5-2013

IT operational risk awareness building in banking companies: A preliminary research design highlighting the importance of risk cultures and control systems

Stefan Bauer
Vienna University of Economics and Business, stefan.bauer@wu.ac.at

Edward W. N. Bernroider
Vienna University of Economics and Business, edward.bernroider@wu.ac.at

IT operational risk awareness building in banking companies: A preliminary research design highlighting the importance of risk cultures and control systems

Stefan Bauer
Vienna University of Economics and Business
Stefan.Bauer@wu.ac.at

Edward W. N. Bernroider
Vienna University of Economics and Business
Edward.Bernroider@wu.ac.at

Research in Progress

Abstract
This research in progress paper introduces a research initiative focusing on bank employee risk behaviour to mitigate IT operational risks in Austrian banks. The study focuses on the role of IT risk culture and internal controls in relation to employee risk behaviour and the effectiveness of different awareness building practices in banking companies in response to international banking regulation. We offer a short introduction to central theoretical concepts, main research assumptions and a two-staged methodological design to conduct the underlying study. The indicative findings suggest important properties of awareness building methods and guidelines to create a proactive IT risk culture.

Keywords
Key words: IT Operational Risk, IT Risk Culture, Information Security Awareness, Employee Risk Behavior, IT Governance

1. Introduction
Recent regulations such as Basel II forces banking companies to systematically manage risks and in particular operational risks (Basel Committee on Banking Supervision, 2004; Bauer, 2012). Banks have to reserve minimum capital requirements for potential operational loss events. The more minimum capital is required, the less money banks can use for generating profits (Jobst, 2007). Given an effective operational risk management, banks can put back less capital to safeguard their organization and comply with Basel regulations (Luthy & Forcht, 2006). Recent IT operational loss events such as information security breaches or software update failures in banks from all over the world substantiate the problematic situation (Goldstein, Chernobai, & Benaroch, 2011). The objectives of IT operational risk management largely conform with traditional information security goals, which seek to assure availability, confidentiality, and integrity

of data and systems (Benaroch & Chernobai, 2012; Goldstein et al., 2011). Efficient and effective IT operational risk management is a constituent element of IT governance (Bernroider & Hampel, 2005; Novotny, Bernroider, & Koch, 2012) and a range of IT controls can be implemented, for example, to reduce IT operational risks caused by IT changes (Bernroider & Ivanov, 2011). More attention is required to understand the role of the employee to detect operational weaknesses and loss events early (Bauer, 2012).

Basel II engages banking companies to build awareness concerning operational risk, especially on information technology aspects of operational risk (Pinder, 2006). However, the generic Basel II regulation does not describe how banks can build awareness. As the research team discovered from exploratory interviews in Austrian banks, banking companies use different practices to train their employees in this context. Austrian banks build employees awareness through an obligatory E-Learning program at organizational entry. Moreover, some banks conduct regular risk meetings in their subunits, self assessments and provide marketing goodies such as coffee cups for the employees. Exploratory interviews in Austrian banks have shown that operational risk managers rate the awareness building process as a very important issue in operational risk management. Operational risk managers have limited financial and human resources and hence they are interested to find effective and innovative ways to successfully build IT operational risk awareness of their employee.

The aim of this research in progress is to two-fold. First, we seek to empirically explore current IT operational risk awareness building methods in Austrian banking companies. Second, we seek to design a new data- and theory-driven mixed-method approach and test its effects in the same banking companies. The new awareness building approach should be flexible enough to adapt to specific cultural contexts of each sub-unit and reflect upon their internal control systems. Next, we extend our theoretical considerations and sketch the methodological approach for this study. The final section concludes the paper.

2. Theoretical Background and Research Hypotheses

The *socio-cultural perspective* of IT operational risk management deals with the human factor as a main reason for operational loss events (Jahner & Krcmar, 2005; Thomson, Solms, & Louw, 2006). Technology is only one factor to secure (Herath & Rao, 2009). The other focuses on the improvement of employee risk behaviour. According to the main body of related literature, risk behaviour deals with attitudes towards negative outcomes and policy compliance (ISACA, 2009; Sitkin, Pablo, & Sim, 1992).

To improve the risk behaviour of the employees, the organization needs a functioning and active *IT risk culture* (Da Veiga & Eloff, 2010; Jahner & Krcmar, 2005). Essential for a functioning risk culture is the behaviour towards negative outcomes, because some organizations established learning cultures, where employees learn from their failures. In contrast, some organizations establish an unintended blaming culture, because they punish their employees if their behaviour does not comply with corporate guidelines (ISACA, 2009). Learning theories such as the social learning theory or the organizational learning theory are essential to understand how employees can learn from failures to improve risk behaviour (Argyris, 1977; Thomson et al., 2006). Again, cultural difference seem to matter in IT management, in particular, when comparing Austria with

economies from Central and Eastern Europe (CEE), where Austrian banks tend to operate (Bernroider, Sudzina, & Pucihar, 2011).

