# Segregation of Duties and Sensitive Access: Leveraging System-Enforced Controls

BY LARRY CARTER

PUBLISHED BY COMPLIANCE WEEK

September 2014

# Contents

# Executive summary

EVERY ONCE in a while, a somewhat misunderstood aspect of internal control presents itself in a fresh light that calls attention to the value it can offer an organization. This e-book attempts to do just that, with an in-depth look at sensitive access (SA) and segregation of duties (SoD) – presenting essential information for business and IT users so they can gain a deeper understanding of the issue and capture greater benefit from it.

The book begins by discussing some of the standard views – and common misconceptions – about how segregation of duties should work, and highlights the effect that sensitive access and segregation of duties controls can have on fraud risk. It then offers a step-by-step approach that covers the process of SA/SoD discovery and control implementation. Applying this guidance can help to elevate internal control's "elephant in the room" into one of the critical pillars in an organization's control environment.

The core of this subject is not new; businesses have always been concerned with fraud and new ways to limit their exposure to fraud risk. Today, however, we see increased attention toward corporate fraud and the risks associated with the opportunity for fraud. It's coming from a number of places, such as:

- External audit firms are required under various auditing standards to consider and assess the risks related to fraud at their clients, specifically misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets. In addition, new standards from the Public Company Accounting Oversight Board (PCAOB) will ultimately require even more disclosure about procedures performed during the audit related to the detection of fraud.
- Technology and social media are evolving rapidly. Unfortunately, fraud risks are evolving right along with them, because the new technologies create even more pathways to *commit* fraud. With cloud computing, organizations have less control over access to their physical systems. At the same time, access to corporate applications and data is proliferating thanks to mobile technologies. Both cry out for a greater awareness of the need for strong access management.

- The COSO Internal Control Framework was updated and released in 2013. All public companies (and many other organizations) will need to align their control environment to comply with the new version before the end of 2014. The new framework contains an increased emphasis on risks related to fraud, and on maintaining appropriate segregation of duties. The principles contained in the amended version also call for management to consider greater reliance on IT for internal control.
- Segregation-of-duties is a control design that has never been understood as well as it should be. Rather, the tendency has been to assume (often blindly) that appropriate segregation was already in place, simply because it sounds like a good business practice. When you look more closely, however, you often find that more work needs to be done. When new business systems are implemented, segregation of duties rarely gets the attention it deserves. Many organizations that have recently implemented Governance, Risk and Compliance (GRC) software suites discovered serious risk exposure when they rolled out the access security and monitoring module – indicating that past confidence in segregation of duties was unwarranted.
- The strategy of "shared services" at a business has gone mainstream, which adds more complexity into processing business transactions. Along with the shift of accountability that comes with shared services, it's paramount that organizations pay increased attention to "who has access to what," to control operational and fraud risk.

How do you address this need for better SA and SoD? First, get a comprehensive understanding of the fraud risk exposure that exists within the organization; then design a control standard that leverages system-enforced access to reduce fraud risk to an acceptable level. The business and support processes need to be explored so you can determine the precise access rights that warrant attention, and create control activities to detect issues or exceptions. To ensure sustainability, activities to monitor the controls on a repeatable basis must be developed and placed into operation. Ideally, these control activities should reflect strong risk mitigation while requiring minimal effort to prove their effectiveness.

As straightforward as the above might sound, in reality it is a difficult challenge – because, as noted earlier, many audit and compliance professionals assume that this isn't a problem to begin with, *and that is not true*. You might reasonably believe that these control issues were fully covered as part of a system implementation, but in truth it takes a strong, targeted effort to unearth the gaps and deficiencies left unnoticed or unresolved. And if there is more than one application in the environment – which is the case at almost every business – it's almost assured that inter-application risks have never been considered.

Once you understand the challenge, the next steps may be just as perplexing. It's common to see the meeting room fill with deer-in-the-headlight looks when the topic moves to, "Precisely what needs to be done, and who is going to do it?"

Since these system-enforced access controls rely on IT systems to operate, they are often mis-labeled as "IT controls." They are *not* IT controls, even though the IT department plays a crucial role in managing them. SA and SoD controls are best viewed as "business controls" that leverage IT to enforce them.

The actual *creation* of SA and SoD control activities is a different story. The IT team doesn't always know which users need access to what, and the business owners aren't experts on system security. Even with cooperative effort between the two, it's likely that significant risk factors will be overlooked. The best answer is to assign *shared responsibility* for the development of these controls between the business and IT, with help from the compliance and internal audit teams. Oftentimes, it also requires external help by experts who specialize in security and systems access. Clear assignment of responsibilities and a concise plan are instrumental for success.

Successful development of SA/SoD controls also requires sound understanding of fundamental concepts of access, fraud risk, and how systems enforce the controls. This e-book provides a deep dive into the topics needed to gain working knowledge in such areas as: sensitive access (SA) and segregation of duties (SoD); the differences between detective and preventive controls; manual versus system-enforced controls; the principle of least privilege (PoLP); and the effect this has on the fraud triangle.

This book also offers a simple 11-step plan that begins by examining overarching business processes that exist within the organization to identify the risks that warrant mitigation. Access control rules are then established, and initial testing is performed. Following iterations of corrections and retesting, residual risk may warrant the discovery of complementary or alternative controls. Finally, suggestions about forming a periodic review process are provided.

Beyond the value of risk mitigation and stronger compliance that can be expected from completing this exercise, this new instrument in the internal control "tool kit" has even more to offer. Not only does this make good business sense toward risk mitigation and keeping honest people honest; it can be leveraged to increase the efficiency of compliance efforts.

After completing this project, management should (hopefully) be encouraged to incorporate more access-related controls into the control environment. Testing the effectiveness of these controls is extremely efficient; when based on process-level risk, they allow you to eliminate complimentary manual controls that are more time-intensive to test. In addition, this exercise will provide business management with solid examples of IT-automated controls that even the non-audit executive can understand. Comfort with the access-related controls will encourage greater adoption of automated controls embedded within the business. This includes the concept of "continuous controls monitoring," universally seen as the future of the control environment.

In conclusion, readers from all stakeholder realms will obtain a clear understanding of what these controls mean and why organizations struggle with identifying and implementing them. The e-book contains step-by-step instructions to establish a robust control design for organizations of all sizes. For C-suite leadership, it provides a compact overview needed to understand the problem and to work with audit and compliance executives solving it. For those involved in control design projects, or the adoption of an SA/SoD module that came with a purchased GRC software suite, participants will become more valuable contributors. For those fortunate enough to head one of these projects, they will find the information, guidance, and reference materials valuable for success.