Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2017 Proceedings | Southern (SAIS)

3-25-2017

Integration of the COBIT 5 Framework into the SDLC for Development of a User Access Attestation System

Lawrence Bunnell
Virginia Commonwealth University, bunnelll@vcu.edu

H. Roland Weistroffer
Virginia Commonwealth University, hrweistr@vcu.edu

INTEGRATION OF THE COBIT 5 FRAMEWORK INTO THE SDLC FOR DEVELOPMENT OF A USER ACCESS ATTESTATION SYSTEM

Lawrence Bunnell, MBA, MSIS
Virginia Commonwealth University
bunnelll@vcu.edu

H. Roland Weistroffer, PhD
Virginia Commonwealth University
hrweistr@vcu.edu

ABSTRACT

As organizations face increasing legal and regulatory oversight due to legislation such as SOX and HIPPA, controls for information technology (IT) have become a critical focus. Thus, it is essential that those charged with IT governance pay particular attention to which users may initiate, authorize, process, store, and report transactions. Periodic user access attestations, authorizing appropriate employee use of IT artifacts, are a means of ensuring that proper controls are maintained. Cost-efficient applications to support managing appropriate IT user access are needed to ensure regulatory compliance. This research maps the COBIT 5 framework to the systems development lifecycle (SDLC) to develop a user access attestation system using widely available in-house tools.

Keywords

IT Governance, user access attestation, identity governance, access management, COBIT 5, SDLC

INTRODUCTION

Compliance standards and legislative regulations such as *Sarbanes-Oxley* (SOX), *Gramm-Leach-Bliley* (GLB), and the *Health Insurance Portability and Accountability Act* (HIPAA), have resulted in an increasing emphasis for organizations to better realize information systems (IS) controls (Getter 2007, Li et al. 2012, Hodges 2013, Kushwaha et al. 2013, Wu et al 2015). An important part of information technology (IT) governance is identity governance and administration (IGA) through identity access management (IAM) lifecycle policies and procedures. These policies and procedures regulate which individuals may access and use corporate IS and when those access rights should transition or terminate. This is of acute relevance as it is estimated that currently 75% of organizations have gaps in their identity and access management perimeter (Iverson 2016), and the *Computer Emergency Readiness Team* (CERT) estimates that about 80% of malicious activities come from current and former employees (Moturi and Bitta 2013). Regular, periodic user access attestations, authorizing appropriate access and use of specific IT artifacts by employees and contractors are a key means of ensuring that proper IT governance risk management controls are maintained and that user access continues to comply with policies and procedures.

To ensure regulatory compliance and effective management of IT-related risks, cost-efficient applications to support ensuring appropriate IT user access are needed. The *Information Technology Governance Institute* (ITGI) and the *Information Systems Audit and Control Association* (ISACA) offer an open standard, the *Control Objectives for Information and Related Technology* (COBIT), enabling organizations to focus their IT activities in support of overall business goals such as information security. This research provides a roadmap for integrating COBIT 5 domain processes into the systems development lifecycle (SDLC) by demonstrating the development process for creating a user access attestation system. A prototype of the system is designed for future assessments of its efficacy in achieving IGA objectives related to user access attestation.

BACKGROUND AND CONTEXT

Contemporary user access attestation is a manual process whereby managers physically review a list of their employees' IS access privileges and either approve, modify or revoke authorizations to use or view particular IS artifacts, such as software applications, data, and financial reporting. In current practice, user access attestation can be a cumbersome process in organizations with thousands of employees, each of whom may have numerous and dynamic needs for access privileges to a variety of datasets, reports and applications. Reviews should examine the access levels of each individual in conformity with the concept of *least privilege*, and whether accounts are still active and management authorizations are up-to-date, etc. (Swanson and Guttman 1996). User access attestations allow organizations to demonstrate their adherence to two general information security rules applicable to access and use of information systems. One is *segregation of duties* (SoD), which refers to distributing roles, responsibilities and associated authorizations among multiple users, so that a single user is unable to circumvent or subvert a critical process (Swanson and Guttman 1996, Basin et al. 2012). SoD helps "eliminate 'toxic combinations' of access which may happen when an employee is transferred to a new position" (Nosseir 2010). The second

one is the principle of granting employees the 'least privileged' access necessary to carry out their job function. This mandates that "every user of a system should operate using the least set of privileges necessary to complete the job" (Saltzer and Schroeder 1975). User access attestation directly reduces risk by addressing threats associated with over-privileged, expired or potentially hazardous combinations of excessive access.

