A Consensus of Thought in Applying Change Management to Information System Environments

Jeffrey S. Zanzig, Jacksonville State University, Jacksonville, AL, USA
Guillermo A. Francia III, Jacksonville State University, Jacksonville, AL, USA
Xavier P. Francia, Jacksonville State University, Jacksonville, AL, USA

ABSTRACT

Failure to keep pace with rapid developments in information technology can subject an organization to inefficiencies in obtaining reliable information that is imperative in making important decisions. The concept of change management attempts to move organizations in an efficient manner toward a desirable future state. In the realm of information processing, there is a continuing development of thought as to an appropriate framework to cover a vast array of issues from patching a specific software application to changing an overall system to better meet the strategic issues of an organization’s environment. This article considers related guidance provided in a Global Technology Audit Guide (GTAG) from The Institute of Internal Auditors, COBIT from the ISACA, and current change and patch management literature in order to demonstrate that there is a common stream of thought in the evolution of a framework for applying change management to information systems.

Keywords: Change Management, COBIT, Configuration Management, Internal Audit, Patch Management

INTRODUCTION

The functioning of organization information systems is constantly adapting to provide reliable information to allow organizational personnel and other stakeholders to make a variety of important decisions. 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. 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.” 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 and Bunge, 2012). In another incident, a software configuration error at Goldman Sachs mistakenly “converted the firm’s ‘contingent orders’ for various options series into live orders and assigned them all a price of $1.” In a recent press release, the Securities and Exchange Commission (SEC) concluded that “Goldman’s written policies relating to the implementation of software changes did not require several precautionary steps that, if taken, would likely have prevented the erroneous options incident. Goldman Sachs agreed to pay a $7 million penalty to settle the charges (SEC, 2015)”.

In 2012, The Institute of Internal Auditors (IIA) 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 ISACA is well recognized for developing international information system auditing and control standards. They are particularly well known for their Control Objectives for Information and related Technology (COBIT) framework. COBIT 5 “helps enterprises create optimal value from information technology (IT) by maintaining a balance between realizing benefits and optimizing risk levels and resource use.” The management process of COBIT 5 contains four domains:

- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

For each of the above domains, COBIT 5 contains descriptions of specific management practices to consider in establishing a variety of purposes within the domain. COBIT 5 states that “each enterprise must define its own process set, taking into account its specific situation.” In addition, the ISACA provides a process capability model in COBIT 5 that possesses some overlap with the maturity model of COBIT 4.1 (ISACA, 2012a).

This article considers the GTAG and COBIT guidance in conjunction with current change and patch management literature for the purpose of showing common threads of thought as to major components that should exist in applying change management to information system environments. Both the GTAG guidance and COBIT framework provide valuable resources that can be used to help organizations reach a higher level of process capability over change management. Specific COBIT 5 management practices are provided within the discussion to show examples of the relationship between the GTAG and COBIT. The remaining sections of this article provide: some background on the change management process, an overview of the steps of change management, an overview of patch management, measuring capability over information system changes, and some future research directions and conclusions.

**BACKGROUND**

Before the use of computer technology, competently trained and honest persons were pretty much the exclusive source of ensuring proper information processing. Although technology can never replace the value of such persons, human beings are subject to occasional mistakes and situations that may tempt them to manipulate information. For example, inadequately trained employees may incorrectly process information. In other cases, fraudulent financial reporting has
How to Create a Credible Software Engineering Bachelor's Program: Navigating the Waters of Program Development
www.igi-global.com/chapter/create-credible-software-engineering-bachelor/29605?camid=4v1a

Security Integration in DDoS Attack Mitigation Using Access Control Lists
www.igi-global.com/article/security-integration-in-ddos-attack-mitigation-using-access-control-lists/208639?camid=4v1a