DE GRUYTER
OPEN

DOI 10.1515/ptse-2016-0008 PTSE 11 (1): 55-61

Compliance Issues in Higher Education

Petra BENEDEK

benedek@mvt.bme.hu
(University of Technology and Economics, Budapest, Hungary)

Received: 09.06.2015; Accepted: 30.10.2015

Abstract: *Efficiency in the 1980's, quality in the 1990's, compliance in the 2010's - private sector management techniques and mechanisms find their way to public services. This paper facilitates the understanding of how compliance management controls can improve operations and prevent or detect failure or wrongdoing. The last few years' empirical research and benchmark studies demonstrate how organizations are confused about the use of compliance controls. In brief, better organized and integrated IT controls generally lead to better compliance all over the business.*

Keywords: compliance management, operational efficiency, IT controls, compliance in education, education organizing

Introduction

Efficiency in the 1980's, quality in the 1990's, compliance in the 2010's - private sector management techniques and mechanisms find their way to the public sector.

Compliance management is a relatively new perspective to keeping up with fast-changing and challenging legal requirements. Compliance management is a business support function which aims to minimize the risks of organisational wrongdoing and legal non-compliance. Compliance management is a relevant approach in the strictly regulated sector of education. Universities and other business sectors could benefit from sharing experiences and implementing best practices.

Especially IT compliance issues, like data loss or information privacy, affect the daily procedures of every department of any educational institution. The last few years' empirical research and benchmark studies demonstrate how organizations are confused about the use of compliance controls in support of operational compliance. Realizing the fact, this paper focuses on importance of compliance management controls.

Compliance Management in Higher Education

Universities use great resources to ensure high standards of operations in education, research, preservation of knowledge and other significant activities. Each and every member of an institution has their responsibility in management of the resources (time, budget, attention, personnel and other resources). Business and ethical practices and processes serve as control mechanisms throughout every operation. Compliance management supports responsible operations ranging from admission processes to quality control by focusing on compliance with laws and regulations.

The scope of compliance management is set in the approach that an effective internal control system can find the balance between the risks of operations and the costs of control (e.g. increased bureaucracy). Few risks cannot be eliminated, but can be managed. In the evaluation process of a specific compliance management function the extention of the compliance scope is reviewed from time to time.

What can be considered an effective internal control system? The answer is specific to every single organization. Still, general guidelines apply, from publicly traded companies to public service. A good example is Sarbanes-Oxley Act (SoX). The company has applied a set of new standards of financial reporting and internal governance. This has been carried out following the idea that public trust is a basic issue. To achieve this, a system of communication that openly discusses failures and corporate wrongdoing was implemented.

Another example is the Committee of Sponsoring Organizations of the Treadway Commission (COSO). It introduced two decades ago an Integrated Framework. Now, more than twenty years after the original version, the updated COSO Business Risk Management - Integrated Framework was introduced that is SoX control compatible.

The COSO framework and the FSGO (Federal Sentencing Guidelines for Organizations) had significant impact on what is considered as acceptable business practice, what internal controls are necessary. Both emphasize the responsibility of each member of the organization regarding internal controls and proper operations. The COSO framework provides a reference point in creation or monitoring of a specific internal control system.

Compliance controls

This paper presents internal controls in the service of compliance management. What is the difference between compliance controls, and internal controls:

- both effectiveness and efficiency of operations,
- compatibility with laws and regulations.

Internal controls have the financial aspect, they include processes that ensure the stability of financial reports. Developing a common understanding of compliance management is a real challenge in every educational organization. On the other hand, it is an opportunity to move towards excellent performance. It is important to understand that implementing laws and regulations, internal or external, are *the responsibility of each and every employee*, including professors, assistants, managers, librarians, facility workers and so on. Awareness is a key factor of delivering results. Therefore, there is a strong focus on education and training.

Executive commitment is necessary. The leadership is ultimately responsible for ensuring that internal controls are designed, implemented, documented and monitored effectively. Setting the tone is critical in order to achieve results. The organization-wide recognition of compliance, the inclusion of rule-following behaviour into organizational values is an important task to leaders at all levels (Lipton et al., 2014). Spot checks, basic sampling in general, and focus on high risk areas provide some sense about whether compliance controls function as intended.

Error, delay, fraud, health and safety, such common risks – and many more - are inherent to the operations of highly complex organizations such as higher education institutions. Operational risks can have compliance implications, and improved compliance could bring measurable results in many aspects, like reliability of information or reducing potential costs of penalties or loss of reputation. Some risks are by nature both operational and compliance. According to the COSO framework *risk management* is based on

1. Clearly set *objectives* from university to departmental activity level. Some activities are very general, like hiring employees or procurement.
2. Risk *assessment* includes identification and analysis.
3. *Prioritizing* risks is based on the evaluation of potential quantitative costs (e.g. cost of equipment) and qualitative implications (e.g. bad publicity).
4. Established *control* activities are the mechanisms that reduce the probability of risk occurrence.