According to Gartner Research, there are a number of companies that have begun to deliver consolidated platforms to manage digital identity and access rights, including Atos (Evidian), CA Technologies, Dell Software, and IBM (Gaehtgens et al. 2016). However, installing and maintaining an IGA tool requires considerable software and professional services. IGA often consumes more of an identity and access management (IAM) program's capital and operating expenditure budget than all other IAM investments combined (Iverson et al. 2016). These applications handle various functions, such as 1) identity life cycle management, 2) entitlement management, 3) access requests, 4) workflow orchestration, 5) access certification, 6) fulfillment via automated connectors and service tickets, and 7) reporting and analytics. The focus of the research reported in this paper is on the specific IGA function of *user access attestation*, i.e. requiring managers and resource owners to certify the access rights that users have on a periodic basis, to ensure access continues to comply with policies (also called *user access certification*).

The remainder of this paper is organized as follows. First, after providing an overview of the COBIT 5 framework and of the systems development life cycle (SDLC), we map SDLC to the COBIT 5 domain processes. We then apply these mappings to demonstrate how to create a model for the development and implementation of a software system for user access attestation (AtTest), and describe a working prototype of the AtTest system using Microsoft's Sharepoint collaboration tools coupled with Nintex workflows. We conclude with noting the contributions, limitations and future research suggested by this study.

INTEGRATING COBIT 5 WITH THE SYSTEMS DEVELOPMENT LIFE CYCLE

COBIT 5

According to the ISACA website, COBIT is "the leading framework for the governance and management of enterprise IT" (ISACA 2016). COBIT is a holistic, integrated framework designed to assist in enabling the IT governance and management objectives of the organization. COBIT 5 is based on five principles: 1) *Meeting Stakeholder Needs*, which addresses the need to align individual and department objectives with enterprise and stakeholder needs; 2) *Covering the Enterprise End-to-End*, which recognizes the need for business managers to assume accountability for effectively governing and managing their use of IT; 3) *Applying a Single Integrated Framework, which* signifies the effort to allow alignment of COBIT with other IT governance frameworks currently in use, 4) *Enabling a Holistic Approach*, which emphasizes that efficient and effective implementation of governance of enterprise IT (GEIT) requires a systems approach, and 5) *Separating Governance from Management*, which indicates that GEIT processes entail different types of activities (Figure 1) (ISACA, 2014).

