being challenged to scale and/or to reposition themselves to gain competitive advantage and increase shareholder value. But, accommodating growth in the short-term can pose resource constraints, with companies often turning to shared services centers or outsourcing to drive efficiency and effectiveness. This in turn raises concerns about accountability and risk management. For instance, if work is shifting from corporate and the business units to shared services organizations, who is ultimately accountable? Who owns the profit and loss statement? Is there adequate visibility into transactions in different parts of the world? Are quality and integrity being compromised as the company makes dramatic infrastructure changes to people, process, and technology? These concerns fall under the purview of "business integrity," an emerging concept in risk management that deals with putting the controls, reporting, and governance structure in place to ensure that as a company grows, it does the right things the reliable way. In many instances, the shared services organization is well-positioned to add value regarding business integrity, if not be the full guardian of it.

What is business integrity?

Business integrity refers to having reliable data upon which to base decisions before, during, and after a significant structural change to the business. This change can involve the implementation of a growth strategy, such as a merger or acquisition, expansion of a business line, or entrance into a new market. Or, the change can be precipitated by a major market event, such as a new regulatory mandate or the availability of a new technology capability. Global business services (GBS) organizations and shared services centers come into play because companies frequently look to them to help manage these structural changes efficiently and effectively, often by expanding their capabilities and/or scaling them to handle more volume across different geographies. Indeed, anticipated growth in service delivery is significant. According to the 2015 Deloitte Shared Services Survey, 81 percent of respondents expect companies to move more functions—both transactional and knowledge-based—to shared services centers, especially in the areas of finance,

human resources, information technology, accounting, and tax. Just as companies are increasingly looking to their shared services centers to scale capabilities, they now have an additional opportunity to leverage them for maintaining business integrity.

How can business integrity add value to shared services?

Shared services centers work with cross-functional processes and data so they are well-positioned to add value by being the guardians of business integrity. Companies can better manage their risks and improve their overall business performance by adopting the principles of business integrity within their shared services functions. As illustrated in Figure A, these principles can be grouped into six focus areas, which center upon: 1) clear accountability as well as efficient workflow and document management; 2) accuracy in processing and customer satisfaction; 3) completeness in transactions and implementation of standard, global policies with common procedures; 4) audit-ready controls that are performed in a timely manner to detect errors; 5) holistically driven compliance, along with policies that provide adequate guidance; and 6) information security and brand protection. Here are a few examples of how putting these principles into practice can add value to shared services centers of excellence:

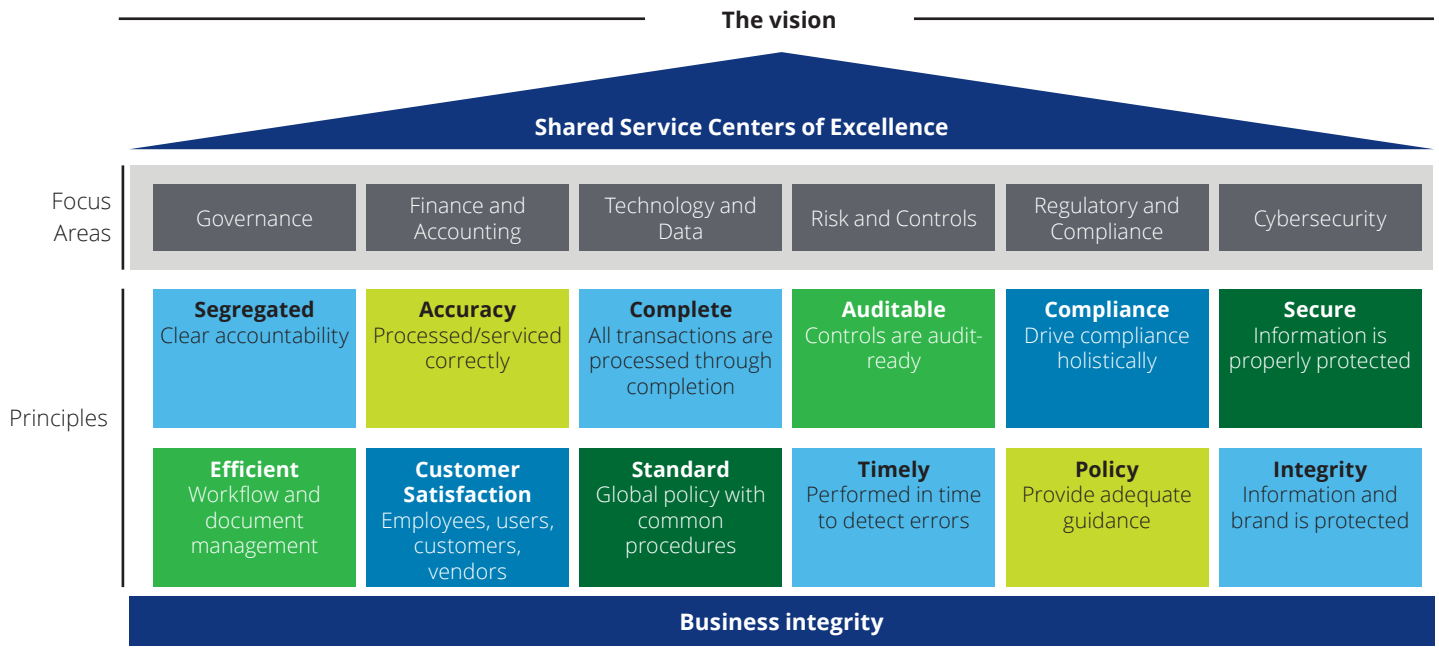
1. **Governance**—A strong governance and compliance model is essential as shared services centers scale and adapt to accommodate growth. Organizations will need to manage expectations and develop a common approach to address the governance of people, processes, and technology during service delivery transformation. However, misalignment among teams concerning controls and risk management activities is a common pitfall. That is why organizations should consider establishing an oversight and monitoring function to ensure that teams are aligned and that they are implementing controls and executing compliance practices in an effective, standardized way. In addition, the company's internal audit group can aid the governance process by performing readiness activities during process design. After the transformation, processes and controls should be continuously monitored and frequently tested. Business leaders, for instance, should have the authority to oversee the alignment of business processes with company policies, validate compliance with regulations, and evaluate risk measurement methods (i.e., key performance indicators and key risk indicators).
2. **Finance and accounting**—During rapid growth, accuracy is often compromised due to differences in how data is entered and stored and the way in which metrics and ledger items are defined. For instance, as companies come together in mergers and acquisitions (M&A), they may need to rationalize their product offerings or business lines. But, if you want to make informed, fact-based decisions about what to keep and what to divest, you must first have integrity between the definitions and data sources. Take profitability for example. Companies often define profitability differently in terms of cost inputs and revenue sources. The same goes for expense classifications. For instance, one company may classify advertising cost as a selling, general, and administrative expense, while another might embed it into cost of goods sold. A shared services center of excellence in accounting and finance can assist in aligning these definitions, as well as in assessing the quality and accuracy of data sources.
3. **Technology and data**—With its enterprise view of technology and data sources, shared services can play an important role in securing data, while improving its quality and providing appropriate access. For instance, careful attention should be paid to designing the user authorities for payments approvals and vendor master files when setting up a transaction-based accounts payable function within a shared services center. Lack of strong controls could lead to inappropriate payments or even embezzlement—not to mention that companies could miss out on the upside potential in getting things right. For instance, a newly acquired or expanded part of the business may be entitled to a five percent discount if it pays a vendor within 10 days. But, if the payment terms have not been captured or recorded correctly in the corporate enterprise resource planning system, the enterprise may forgo the early payment discount or miss other opportunities to take advantage of its enhanced purchasing power. In the end, it is about verifying the definitions and sources of data so a company can understand the true risks and rewards associated with its growth strategy.
4. **Risks and controls**—As a company grows, risk management is a frequent area of misalignment. Take credit risk for example. As a company gains or inherits new customers, decision makers should assess the credit risk they represent. However, different parts of the company may have different policies around granting credit, assigning interest rates, and collecting balances due. Additionally, if credit-related data is coming into a shared services center from disparate sources, you should question if it has been manipulated in some way. A strong risk management program can be instrumental in spotting areas of misalignment or manipulations, such as when stores or sales people have overridden the credit limits established by corporate. Such a program is also vital for putting checks and balances in place so the situation does not occur again.
5. **Regulatory and compliance**—When a company scales, a shared services center, governed by the principles of business integrity, can provide stability by helping to ensure that critical knowledge is retained, compliance requirements are understood globally, and important documents are aggregated and centralized. For instance, the Financial Accounting Standards Board recently released guidance on lease accounting designed to improve financial reporting about leasing transactions. Many companies,

however, do not store their leases, or other types of contracts for that matter, all in one place. Shared services offers companies an opportunity to create a centralized contract management database through which data integrity can be verified, compliance processes can be expedited, and value-generating analyses can be performed. There is an additional upside: shared services personnel, through compliance programs, could investigate when leases expire or examine how long it has been since they were first signed and whether or not they are recurring or "evergreen." In an M&A context, they might find opportunities to renegotiate, consolidate, or restructure in light of the collective needs and purchasing power of the newly combined company—all of which could potentially reduce costs.