Many *control activities* use computer systems; others are purely manual or combine system-related and manual procedures. Another classification of controls is preventive versus detective (The Institute…, 2012). Preventive controls help to prevent wrongdoing or systematic mistakes, detective controls aim to detect the occurrence of noncompliance incidents, while revealing the weaknesses of preventive controls. A few types of controls are mentioned in the COSO framework, like some of the following (COSO…, 2015):

1. Authorization, approval: a supervisor’s approval (e.g. signature, electronic) implies that a specific activity complies and conforms to regulations.
2. Reconciliations: comparison of different data, investigation of the differences and corrective actions.
3. Reviews: current performance compared to forecast, budget or benchmarks.
4. Asset security: safeguarding assets, periodic inventories.
5. Segregation of duties: responsibilities divided between people.
6. Information systems: support information processing, detailed in the next section.

Communication has also an important role in an effective compliance system. The challenge, discussed later in details, is obtaining and sharing relevant and reliable information, as well as presenting it in the appropriate form and in the right time.

Compliance *evaluation* is focused on design effectiveness, operational efficiency or measurement of results (performance and administration) according to three phases of self-regulation.

Compliance issues and challenges

The top compliance challenges for organizations are partly external and partly internal. Such external challenges can be mentioned as the quickly changing and complex regulatory and legal environment and the access to qualified compliance professionals. Internal challenges include budgetary constraints and the management of new risks, due to new services, partners or organizational structures.

Getting and sharing reliable and relevant information on time and in appropriate form is a challenge to most institutions. Free flow of information and information system effectiveness is strongly connected to all management and control activities. On one hand, information technology (IT) provides the infrastructure and resources that enforce the compliance activities. On the other hand, IT itself presents some compliance risks like information security and privacy issues. Four types of IT controls can be distinguished:

1. General Controls refer to the whole IT environment.
2. IT Dependent Manual Controls are based on computer generated information. A responsible person/group validates the accuracy and completeness of the system-generated information.
3. IT Application Controls ensure the complete and accurate processing of information on the application level, ranging from input to output controls (like field checks, completeness checks, error listings, etc.)
4. End-User Computing Controls include employee access, backup, etc.

IT compliance issues, like data loss or information privacy, affect the daily procedures of every department of any educational institution. This section presents and studies how IT controls contribute to the overcoming of the above challenges. In brief, better organized and integrated IT controls generally lead to better compliance all over the business. Fragmented IT operations may result in reciprocally fragmented compliance initiatives that lead to neither cost reduction nor increased efficiency. We have found that the underdevelopment of automated IT controls affect compliance management in a negative way.

To give an overview of the various forms of IT controls in the service of compliance management the method of critical review, analysis and interpretation of the literature on the IT infrastructure of compliance management was used. Collet (2008) and Silverman (2008) offer a basic insight into the problem.

IT controls in relation to compliance management include a variety of fields like relational database management, database auditing, process integrity and application availability, records retention and disposition, unified threat management, information integrity and confidentiality, IT supported audit management, compliance dashboards, exception reporting, software supported risk assessment, data loss notification, credit cardholder protection and more.

Verizon's 2013 Data Breach Investigations Report (DBIR) is based on a non-random sample of 621 data breaches and more than 47000 security incidents from 27 countries over a period of nine years (2004-2012) (Verizon, 2013). The terminology and context is Vocabulary for Event Recording and Incident Sharing (VERIS) which focuses on the narrative of "who did what to what (or whom) with what result" and translates it into a structured dataset.

The Verizon study has found that data breach attacks are mainly opportunistic and not targeted. Attackers exploit weaknesses that are communicated publicly with no such intention. No organization is immune or out-of-scope. Essential controls and monitoring of controls are one of the recommendations of the study.

Furthermore, the Ponemon Institute, member of the Council of American Survey Research Organizations, and Tripwire, Inc. conducted a benchmark study to determine the full economic impact of compliance activities based on a small representative sample of 160 functional leader interviews from 46 multinational organizations. The 12-month time frame benchmark analysis was published in January 2011. An indexing methodology, the Security Effectiveness Score, was used to measure the effectiveness security activities.

Data security refers to all activities and technologies to protect data and control access. Compliance with various privacy and data protection laws and requirements (i.e. European Union Data Protection Directive) are considered a great challenge according to the responses. Data protection is the most costly compliance activity according to the Ponemon study (Ponemon..., 2011).

Despite the fact, that the benchmark study has found that there is "no apparent relationship between compliance cost and security effectiveness", the generally much greater costs of non-compliance, like fines, penalties, revenue loss, etc., show an inverse relationship with security effectiveness. (Ponemon..., 2011).

