Chapter 22
Detecting Compliance Failures in Unmanaged Processes

Yurdaer N. Doganata
IBM T.J. Watson Research, USA

ABSTRACT
The importance and the challenges of detecting compliance failures in unmanaged business processes is discussed, and the process of creating and verifying internal controls as a requirement of enterprise risk management framework is explained. The effect of using automated auditing tools to detect compliance failures against internal control points in unmanaged business processes is investigated. Risk exposure of a business process due to compliance failures is analyzed, and the factors that affect the risk exposure of a business process are evaluated.

INTRODUCTION
Detecting compliance failures help organizations better control their operations and remain competitive. The quality of product and services can not be ensured in a business if the processes do not conform to design goals and comply with the rules and regulations. Moreover, organizations may be subject to serious financial penalty as well as civil and penal consequences if they failed to comply with established guidelines, rules and regulations. Hence, the impact of non-compliance may have severe consequences that need to be managed either by reducing or eliminating the associated risk. Companies invest significantly on detecting compliance failures to ensure governance and manage risk. The cost of reducing the risk of being non-compliant could run into millions of dollars (Greengard, 2005). AMR Research survey reveals that the spending of companies on governance and risk management and compliance expected to grow to $29.8 billion in 2010, up nearly %4 over the $28.7 billion spent in 2009 (AMR Research, 2010).
Compliance can be managed relatively easy when the set of interrelated and interacting activities to achieve business goals are coordinated by business process management systems. This is the case where processes are well structured and documented. When the activities in a business process are structured enough, the transitions from one activity to another are automated by software systems. In a fully automated structured business process real time information about the status of various activities can be collected by business activity monitoring software (McCoy, 2002). Hence, compliance of processes against rules and regulations can be checked automatically. In such automated environments, the trace of the business operations is completely visible and it possible to know who did what and when.

In reality, business activities span multiple systems and organizations across modern enterprises, integrating legacy and newly developed software applications. There exists no single system or organization that controls the process end to end. Operations often depend on activities that rely heavily on human interaction without predefined control structures. Human actors decide what to do to achieve business goals. Since the transitions between human activities can not be fully automated or monitored by software systems, the visibility of end to end business operations is reduced. The processes that consist of such activities are called unmanaged processes. In the absence of business process management software with business activity monitoring that registers various aspects of the business operations, compliance check is usually performed manually by auditors, hence it is costly, time consuming.

There are primarily two challenges in ensuring compliance of unmanaged or partially managed processes. The first challenge is to increase the traceability of end to end operations. This requires tracking, capturing and correlating relevant aspects of the business operations. Once the visibility of the operations is increased, the second challenge is to create internal controls without depending on in depth knowledge of IT system and business application code. Creating and deploying new internal controls should be done without incurring additional IT cost. If the operations are tractable and the relevant business artifacts can be gathered, automated auditing systems and tools can detect compliance failures continuously and reduce the cost of employing auditors significantly.

In the absence of process automation software that can control and record who did what and when, the compliance check is a costly and time consuming task performed manually by auditors (AMR Research, 2010). Automated continuous auditing systems, on the other hand, provide for an almost cost-free auditing opportunity if the initial cost of building such a system is excluded. Such a system can run continuously and performs evaluation for all process instances without adding to the cost of auditing. While continuous auditing systems eliminate or reduce the dependency on audit professionals, they are not infallible. The tools that are built to realize automated continuous auditing rely on information extraction from process events and information, including e-mail transactions between the people within the organizations. The extracted information about the processes may contain errors and due to these errors the decision on the compliance may be faulty. Moreover, the testing of a compliance condition may require a level of text analysis that is not yet available in automated systems. Hence, the automated systems can perform fast and extensive auditing of the internal control points at the cost of making mistakes. As a result, some compliance failures may be missed while some other cases that are compliant may be declared non-compliant.

The focus of this chapter is to discuss the factors that impact the effectiveness of continuous assurance with automated audit tools. The subject is important for organizations which need to determine how much they should invest to remain compliant. The chapter helps understanding the characteristics of the operational environment that affects the efficiency of automated tools and
Related Content

A Research on Students’ Perceptions on a B-Learning English Environment to Improve Written Skills
Ana María Pinto-Llorente, Mª Cruz Sánchez-Gómez and Francisco José García-Peñalvo (2018).
Multidisciplinary Perspectives on Human Capital and Information Technology Professionals (pp. 179-201).
www.igi-global.com/chapter/a-research-on-students-perceptions-on-a-b-learning-english-environment-to-improve-written-skills/198257?camid=4v1a

Authentication, Authorisation, and Access Control in Mobile Systems
www.igi-global.com/chapter/authentication-authorisation-access-control-mobile/22048?camid=4v1a

Employing Cost Effective Internet-Based Networking Technologies to Manage B2B Relationship:
The Strategic Impact on IT Security Risk
www.igi-global.com/article/employing-cost-effective-internet-based/65729?camid=4v1a

Security in Service Oriented Architectures: Standards and Challenges
www.igi-global.com/chapter/security-service-oriented-architectures/40592?camid=4v1a