An increased *risk awareness* is the most cost-effective control of an organization (Dhillon, 1999). Different methods can be used for awareness building among the employees, which attempt to educate and inform employees about IT operational risks. Some aspects such as media richness should be more important than others to transfer knowledge (Daft & Lengel, 1986). If the employees are aware of the threats, their behaviour concerning IT operational risks should improve. The highest stage of awareness is when the employees have internalized best practice behaviour (Nonaka, 1994). Hence, these considerations lead us to the following preliminary research assumptions.

A1. The effective use of IT operational risk awareness building methods by management depends on their properties, such as media richness, and the given organizational risk culture.

Prior work suggests that risk behaviour of employees can be also improved by increasing awareness of the purpose and operation of internal controls. In general, employees seem to know about the existence of an internal control system, but less about its purpose and functions. Greater levels of awareness should lead to improved IT operational risk behaviour and make it more likely to prevent or timely detect IT operational loss events. An effect similar to the well known productivity improvement effect known as Hawthorne effect is expected (Brannigan & Zwerman, 2001). The Hawthorne experiment highlighted that if an employer pays attention to the performance of employees, the likelihood of increased performance levels increases. The same can be expected in the context of IT operational risk prevention, mitigation and reporting. Hence, we expect that a communication campaign about the internal control system improves employee risk behaviour, which leads us to our second main assumption. Hence, we assume

A2. Awareness building about the internal control system is positively associated with employee IT operational risk behaviour.

3. Research Methodology

The suggested two-staged research methodology is displayed below (see Figure 1). In stage 1, a nested case study with different sub-cases within one large banking company will be conducted allowing for analytical generalization from empirical observation to theory (Benbasat, Goldstein, & Mead, 1987). Analytical generalization will be supported by extensively profiling each case and by cross-case analysis (Eisenhardt, 1989). Reliability will be supported e.g. by a transparent process involving semi-structured instruments, protocols and taped interviews, which will be transcribed and coded. Our triangulated research strategy will involve data triangulation (interviews with employees at several levels, direct observations and archival data) and investigator triangulation. As (Vroom & Von Solms, 2004) mentioned, behaviour of individual employees concerning information security is difficult to assess. We plan to apply a set of innovative methods to analyse risk behaviour such as non-reactive measurement methods (e.g. experiment reaction of employees on a stimulus like a specific safety message).

For stage 2, we apply a quantitative survey which will build on the findings from the previous phase and theory from literature. We plan to carefully apply measures to avoid validity problems,

coverage error and non-response error (King & He, 2005). From our current viewpoint, we, e.g., will consider how E-Learning affects risk awareness through wave analysis to assess pre- and post-stimulus impacts. The sampling frame will most likely be all employees from specified organizational units. Before administration of a mass survey, we will seek comments on the clarity and accuracy on conceptualization of the variables from a panel of academic and managers. We will also conduct a pilot test to evaluate the validity and reliability of our survey instrument. After modification of the instrument based on comments from the panel and pilot test, we will launch the survey in a multi-staged procedure ensuring an acceptable return quota.

