Chapter 18
Towards a Framework to Improve IT Security and IT Risk Management in Small and Medium Enterprises

Stephan Mühe
University of Duisburg-Essen, Germany

Andreas Drechsler
Victoria University of Wellington, New Zealand

ABSTRACT

In this article, an IT risk management (ITRM) framework for small and medium enterprises (SMEs) is designed and evaluated. The framework's objective is to provide an uncomplicated and accessible ITRM approach primarily aimed at SMEs without a dedicated ITRM. The framework combines essential elements from three leading (IT) risk management frameworks: COBIT 5 for Risk, ISO/IEC 27005:2011 and M_o_R. The framework was developed by employing a design science research methodology for social artefacts and evaluated in two healthcare SMEs. The ITRM framework itself was assessed as comprehensible and potentially useful. Simultaneously, over-arching IT governance issues prevented the immediate framework implementation in the two cases. IT management researchers can draw on this article's findings to better understand the role of the social context in SMEs to achieve an effective practical impact. Practitioners in SMEs can draw on the current state of the framework for an initial ITRM implementation or to increase their current ITRM approaches' maturity.

1. INTRODUCTION

This paper's goal is to design and evaluate an IT risk management (ITRM) framework that is better suited for small and medium enterprises (SMEs) than existing comprehensive ITRM frameworks such as the ISO/IEC 27005:2011 or COBIT 5. The literature often describes the SME sector as vibrant and growing (Levy & Powell, 2005) and – at least within the European Union (EU) – as the backbone of the

DOI: 10.4018/978-1-7998-1760-4.ch018

economy (Wymenga, Spanikova, Barker, Konings, & Canton, 2012). Whereas the authors acknowledge that SMEs are commonly defined as having 250 employees or less (Australian Government, 2014; European Commission, 2014; U. S. Census Bureau, 2014), they do not limit themselves exclusively to this quantitative, and somewhat arbitrary, characteristic (Osteryoung & Newman, 1993). Instead, somewhat larger organizations are also included as long as they exhibit typical SME characteristics, particularly regarding the way they have institutionalized their IT management (ITM).

Here, Welsh and White (1982, p. 18) make the point that "a small business is not a little big business", i.e. SMEs function and need to be managed in a fundamentally different way than large enterprises. The key differences in SMEs' ITM include 1) emphasising personal leadership rather than abstract management frameworks and 2) that formal measuring and controlling instruments are less important than achieving transparency to inform decision-making and foster communication with managers within and beyond the IT organization (Drechsler & Ahlemann, 2016). SMEs also tend to have a low number of ITM personnel – perhaps only even 'involuntary IT managers' (AMI Partners, 2013).

Operating a business always incurs risks, and if SMEs' business models or their internal processes are reliant on information systems and technology, managing the corresponding IT risks (including IT security threats) are as important for them as they are for large enterprises. The Information Systems Audit and Control Association (ISACA) defines IT risk as the "business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise" (ISACA, 2015, p. 56) and thus includes the need for IT security management (ITSM). Therefore, ITRM and ITSM are important tasks for SMEs, since they often do not have the necessary financial reserves to overcome crises caused by severe incidents that an effective ITRM and ITSM could have prevented. Moreover, owing to the SMEs' importance for an economy, the wide-spread occurrence of IT risks in and IT security threats to SMEs may even have severe consequences for an entire economy, which the recent series of ransomware attacks ("Locky", "WannaCry", and others) showed (Pencavel, 2016). Moreover, the increasing digitalization of entire industries will not only increase SMEs' dependency on IT, but also the relevance of ITRM and ITSM.

Simultaneously there is consensus in the literature that only a small percentage of SMEs undertake RM on the corporate level and even, if they do, they only consider a few selected aspects (Britzelmaier, Häberle, & Landwehr, 2015; Hölscher, Giebel, & Karrenbauer, 2006, 2007; Verbano & Venturini, 2013). The same applies for ITRM and ITSM in SMEs (Sadok & Bednar, 2016). One contributing factor for the lacking RM in SMEs are poorly tailored approaches that do not take the special requirements of SMEs into account, but merely try to scale down existing large enterprise approaches for SME purposes (Altman & Sabato, 2007; Stroeder, 2008). Consequently, SMEs do not often adopt management frameworks they perceive as complex or costly to implement (Laporte, Alexandre, & O'Connor, 2008; O'Connor & Coleman, 2009). Hence, none of the three most common RM / ITRM frameworks (COBIT 5 for Risk, ISO/IEC 27005:2011 and Management_of_Risk) seems particularly well suited to institutionalize effective ITRM and ITSM in the SME context. The same applies to existing predominantly technically-oriented ITRM or ITSM solutions, as SMEs would have neither the managerial awareness for the necessary decision-making to introduce these solutions nor the necessary expertise available to effectively implement and maintain these solutions.

Consequently, this paper's main goal is to design an ITRM framework that is more suitable for the SME context than the existing frameworks. The designed ITRM framework is evaluated ex-ante (Pries-Heje, Baskerville, & Venable, 2008) by means of an interview study with the managers of a small and a medium enterprise in the healthcare industry who would be responsible for deciding whether to adopt