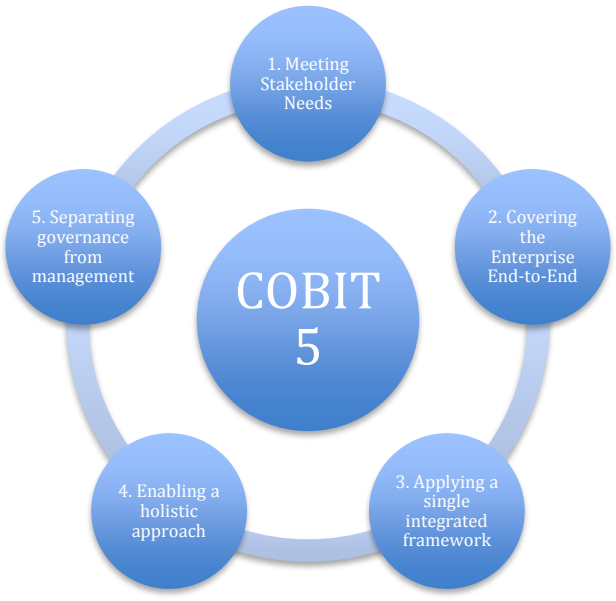

Figure 1. COBIT 5 Principles

In COBIT 5 there is a distinction made between governance and management. Governance processes deal with value delivery, risk optimization, and resource optimization, and include practices and activities aimed at evaluating strategic options and providing direction to IT. Management processes deal with planning, building, running and monitoring enterprise IT (ISACA 2012). COBIT 5 provides for one governance domain: *evaluate, direct and monitor*, and four management domains: *align, plan and organize*; *build, acquire, implement*; *deliver, service and support*; and *monitor, evaluate and assess*. Each domain contains several domain processes, where the three essential COBIT 5 processes related to information security are *manage risk (APO12)*, *manage security (APO13)* and *manage security services (DSS05)* (Greene, 2015). The focus of our research, dealing with user access attestation, is sanctioned by the COBIT 5 domain of *deliver, service and support* under the *manage security services* process section DSS05.04: "User identity and logical access should be managed on business need-to-know and least-privilege bases" (ISACA, 2016). One of the user account management control practices recommended by COBIT is a timely and regular review that the user has authorization for the use of the information system or service, and the

level of access granted is appropriate to the business purpose and consistent with the organizational security policy (ISACA, 2016).

Systems Development Life Cycle (SDLC)

There are a number of systems development approaches, e.g. waterfall, agile, and unified process. Generally, these approaches follow a systems development life cycle (SDLC), and although the list (and delineation) of SDLC phases or workflows may vary between approaches, it can be generally agreed that the following seven workflows are included within SDLC: 1) planning 2) requirements gathering and analysis, 3) design, 4) implementation, 5) testing, 6) deployment, and 7) maintenance. These may be structured as linear, sequential phases or within an iterative approach (Royce 1970, Jacobson et al. 1999, Pollard et al. 2010, Dennis et al. 2012).

In the planning phase a determination for the need for a new system to meet stakeholder needs is made. The purpose of this workflow is to determine the scope of the problem and come up with potential solutions with an eye to the overall value of the system to the business. Resources, costs, time and benefits are considered at this stage. The requirements gathering and analysis phase involves the determination of a complete and accurate list of system requirements. This workflow is a process of gathering information, identifying problems, understanding the processes involved and recommending feasible solutions. The result of this phase is a logical design for the system. In the design phase, using a detailed analysis of the problem situation along with systems requirements, a detailed description of what is needed to solve the problem at hand is produced including inputs, outputs, databases, applications, forms, code schemes and processing specifications. This phase transforms the logical design from the requirements gathering and analysis phase into a physical design. The implementation phase is where the actual coding and/or configuration of the system takes place in order to create a working system that solves for the demands of the problem. The testing phase is to ensure the reliability and quality of the system. Here components are integrated and tested to determine whether they perform as expected and achieve the system's goals. The deployment phase is where the new system is put into production and users are trained. Transition from any existing system to the new system takes place at this time as well as documentation for the system. During the maintenance phase the system is reviewed for any errors that need correction and needs for future functionality and features are determined on an ongoing basis.

Mapping Software Development Process to COBIT 5 Domain Processes

"COBIT is a high-level framework that suggests what needs to be done by an organization in order to be compliant and effective. But how to address the requirements of COBIT in detail and achieve the desired outcomes must be resolved by each organization individually" (Mishra and Weistroffer 2007). For this reason Mishra and Weistroffer proposed a conceptual mapping of COBIT 4.1 control objectives to the core workflows of the SDLC. Our research incorporates and updates their conceptual mapping of the SDLC to the COBIT 5 framework and includes a more atomic division of SDLC workflows. As indicated in Table 1 and Figure 2, each of the SDLC workflows can be mapped to several COBIT 5 domain processes. This mapping will allow us to integrate COBIT's controls to the development process for our user access attestation system.

