

# On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering

Yuri Bobbert, University of Antwerp, Antwerp, Belgium & Radboud University, Nijmegen, Netherlands & NOVI University of Applied Sciences, Utrecht, Netherlands

## ABSTRACT

This paper examines research methods for designing and engineering a Business Information Security (BIS) artefact. Preventing and responding to cybercrime is becoming an integral part of management practices which are supervised by the Board of Directors (BoD), and it can no longer be perceived as just traditional IT. In order to improve the maturity of business information security a transformation is needed and this requires adequate reporting and dashboarding. Dashboard functions such as the current versus the desired state of the Maturity of Business Information Security (MBIS) reflect certain parameters that boards can influence. Determining the key dashboard functions that reflect these parameters of control was the main motivation for this research paper and the ultimate goal was to engineer a BIS artefact. We propose a research and design method that could be used to establish an experimental dashboard with initial parameters of control based on a Group Support System (GSS) approach. Finally, GSS is evaluated as a method for a) examining which parameters are effective for BIS, from multiple perspectives and b) helping to implement the artefact (make it fit the purpose) as well as the associated business alignment and decision-making.

## KEYWORDS

Business Information Security, Design Science Research, Enterprise Transformations, Group Support System, Information Systems Design and Development

## INTRODUCTION

Information Security is now a strategic issue for business leaders and several institutions and communities have launched numerous initiatives to encourage business leaders to ensure good stewardship in this area (WEF, 2015). The associated compliance obligations and the increase in security breaches have made many business leaders aware of its impact on the business continuity (Cashwell, Jackson, Jickling, & Webel, 2004), civil and legal liabilities (Fox-IT, 2011) reputation (Walsh et al., 2009; Peters, 2012), employability and financial position (Ishiguro et al., 2011; Cavusoglu et al., 2002). This is why Von Solms (2009) has argued that Information Security Management (ISM) is part of Information Security Governance (ISG). The IT Governance Institute (ITGI) states that ownership of data and its information risks are the responsibility of businesses and their owners (ITGI, 2005) as well as the IT department (Solms, 2005). The IT department might own the physical hardware and software assets, but not the data. To define security requirements in critical value chains and business processes, such as segregation of duties or use cases for logging, business involvement is required (S. Von Solms & R. Von Solms, 2009). Within this multidisciplinary context of Information

DOI: 10.4018/IJITBAG.2017070102

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Security we therefore use the term “Business Information Security” (V. Solms, 2005). Managing Business Information is a prerequisite for improving Business Information Security maturity (Allen, 2007). The International Federation of Accountants (IFAC) (IFAC, 2004) and ISACA (ISACA, 2012) describe information security as an integrated enterprise activity requiring proper governance of the work done in this area by the board and executive management.

Basie and Rossouw von Solms differentiate three levels: the strategic level (Board of Directors and Executive Management), the tactical level (Senior and middle management) and the operational level (lower management and administration). All directive setting and controlling activities (including monitoring and evaluating) are seen as part of the strategic level of governance (R. Von Solms & B. Von Solms, 2006). An example is the adoption of Information Security Control Frameworks such as the Information Security Forum (ISF) Standard of Good Practice. All activities designed to put these directives into practice take place at the tactical management level. The tactical level involves formulating policies and guidelines, for example establishing minimum standards that the organisation needs to adhere to, such as incident management and supply chain management. The level below the tactical level is where these policies and guidelines are translated into procedures and working methods. For example, this is the level where monitoring software is configured which triggers incident response processes or imposes stricter guidelines for suppliers. This paper focuses on defining artefact requirements for the strategic level which are substantiated by tactical and operational data.

Most of the contributions by practitioner’s bodies such as the ISACA (ISACA, 2012), the National Institute of Standards and Technology (NIST), the Information Security Forum (ISF) and the ITGI (ITGI, 2005) are prescriptive in nature (Koning & Bikker, 2013). Little academic research has been done on determining the BIS parameters which boards can use to improve their BIS maturity. This paper focusses on examining the “parameters of control”, that can function as requirements, via multiple qualitative research methods proposed by Johannesson and Perjons’ Design Science Research (DSR) Framework (Johannesson & Perjons, 2014). DSR aims to solve real problems by creating knowledge and understanding of a design problem and the solutions are acquired by establishing and applying artefacts. In this research, we therefore refer to an artefact that contributes in solving the Business Information Security at hand. This is why we formulated the following research question: Which research methods contribute to defining the requirements for the parameters of a Business Information Security artefact?

## **Structure of the Paper**

This paper first positions the main concepts of business information security and the problems at hand. It addresses the relevance of doing interpretivist qualitative research by making use of multiple research methods. These methods are being elaborated, in the fourth section of this paper, completed with their contribution towards BIS research and the way forward in artefact requirement setting. It concludes with the most relevant qualitative research methods, as part of DSR research, to be adopted in the continuation of this artefact research and development project. It positions two propositions, the first is on how to capture and structure the research data into the artefact (data and product view) and the second one is applying this data towards organisations in order to improve the BIS state (focuses on implementing the artefact and facilitating meetings), also referred to as Improving the Maturity of Business Information Security (MBIS). It finishes off with some examples of the methods being used in scientific and empirical studies and publications.

12 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/article/on-exploring-research-methods-for-business-information-security-alignment-and-artefact-engineering/189069](http://www.igi-global.com/article/on-exploring-research-methods-for-business-information-security-alignment-and-artefact-engineering/189069)

## Related Content

---

### Blockchain: A Disruptive Technology

Arish Sidiqqi and Kazi Jubaer Tansen (2022). *Blockchain Technology and Computational Excellence for Society 5.0* (pp. 48-58).

[www.irma-international.org/chapter/blockchain/295164](http://www.irma-international.org/chapter/blockchain/295164)

### Organizational Structure's Influence on Business-IT Alignment: Looking Back to Look Forward

Gideon Mekonnen Jonathan, Lazar Rusu and Erik Perjons (2018). *International Journal of IT/Business Alignment and Governance* (pp. 15-29).

[www.irma-international.org/article/organizational-structures-influence-on-business-it-alignment/220438](http://www.irma-international.org/article/organizational-structures-influence-on-business-it-alignment/220438)

### From Web Log to Data Warehouse: An Evolving Example

John M. Artz (2001). *Managing Internet and Intranet Technologies in Organizations: Challenges and Opportunities* (pp. 203-216).

[www.irma-international.org/chapter/web-log-data-warehouse/25895](http://www.irma-international.org/chapter/web-log-data-warehouse/25895)

### Cloud Computing: IT Governance, Legal, and Public Policy Aspects

Carlos Juiz and Victor Alexander de Pous (2014). *Organizational, Legal, and Technological Dimensions of Information System Administration* (pp. 139-166).

[www.irma-international.org/chapter/cloud-computing/80716](http://www.irma-international.org/chapter/cloud-computing/80716)

### The Intelligent Enterprise

Laurence Lock Lee (2009). *IT Governance in a Networked World: Multi-Sourcing Strategies and Social Capital for Corporate Computing* (pp. 54-82).

[www.irma-international.org/chapter/intelligent-enterprise/24746](http://www.irma-international.org/chapter/intelligent-enterprise/24746)