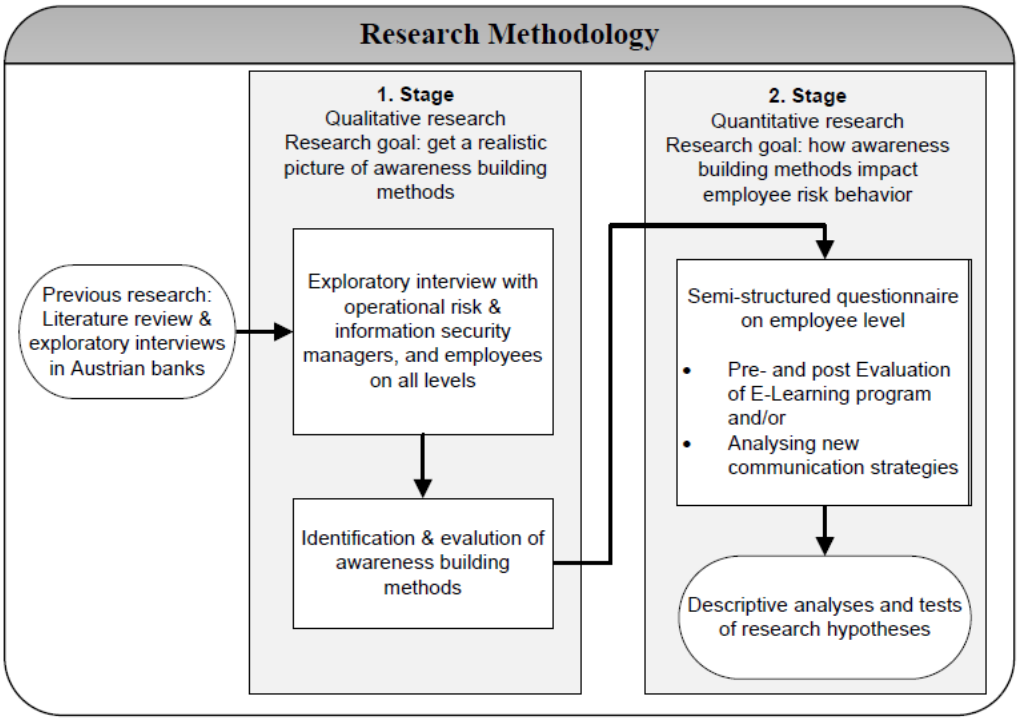

Figure 1: Overview of research methodology

4. Conclusion

This work in progress paper has provided a short introduction to IT operational risks. From a socio-technical perspective, the understanding of different risk cultures and properties of risk awareness building methods are essential for developing desired employee behaviour. Important theories to consider in particular include learning theories such as the social learning theory or organizational learning, and the Hawthorne effect to understand how performance measurement in the context of internal control systems may affect IT operational risk levels. The presented two-stage study should shed more light on these issues in the context of an international Austrian bank.

References

Argyris, C. (1977). Organizational learning and management information systems. Accounting, Organizations and Society, 2(2), 113–123.

Basel Committee on Banking Supervision. (2004). International Convergence of Capital Measurement and Capital Standards.

Bauer, S. (2012). A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector. International Conference on Information Resource Management, Vienna. The University of Aukland and WU Vienna (pp. 1–14).

Benaroch, M., & Chernobai, A. (2012). IT operational risk events as COBIT control failures: A conceptualization and empirical examination. Information Systems (ILAIS) Conference (pp. 115–117).

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11(3), 369–386.

Bernroider, E. W. N., & Hampel, A. (2005). Enterprise Resource Planning and IT Governance in Perspective: Strategic Planning and Alignment, Value Delivery and Controlling. Fifth International Conference on Electronic Business (ICEB 2005).

Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. International Journal of Project Management, 29(3), 325–336.

Bernroider, E. W. N., Sudzina, F., & Pucihar, A. (2011). Contrasting ERP Absorption Between Transition and Developed Economies From Central and Eastern Europe (CEE). Information Systems Management, 28(3), 240–257.

Brannigan, A., & Zwerman, W. (2001). The real "Hawthorne effect". Society, 55–60.

Da Veiga, a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196–207.

Daft, R., & Lengel, R. (1986). Organizational information requirements, media richness and structural design. Management science, 32(5), 554–571.

Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, (1999).

Eisenhardt, K. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532–550.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. Journal of the Association for Information Systems, 12(9), 606–631.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. doi:10.1057/ejis.2009.6

ISACA. (2009). The Risk IT Framework. (Information Systems Audit and Control Association, Ed.).

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. Americas Conference on Information Systems AMCIS (pp. 1–11).

Jobst, A. (2007). The treatment of operational risk under the New Basel framework: Critical issues. Journal of Banking Regulation, 8(4), 316–352.

King, W. R., & He, J. (2005). External Validity in IS Survey Research. Communications of the Association for Information Systems, 16, 880- 894.

Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. Information Management & Computer Security, 14(2), 155–166.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. Organization science, 5(1), 14–37.
Novotny, A., Bernroider, E., & Koch, S. (2012). Dimensions and Operationalisations of IT Governance: A Literature Review and Meta-Case Study. International Conference on Information Resource Management, Vienna. The University of Aukland and WU Vienna.
Pinder, P. (2006). Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II). Information Security Technical Report, 11(1), 32–38.
Sitkin, S., Pablo, A., & Sim, B. (1992). Reconceptualizing the determinants of risk behavior. Academy of management review, 17(1), 9–38.
Thomson, K., Solms, R. Von, & Louw, L. (2006). Cultivating an organizational information security culture. Computer Fraud & Security, (October), 49–50.
Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191–198.