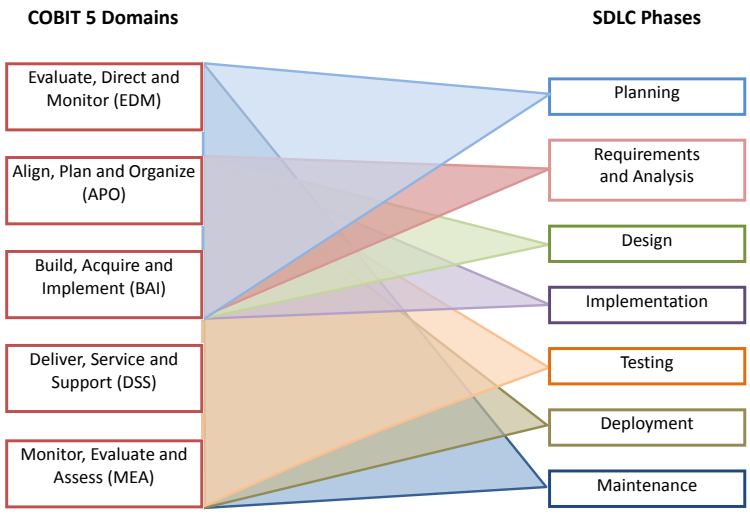

Figure 2. Mapping SDLC Phases to COBIT 5 Domain Processes

To illustrate the mappings in Table 1, the COBIT 5 APO domain provides guidance for planning for acquisition, including investment planning, risk management, program and project planning and quality planning (ISACA 2012). So, for instance, the APO12 Process for *Manage Risk* would map to all of the SDLC phases as we would need to 1) *plan* for risk mitigation, 2) *gather requirements and perform analysis* with risk in mind, 3) *design* for risk avoidance, 4) make sure that risks are addressed within the code or system acquisition *implementation*, 5) *test* to ensure the system avoids potential risks, 6) document for compliance purposes during *deployment* and 7) perform periodic reviews of the system in order to ensure *maintenance* of risk aversion in a dynamic regulatory environment.

COBIT 5 Domain Processes	SDLC Development Workflows						
	Planning	**Requirements Gathering and Analysis**	**Design**	**Implementation**	**Testing**	**Deployment**	**Maintenance**
Align, Plan and Organize (APO)	P	R&A	Des	I	T	Dep	M
APO01 – Manage the IT Management Framework	◆	◆	◆				◆
APO02 – Manage Strategy	◆	◆	◆				◆
APO03 – Manage Enterprise Architecture	◆	◆	◆				◆
APO04 – Manage Innovation	◆	◆	◆				◆
APO05 – Manage Portfolio	◆	◆	◆				◆
APO06 – Manage Budget and Costs	◆	◆	◆	◆	◆	◆	◆
APO07 – Manage Human Resources	◆	◆	◆			◆	◆
APO08 – Manage Relationships	◆	◆	◆			◆	◆
APO09 – Manage Service Agreements	◆	◆	◆				◆
APO10 – Manage Suppliers	◆	◆	◆			◆	◆
APO11 – Manage Quality	◆	◆	◆	◆	◆	◆	◆
APO12 – Manage Risk	◆	◆	◆	◆	◆	◆	◆
APO13 – Manage Security	◆	◆	◆	◆	◆	◆	◆

Table 1. Mapping of COBIT 5 APO Domain Processes to SDLC Phases

DEVELOPMENT OF THE USER ACCESS ATTESTATION SYSTEM (*AtTest)*

Our approach for integrating COBIT 5 domain processes within the SDLC of our user access attestation system (**AtTest)** is to apply the mappings from the SDLC to the COBIT 5 domain processes (see Figure 2). For example, for the SDLC Planning phase for out **AtTest** system, in order to align with the processes of COBIT 5's governance domain, EDM, we need to ensure that there is a stakeholder need for the system. The COBIT 5 governance domain process EDM03 – *Ensure Risk Optimization* provides guidance to the SDLC process that the information security needs of the organizational stakeholders should be aligned with development of a new or replacement system. As previously described herein, legal and regulatory IT governance requirements inform us that there exists an organizational stakeholder need for a user access attestation system to ensure appropriate user access to IS. This aligns with the COBIT 5 principle of meeting stakeholder needs. Other COBIT 5 domain processes involved in the planning phase (see Table 1) are APO2 – Manage Strategy, APO3 – Manager Enterprise Architecture, APO4 – Manage innovation, APO08 – Manage Relationships, AP12 – Manage Risk and APO13 – Manage Security (Suer et al. 2014). Each of the successive workflows can be mapped in a similar fashion.