Ultimately, in January and February 2013, a survey of the state of internal audit and compliance was conducted in cooperation with the Hungarian Institute of Internal Auditors (IIA). Deloitte invited supervisors of internal audit, fraud detection and compliance departments, financial directors and company executives from 250 companies to complete the questionnaire and supply data (Deloitte, 2013). Responses were received in 75 % from internal audit executives, from more than 70 companies, adding up to a return rate of 28%. As for the distribution of industries financial service providers represent the highest percentage of respondents.

According to the Deloitte survey results 87% of the respondents have fraud prevention activities to some extent. About 49% of the respondents have perceived cases of fraud as regular in their industry. But only 7%

apply or plan to introduce fraud detection applications. 52% of the companies operate hotlines, which are considered to be a common non-compliance reporting channel. For 42% the lack of hotline is the way to go, introduction of a hotline is not even planned. 86% of respondents emphasize insufficient internal control and underdeveloped and inefficient fraud detection as the factor giving opportunity for corporate fraud.

The above research and benchmark studies demonstrate the complexity of the issue of compliance controls in support of operational compliance. Based on the results it can be concluded that the lack of a developed compliance management IT strategy is a major underlying problem. This paper indicates that investment in developing an IT compliance strategy is a path to better integration of IT and compliance.

Further research

Growing business complexity is one of the main challenges of our time (Capitalizing..., 2010). Compliance itself is not a simple issue. It involves among others fields of law, finance, risk and quality management and operations management. From 2008, global financial and economic crisis has provoked numerous new research.

The challenge is to agree on what is in the core of best practices regarding IT controls in compliance. The chosen standard or framework (like COSO) sets the whole design and implementation of compliance management which will determine to a certain point the IT controls used or ignored. It can be concluded that information security is one critical point of the matter.

The investment in IT related in compliance activities indeed makes sense. Investment in training and expert staffing also helps the profitability of compliance efforts. Ensuring the budget for compliance is inevitable to bring acceptable results and meet the complex objectives. According to the findings, the main directions for IT competence development are IT audit and IT strategy.

We recommend that future research should consider studying the return on investment of compliance activities. We call for research on the complexity of compliance due to new products and services, new markets, or new business systems. We propose the following future research hypothesis:

1. Better compliance improves operational efficiency.
2. Risk and compliance are both connected to compliance maturity.
3. Higher ROI on compliance expenditure comes from completely integrated controls achieve.

Summary

In this age, constantly changing laws and economic environments provide a constant challenge for organizations, including higher education institutions. Compliance management as a new corporate function has emerged and this approach is, along with many other management techniques and mechanisms, finds its way to universities and other educational institutions. Under the microscope we can see that laws and regulations often generate compliance issues. But broadening our view it reveals itself that transparency, accountability, ethics are connected. Also, all the efforts start and end with reputation and public trust.

Agreement controls are embedded into internal controls systems. We highlighted some IT compliance issues that affect the daily procedures of every department. This paper indicates that investment in developing an IT compliance strategy is a path to better compliance.

References

Capitalizing on Complexity (2010). *IBM*. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03297usen/GBE03297USEN.PDF [30.06.2015].

Collet, H. (2008). IT Controls Automation and Database Management: Defending Against the Insider Threat. In: Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices (ed A. Tarantino), Hoboken: John Wiley & Sons. Ch. 23.

COSO (2015). *Internal Control – Integrated Framework, Executive Summary*. Retrieved from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf [30.06.2015].

Deloitte (2013). *Felmérés a belső ellenőrzés és a compliance helyzetéről 2013*. Retrieved from http://etk-rt.hu/images/dokumentumok/deloitte_eloadas.pdf, [30.06.2015].

Lipton, M., Neff, D. A., Brownstein, A. R., Rosenblum, S. A., Emmerich, A. O., Fain, S. L., & Cohen, D. J. (2014). *Risk Management and the Board of Directors – An update for 2014*. Wachtell, Lipton, Rosen, Katz. Retrieved from http://www.wlrk.com/webdocs/wlrknew/WLRKMemos/WLRK/WLRK.23290.14.pdf [30.06.2015].

Ponemon Institute (2011). *The True Cost of Compliance, A Benchmark Study of Multinational Organizations*. Retrieved from http://www.tripwire.com/register/ponemon-report-the-true-cost-of-compliance/ [30.06.2015].

Silverman, M. (2008). *Compliance management for Public, Private, and Nonprofit Organizations*. New York: Mc Graw Hill.

The Institute of Internal Auditors (2012). *Global Technology Audit Guide, Information Technology Risk and Controls*. [2nd Edition]. Retrieved from http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag1%202nded.pdf [30.06.2015].

Verizon, 2013: 2013 Data Breach Investigation Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, 30/06/2015