


Chapter 6

Assurance for Change Management With COBIT 2019 and CMMC Maturity Frameworks

Jeffrey S. Zanzig
Jacksonville State University, USA

Guillermo A. Francia, III
 <https://orcid.org/0000-0001-8088-2653>
University of West Florida, USA

ABSTRACT

As technology plays an ever-increasing role in carrying out structured tasks in today's society, people are given more time to focus their attention on higher levels of service and personal development. However, technology is in a constant state of change and assurance services are needed to help ensure that technology changes are accomplished properly. The Institute of Internal Auditors has identified 10 steps that can be used to effectively implement changes in technology. This process and its accompanying internal controls can be assessed through an internal audit function that considers issues of both functionality and security. In addition, continuous improvement of the change management process for technology can be evaluated through capability/maturity models to see if organizations are achieving higher levels of accomplishment over time. Such models include the COBIT 2019-supported capability maturity model integration (CMMI) model and the cybersecurity maturity model certification (CMMC) framework used by defense industrial base organizations.

DOI: 10.4018/978-1-7998-4799-1.ch006

INTRODUCTION

The technology of today provides organizations with a tremendous ability to store and process information so that people have more time to focus on higher-level activities that are considered to add more value in meeting customer needs. This does not mean that technology once implemented relieves organizations of the need to understand and revise the functioning of computer systems. Current issues of today including privacy of personal data, theft of trade secrets, and safety of company products and services are all affected by the ability of organizations to properly implement changes to the applications that make up today's technology systems. The following examples illustrate that assurance over technology needs to address both issues of functionality and cybersecurity.

A number of tragic incidents involving computer glitches on the Boeing 737 MAX jet illustrates what can happen when computer software is changed but not adequately tested before being placed into operation. The original issues with the jet resulted from a problem in the plane's flight control system called MCAS that assisted in maintaining a proper balance of the plane while in flight. The system misfired in a manner that "repeatedly and forcefully pushed the planes' noses down, overpowering pilot commands and ending in fatal dives." Since the grounding of the 737 Max, Boeing has been working to revise the software to correct the problem by making such misfires less likely and easier for pilots to counter when they do occur. In their efforts to correct the software, Boeing ran into another glitch that stops the plane's flight control computers from powering up and confirming that the system is ready for flight. The software fix was originally tested mostly on ground-based simulators, which did not show the power-up problems (Pasztor, 2020).

A recent event at Garmin Ltd., who makes navigation systems for cars, boats, and planes, illustrates that organizations must also be careful to ensure that proper cybersecurity measures are built into their technology. The company's Garmin Pilot, which provides weather and flight plan data to pilots was recently interrupted when hackers apparently encrypted a few of its systems, but stopped short of a ransomware attack (Choi, 2020).

The ISACA is well known for its development of international information system auditing and control standards. One of their most significant contributions is a continuing project known as the Control Objectives for Information and related Technology (COBIT) framework. The management process of COBIT 2019 contains four domains:

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

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/assurance-for-change-management-with-cobit-2019-and-cmmc-maturity-frameworks/288086

Related Content

Initial Exploration of Cross-Generational Attitudes Towards Piracy of Chinese Online Literature

Rob Kim Marjerison and Sijia Jiang (2022). *Handbook of Research on Emerging Business Models and the New World Economic Order* (pp. 326-342).

www.irma-international.org/chapter/initial-exploration-of-cross-generational-attitudes-towards-piracy-of-chinese-online-literature/289989

Discussion and Conclusion

(2023). *Promoting Regional Industries Through Cross-Sectoral Collaborations: Regional System, Management, and the Management Body* (pp. 217-235).

www.irma-international.org/chapter/discussion-and-conclusion/331530

Towards Digital Transformation: Implications for Strategic Change

John Loonam (2021). *Reviving Businesses With New Organizational Change Management Strategies* (pp. 56-70).

www.irma-international.org/chapter/towards-digital-transformation/280447

Intersectionality in Leadership: Spotlighting the Experiences of Black Women DEI Leaders in Historically White Academic Institutions

Natasha N. Johnson (2023). *The Experiences of Black Women Diversity Practitioners in Historically White Institutions* (pp. 213-238).

www.irma-international.org/chapter/intersectionality-in-leadership/315864

Training for Crisis Situations: A Panoramic View of Theory and Practice Around the World

Helena Martins, Lisa Dollmann, Melanie Lehmann and Ana Cláudia Rodrigues (2023). *Measuring the Effectiveness of Organizational Development Strategies During Unprecedented Times* (pp. 237-267).

www.irma-international.org/chapter/training-for-crisis-situations/326541