A prototype of the **AtTest** system has been developed to provide a method for user access attestation along with workflows for accomplishing the objectives and fulfilling the requirements of the system. The **AtTest** system prototype has been developed using Sharepoint 2013 along with a Microsoft Sharepoint workflow add-on tool, Nintex. Sharepoint is an online, collaboration tool that integrates with Microsoft Office, primarily used for document management and storage. Sharepoint provides custom development capabilities that allow for rapid prototyping and integration with corporate directories and data sources through REST, OData and OAuth (Microsoft Corp. 2016). The **AtTest** prototype system was created by importing an Excel workbook with a list of all users with access to organizational business and financial reports through various memberships in Microsoft Active Directory (AD) Groups into a Sharepoint List app (Figure 3). Sharepoint lists store and display data items using a SQL Server database. The Excel workbook contained the following fields: 1) *employee name*, 2) *employee ID*, 3) *AD Group membership*, 4) *employee email*, 5) *manager name*, and 6) *manager email addresses*. In a real world setting, this information would be obtained from the organizational department charged with IS user access administration. Additional custom fields were added to the list: 1) *Approval* is a choice field type taking the values "Yes" or "No"; 2) *Review date* with a default value of the current date, 3) a *Not Mine* column for the Manager to indicate that the employee is "no longer their employee" or "no longer with the company" and 4) a *Comments* column for the manager to add any notes to the **AtTest** system administrator about the particular employee. Sharepoint automatically adds fields for Creation and Modification date/time and which organizational member Created and/or modified the record.

A built-in feature of Sharepoint is activated in the *Settings* menu to allow *Versioning settings* to record and display any changes to the list records. We also set *Permissions for this list* to prevent any unauthorized users from accessing the list.

Activating and configuring these features provides audit logs and security for our application in accordance with COBIT 5 domain processes APO12-Manage Risk and APO13-Manage Security. Nintex Workflow integrates with Sharepoint as an add-on and is a browser-based, drag-and-drop workflow designer with a graphical user interface. Nintex Workflows allow for the automation of processes and provide an electronic trail of business processes for compliance requirements (Nintex, 2016). Separate workflows were created to allow the system administrator to send notifications to the managers required to make user access attestations and to notify user access administrators once the attestations were complete so that modifications and terminations could be enacted upon and members removed from AD groups. Various Sharepoint List *Views* were created for managers and administrators. For example, a Sharepoint List *View* was created with filters to allow managers to see only the records pertinent to them. This provides an additional layer of security to ensure that managers only view the records of their own employees and made attestation more efficient by filtering out unrelated records.