6. **Cybersecurity**—Implementing a strong, coordinated cybersecurity program is becoming increasingly important to delivering business services and protecting brand reputation and customer trust, particularly as a company scales. Standardized security frameworks, policies, controls, protocols, tools, methods, governance, and monitoring are all required to maintain business integrity amid a growing range of cyber threats. For instance, as companies expand into new geographies, centralized authentication and authorization capabilities are key to maintaining system security and preventing fraudulent transactions. Training and awareness is also critical and often overlooked. Furthermore, monitoring activities should not only be robust, but also integrated, encompassing physical locations and assets as well as systems and networks, so that security events can be readily spotted in a shared services environment. While cybersecurity practices must rapidly evolve to keep pace with the threat landscape, leading organizations today are deploying advanced security controls, such as next-generation firewalls with deep packet inspection and software-defined segmentation. Ultimately, maintaining business integrity is not just about protecting financial and customer data, but also safeguarding daily business operations.

Business integrity should be a mindset

Organizations can guard and improve overall financial and operational performance of their business by deploying principles for strong business integrity.



The expectation

- Well-designed and sustainable internal controls approach with emphasis on performance, accountability, and risk management.
- Focus on governance and continuous improvement will enable business and growth strategies.
- Securing data is key, however, better quality and access to data will help management decision making and driving synergies in the organization.

What is expected of shared services in maintaining business integrity?

As these examples illustrate, the outcomes of maintaining sound business integrity go beyond loss prevention and effective risk management to encompass improvements in profitability and business performance. But in order to reap the full range of benefits, shared services organizations must increasingly help the greater enterprise to "do the right things in a reliable way." In summary, they will increasing be expected to maintain a controlled and sustainable "audit-ready" environment in the midst of rapid change by:

- Taking a well-defined, sustainable approach to internal controls, emphasizing performance, accountability, and risk management.
- Focusing on governance and continuous improvement to enable performance and growth strategies.
- Securing data, which is key amid increasing cybersecurity threats; however, better data quality and access are also critical to supporting informed decision making and improving productivity by eliminating redundancy and manual processes.

How can you get started?

Shared services transformations are often strategic to achieving cost-effectiveness and scalability both within centers of excellence and throughout the enterprise as a whole. However, in the rush to achieve these important objectives, risk management is often an afterthought. Accordingly, many organizations approach risk management on an ad hoc basis through point solutions, addressing prominent pain points as they arise, such as mandatory audit compliance and network and systems access. Project teams often deal with internal controls after the transformation as opposed to designing them in tandem with the process and technology solutions. This causes significant problems downstream, including excessive costs, negative audit and compliance implications, potential loss of revenue, and penalties or fines.

Shared services organizations can start their journeys toward being the guardians of business integrity by considering risk management, compliance, and security at the beginning of any transformation effort. For instance, when evaluating service delivery models, the goal should not be to fit controls into the chosen solution, but instead to factor risk management, compliance, and security into the decision-making process. For example, when considering a captive versus an outsourced shared services center, decision makers should conduct a risk assessment to understand the threat landscape, as well as the potential areas of misalignment associated with each option. They can then compare the organization's existing risk and compliance framework to the target state operating model, identifying where controls will need to be added or revised in order to manage risk.

Ultimately, organizations should adopt a well-designed and sustainable internal controls framework that emphasizes performance, accountability, and risk management. This framework should be industry-specific and address both financial and operational risks. In terms of business integrity, this might mean developing controls that support the validity of purchase orders, accurate and complete delivery of goods and services, timely order fulfilment, veracity of pricing and margin calculations, and authorized access to networks and sensitive data.

Conclusion

Internal controls and risk management activities are often viewed as a "check the box" activity as a company scales. Strong internal controls, accurate internal and external reporting, and comprehensive risk management practices are key principles for maintaining business integrity. With significant value-creation potential as well as escalating risks, maintaining business integrity should be integral to a company's growth strategy. Shared services centers are well-positioned to enable this strategy by aligning definitions, establishing internal controls, and implementing a holistic risk management program to help ensure that the right things are being done, the reliable way.

Contact us:

Daniel Kinsella
Partner, Deloitte & Touche LLP
Tel: +1 402 997 7851
Email: dkinsella@deloitte.com

Janet Roth
Partner, Deloitte & Touche LLP
+1 713 982 4082
Email: jaroth@deloitte.com

Akshay Dhawan
Senior Manager, Deloitte & Touche LLP
Tel: +1 703 251 4127
Email: avdhawan@deloitte.com

Maria Bunch
Senior Manager, Deloitte & Touche LLP
+1 504 561 7169
Email: mabunch@deloitte.com