Chapter 8
Internal Control Considerations for Information System Changes and Patches

Jeffrey S. Zanzig
Jacksonville State University, USA

Guillermo A. Francia III
Jacksonville State University, USA

Xavier P. Francia
Jacksonville State University, USA

ABSTRACT

The dependence of businesses on properly functioning information systems to allow organizational personnel and outside investors to make important decisions has never been more pronounced. Information systems are constantly evolving due to operational and security requirements. These changes to information systems involve a risk that they could occur in a way that results in improper processing of information and/or security issues. The purpose of this chapter is to consider related guidance provided in a Global Technology Audit Guide (GTAG) from The Institute of Internal Auditors in conjunction with current change and patch management literature in order to assist internal auditors and organizational personnel in better understanding a process that leads to efficient and effective information system changes. The authors describe how internal auditors and information technology professionals can work together with organization management to form a mature approach in addressing both major information system changes and patches.

INTRODUCTION

The businesses of today are highly dependent upon properly functioning information systems to provide reliable information to allow organizational personnel and outside investors to make a variety of important decisions. The information processing and reporting environment of organizations is not static. Information systems must maintain flexibility to meet an organization's ever changing needs for both reliable and secure information. Changes to information systems create the risk

that the changes will occur in a way that results in improper processing of information and/or security issues. For example, Knight Capital Group, Inc. recently suffered a $440 million trading loss resulting from changes in a computer program that were being made to integrate with a new system being installed by the New York Stock Exchange. "Knight uses complex computer algorithms to trade swiftly in and out of stocks while retail brokerages rely on the company to execute billions of dollars of trades a year for small retail customers (Strasburg & Bunge, 2012)." An error in the computer software allowed millions of improper trades to go through in less than an hour resulting in the tremendous losses (Strasburg & Bunge, 2012). This chapter provides valuable insight into having a proper framework for the identification and implementation of system changes.

In 2012, The Institute of Internal Auditors issued updated guidance in a Global Technology Audit Guide (GTAG) entitled *Change and Patch Management Controls Critical for Organizational Success*. This resource provides information to assist internal auditors in working with information technology professionals in managing information system changes. The concepts of change and patch management include processes "designed to manage the enhancements, updates, incremental fixes, and patches to production systems." The GTAG points out that the top five risk indicators of poor change management are:

1. Unauthorized changes,
2. Unplanned outages,
3. Low change success rate,
4. High number of emergency changes, and
5. Delayed project implementations.

The IT Governance Institute (ITGI) was organized in 1998 "to advance international thinking and standards in directing and controlling an enterprise's information technology." (IT Governance Institute, 2007) This organization is well recognized for their Control Objectives for Information and related Technology (COBIT) framework providing a common language model for information technology activities. Some of the guidance provided in COBIT 4.1 specifically addresses managing information technology changes. A number of the control objectives suggested by the ITGI can clearly be related to the steps of change management provided in the GTAG guidance. In addition, the ITGI provides a maturity model in regard to change management that could well be accomplished by appropriate application of the change management steps.

The purpose of this chapter is to consider the GTAG guidance in conjunction with current change and patch management literature in order to assist internal auditors and organizational personnel in better understanding a process that leads to efficient and effective information system changes. The GTAG guidance and COBIT framework provide valuable resources that can be used to help organizations reach a mature process of change management. The remaining sections of this chapter provide: some background on the change management process, an overview of the steps of change management, a description of different levels of maturity in the change management process, an overview of patch management, a discussion on the integration of patch management with change management, examples of case studies in change and patch management, and some future research directions and conclusions.

BACKGROUND

Changes to information systems are an inevitable process given dynamic business environments and the speed of technological advances. In years past, changes to information systems have been performed in a reactive manner that can result in both errors and downtime because appropriate planning and control have not been done due to the urgency of needed changes and the lack of a formal process for change.

Related Content

Introduction
Chetan Sankarand Karl-Heinz Rau (2006). *Implementation Strategies for SAP R/3 in a Multinational Organization: Lessons from a Real-World Case Study (pp. 1-24).*
www.irma-international.org/chapter/introduction/22470

A Security Blueprint for E-Business Applications
Jun Du, Yuan-Yuan Jiaoand Jianxin ("Roger") Jiao (2009). *Selected Readings on Information Technology and Business Systems Management (pp. 416-426).*
www.irma-international.org/chapter/security-blueprint-business-applications/28651

Big Data and Machine Learning: A Way to Improve Outcomes in Population Health Management
Fernando Enrique Lopez Martinezand Edward Rolando Núñez-Valdez (2018). *Protocols and Applications for the Industrial Internet of Things (pp. 225-239).*
www.irma-international.org/chapter/big-data-and-machine-learning/202569

The Assessment of Outsourcing IT Services using DEA Technique: A Study of Application Outsourcing in Research Centers
Mohammad Amin Zare, Mohammad Taghi Taghavi Fardand Payam Hanafizadeh (2016). *International Journal of Operations Research and Information Systems (pp. 45-57).*
www.irma-international.org/article/the-assessment-of-outsourcing-it-services-using-dea-technique/142854

Perishable Inventory System with Server Interruptions, Multiple Server Vacations, and N Policy
K. Jeganathan, N. Anbazhaganand B. Vigneshwaran (2015). *International Journal of Operations Research and Information Systems (pp. 32-52).*
www.irma-international.org/article/perishable-inventory-system-with-server-interruptions-multiple-server-vacations-and-n-policy/125661