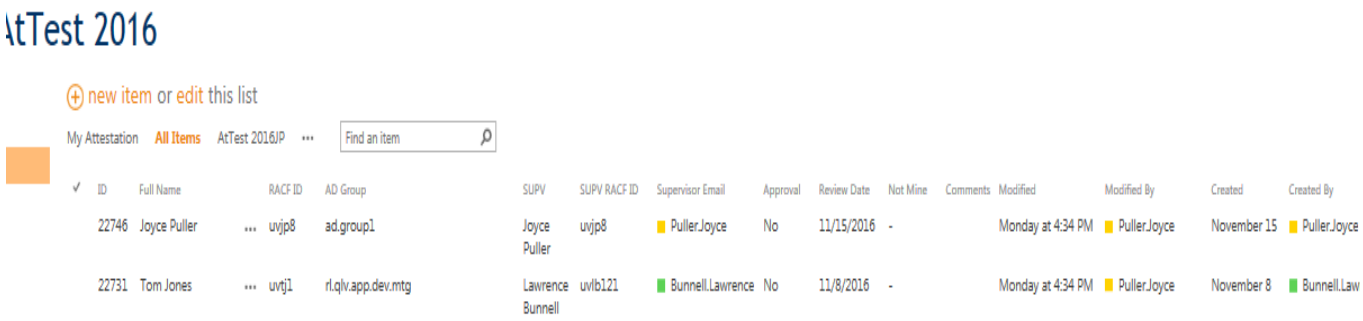

Figure 5. Prototype Sharepoint AtTest List

Proposed Assessment

COBIT 5 provides guidance for the assessment of process capabilities in alignment with ISO/IEC standard 15504 to enable the governance body and management to benchmark process capability. Capability Level 1 describes whether or not a process achieves its goals. Assessing whether the process achieves its goals may be accomplished by reviewing the process outcomes as they are described for each process in a detailed process description using the ISO/IEC 15504 rating scale to assign a rating to what degree the objective is achieved (ISACA 2012). Testing of the AtTest system was conducted to ensure the proper records import, functioning of workflows and modifications to the system by users in the manager role, and correct updating of database records. History and versioning logs were also examined to ensure proper auditing techniques are enforced. A proper assessment of the proposed AtTest prototype would be to demonstrate a Fully Achieved (F) rating for the attributes in each of the assessed COBIT 5 domain processes (EDM01 – Ensure Governance Framework Setting and Maintenance, EDM02 – Ensure Benefits Delivery, etc.) The limitations of research with a prototype system preclude a complete COBIT 5 Capability Model assessment at this time.

CONCLUSION

This research adds to the body of knowledge in the area of IT governance specifically with respect to systems development, by introducing a time, resource and cost efficient approach for developing a User Access Attestation system (AtTest) utilizing widely available software development tools. The research also shows how the COBIT 5 framework can be integrated into the SDLC and illustrates COBIT 5 assessment measures to ensure adherence to IT governance tenets and regulatory compliance. It updates the SDLC workflows to COBIT 5 mapping introduced by Mishra and Weistroffer to the new COBIT 5 framework and provides a framework for systems developers to incorporate IT governance controls utilizing diverse development approaches for systems impacted by legislative and regulatory compliance issues.

The business objectives could not be assessed with a prototype system, but a full implementation is planned and further research would be able to determine whether the systems' use achieves the goals and metrics and accomplishes fully achieved rating in accordance with the COBIT 5 Process Capability Model Achievement Assessment. The COBIT 5 domain processes provided in this research are high-level. Detailed process information for each of the COBIT 5 Domain processes are provided and outlined in COBIT 5 and represent a more granular view of the steps required for each of the domain processes provided herein. We have purposely avoided listing and describing these enabling processes as they are outside the scope of this research.

REFERENCES

1. Bhoj, P. and King, E. (2005) Attestation of Identity Information, Oracle White Paper, Oracle Corporation, Redwood Shores, USA.
2. Dennis, A., Wixom, B.H., and Tegarden, D. (2012) UML Version 2.0: An Object Oriented Approach, 4th Edition, John Wiley & Sons, Inc., Danvers, MA, USA.
3. Gaehtgens, F. and Iverson, B. (2016) Definition: Identity Governance and Administration, Gartner Advisory, Publication ID# G00310264, http://www.gartner.com/document/3408917.
4. Gaehtgens, F., Iverson, P., and Carpenter, P. (2016) Magic Quadrant for Identity Governance and Administration, Gartner Advisory, Publication ID#G00274258, http://www.gartner.com/document/3231517.
5. Getter, J.R. (2007) Enterprise architecture and IT governance: a risk-based approach, *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*.
6. Green, F. (2015) Selected COBIT 5 Processes for Essential Enterprise Security, *ISACA Journal*, 2.
7. Hodges, S. (2013) Examining the Gramm-Leach-Bliley act's opt-out method for protecting consumer data privacy rights on the Internet, *Information & Communications Technology Law*, 22(1), 60–85.
8. ISACA (2012) COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, Rolling Meadows, IL, USA, ISBN 978-1-60420-237-3.
9. ISACA (2014) COBIT 5 Principles: Where Did They Come From? ISACA, Rolling Meadows, IL, USA.
10. ISACA (2016) COBIT, https://cobitonline.isaca.org/, accessed 11/2/2016.
11. ISACA-2, (2012) COBIT 5: Enabling Processes, ISACA, Rolling Meadows, IL, USA
12. Iverson, B. (2016) IGA Best Practices: Establish an Identity Perimeter With Identity Life Cycle Processes, Gartner Advisory, Article ID: G00271345
13. Iverson, B., Carpenter, P., and Gaehtgens, F. (2016) Critical Capabilities for Identity Governance and Administration, Gartner Advisory, Publication ID#G002774989, http://www.gartner.com/document/code/274989.
14. Jacobson, I., Booch, G., and Rumbaugh, J. (1999) The Unified Software Development Process, Addison-Wesley, Reading, MA, USA.
15. Kushwaha, D., Gadankush, A.V., and Das, S. (2013) Mapping of BASEL III and COBIT 5 framework in banking sector of India: a futuristic approach, *International Journal of Advanced Research in Computer Science*, 4(8), 81-85.
16. Lee, A.S. (2004) Thinking about social theory and philosophy for information systems, in *Social Theory and Philosophy for Information Systems*, L. Willcocks and J. Mingers (eds.), Chichester, UK, John Wiley & Sons, 1-26.
17. Lee, A. (2010) Retrospect and prospect: information systems research in the last 25 years, *Journal of Information Technology*, 25, 336-348.
18. Li, C., Peters, G., Richardson, V., and Watson, M. (2012) The consequences of information technology control weaknesses on management information systems: the case of Sarbanes-Oxley internal control reports, *MIS Quarterly*, 36(1), 179.
19. Microsoft Corp (2016) What is Sharepoint? https://support.office.com/en-us/article/What-is-SharePoint-97b915e6-651b-43b2-827d-fb25777f446f, accessed 12/2/2016.
20. Mishra, S. and Weistroffer, H.R. (2007) A framework for integrating Sarbanes-Oxley compliance into the systems development process, *Communications of the Association for Information Systems*, 20, 712- 727.
21. Moturi, C. and Bitta, F.O. (2013) Multiagent model for system user access rights audit, *ISACA Journal*, 3, 1-6.
22. Nintex Global Ltd, The Essential Buyers Guide to Workflow Automation, http://www.nintex.com/-/media/files/resources/white-papers/essential-buyers-guide-to-workflow-automation.pdf, accessed 11/2/2016.
23. Nossier, S. (2010) Access certification & attestation: Best practices for avoiding the rubber stamp syndrome, CA Technologies, https://blogs.ca.com/2010/07/28/access-certification-amp-attestation-best-practices-for-avoiding-the-rubber-stamp-syndrome/
24. Pollard, C.E. (2010) Teaching systems development: a compelling case for integrating the SDLC with the ITSM lifecycle, *Information Systems Management*, 27(2), 113-122.
25. Royce, W.W. (1970) Managing the development of large software systems, *IEEE WESCON*, August 1970, 1-9.
26. Saltzer, J.H., and Schroeder, M.D. (1975) The protection of information in computer systems, *Proceedings of the IEEE*, 63(9), 1278-1308.
27. Sarbanes-Oxley Act of 2002 (SOX), Title III, Section 302, Corporate responsibility for financial reports, https://www.sec.gov/about/laws/soa2002.pdf
28. Suer, M., Cullens, C., and Brancato, D. (2014) COBIT 5 processes from a systems management perspective, *ISACA Journal*, 2.
29. Swanson, M. and Guttman, G. (1996) Generally Accepted Principles and Practices for Securing Information Technology Systems, National Institute of Standards and Technology (NIST) Computer Systems Laboratory, NIST Special Publication 800-14, 1-63.
30. Wu, S., Straub, D., and Liang, T. (2015) How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers, *MIS Quarterly*, 39(2), 497.