Auditing Advanced Information Systems and Technologies in a Modern Digital World

Egon Berghout, Rob Fijneman, Lennard Hendriks, Mona de Boer, and Bert-Jan Butijn

1 Introduction

Complex technology has been around ever since the start of computers. Maxwell Newman's first programmable computer Colossus in 1943 cracking World War II cryptography was a truly complex system at that time (Haigh & Ceruzzi, 2021). In 1965 Gordon Moore posited that the number of transistors on microchips doubles every 2 years, implying that the technical developments underlying our increasingly complex systems continue to develop at an impressive pace (Valacich & Schneider, 2022). We may therefore expect that the complexity of information systems will also continue to increase for the years ahead.

Due to the continuous development of the underlying technology, information systems take over increasingly complex tasks. An example of a currently cutting-edge task concerns autonomously driving cars. The computing power required for

E. Berghout (✉)
Erasmus University Rotterdam, Rotterdam, The Netherlands
e-mail: berghout@ese.eur.nl

R. Fijneman
TIAS School for Business and Society, Tilburg, The Netherlands
e-mail: r.g.a.fijneman@tilburguniversity.edu

L. Hendriks
Ernst and Young, Maarssen, The Netherlands
e-mail: lennard.hendriks@nl.ey.com

M. de Boer
PricewaterhouseCoopers, Amsterdam, The Netherlands
e-mail: mona.de.boer@pwc.com

B.-J. Butijn
Erasmus University Rotterdam, Rotterdam, The Netherlands
e-mail: butijn@ese.eur.nl

E. Berghout et al. (eds.), *Advanced Digital Auditing*, Progress in IS,
https://doi.org/10.1007/978-3-031-11089-4_1

image processing and interpretation is at the edge of today's capabilities. Autonomous-driving systems also affect our business and private lives and could possibly even run you over. Besides this increasing complexity of information systems themselves, there is also their accumulating interaction with people and other information systems.

The complexity of information systems also caused the emergence of the IT audit discipline in the late 1980s. IT auditors initially focused on the quality of financial reporting systems, however, also quickly deployed their knowledge in many other business domains. In this book we will explore the complexity of information systems and how we should develop the IT auditing discipline in order to control this complexity and maintain a trustworthy society.

2 Assurance Continuum

How do we know whether digital applications and solutions are sufficiently secure, are the answers generated by algorithms, for example, honest and fair, are we sufficiently resilient to cyberattacks and do we spend our money on the right digital solutions? These questions are extremely relevant for managers and supervisors of organizations as they must be able to account for their choices. Traditionally, the management report is a form of accountability for policy, which is fairly static in nature in the annual cycle. The Board report could explicitly discuss the digital agenda, and it has recently been explored whether an (external) IT audit "statement"[1] can also be added. Accountability for the quality of digital applications is taking on new dimensions now that developments are moving at lightning speed and everyone is linked to everyone. Certainties must be found on the digital highway.

These issues also play a role in our society. The protection of privacy is under considerable pressure, the numerous digital solutions build up a continuous personal profile. There are also painful examples of the use of algorithms in the public domain (Netherlands Court of Audit, 2021) that seriously harmed a number of citizens. According to the 2021 report on algorithms from the Court of Audit, responsible development of more complex automated applications requires thorough consideration and improved quality control. The social significance of aspects of digital integrity such as, honesty, fairness and security is increasing.

In the eighties of the last century, linked to the introduction of the Computer Crime Act (WCC I), an explicit link was created for the first time with accountability for automated data processing. Since 2019, the Computer Crime Act (WCC) III has been in effect, taking into account many developments in the field of cybersecurity and privacy. As the final element in the chain of control and accountability from WCC I, according to, for instance, the Dutch Civil Code 2, Article 393 paragraph 4, auditors must express their view on the reliability and continuity of the automated

[1] www.norea.nl

data processing insofar as it is relevant for the financial reporting. Many other countries have similar regulations and the European Union accepted the EU Cybersecurity Act and is developing a comprehensive European cybersecurity certification framework. More than 40 years later, we are dealing with complex legislation in the field of information systems and we use digital solutions that affect our administrative processes, but also almost all primary business functions. Consequently, the associated business and societal risk accumulate enormously.

Summarizing, there is an increasing need for quality control along the many new developments. How should accountability be organized, what role do directors and supervisory boards play in this, and how can IT auditing add value and balance risk? As indicated, these questions play a role not only at the individual organizational level, but also at the societal level. For example, how can the government restore or regain the trust of their citizens by explicitly accounting for the use of its digital solutions?

3 Technology Developments

Contemporary businesses maintain a complex mix of technology solutions, partly older (legacy) systems and new online (often front office) oriented solutions. Ensuring integrity of data, ensuring continuity, and being able to make the right investments versus costs for maintenance of older solutions remains challenging for almost all organizations. The following trends seem pertinent (WilroffReitsma, 2021; KPMG, 2020):

- *Flexible working* is becoming the norm. Over the past year, the cloud workplace has grown in popularity—more than predicted. Initially, employees had to start working from home because of COVID. However, soon appreciated this flexible way of working. The cloud-based workplace emerged quickly.
- *Distributed cloud* offers new opportunities. Cloud technology seems more economical for most organizations. Distributed cloud solutions may speed up data transfer, resolve compliance issues and further reduce cost. Storing data within specific geographic boundaries (often required by law or due to compliance) is an important reason for choosing the distributed cloud, where cloud solutions are offered in the proximity of the client.
- Business use of *Artificial Intelligence* (AI) is increasing, for example, chatbots and navigation apps. This technology will become increasingly prominent in businesses, also because computing power and software are becoming cheaper and more widely available. For example, AI will increasingly be used to analyse patterns from all kinds of data.
- *Internet of behaviours*. Today, large amounts of data are generated by many business processes and providing new insights, which plays an increasingly important role in strategic decision-making. Data-driven methods will increasingly be used to change human behaviour. Based on data analyses, suggestions or

autonomous actions can be developed that contribute to issues such as human safety and health. An example is the smartwatch that monitors blood pressure and oxygen levels and provides health tips based on that.
- Maturity of *5G mobile internet* in practice. In many European countries 5G mobile internet is now operational allowing many new applications, especially in the field of the Internet of Things and also autonomous vehicles.

Advancing technology and advancing software engineering practices, together with the increasing installed base of systems, allow the realization of increasingly complex systems. Indicators of system complexity are:

- The number of data entities in the system.
- The number of relations between the above data entities (the relationship as separate entity).
- The diversity of entities (and of relationships).
- The velocity with which entities are added to the system.
- The agility with which those systems can be adapted to new requirements.
- The context of the system, including the number of stakeholders and the systems' impact on these stakeholders.

Unfortunately, the only way to make complex information systems controllable is to add functionality and, therefore, making these systems again more difficult. IT auditors traditionally assessed the quality of financial information systems in order to protect external stakeholders from incorrect financial information; however, they will increasingly also assess non-financial information systems that particularly impact many stakeholders and probably also through a financial risk and return perspective. In analogy with the car industry, the liability of manufacturers remains important; however, this will not be sufficient to control the quality of high impact complex information systems. Comparable to the road readiness certification of cars, third party assurance granted by independent IT auditors remains an important tool to control the quality of complex digital systems.

4 Management Responsibilities

Managing and supervising digital solutions remains an extremely complex and often less desirable management topic. The complexity of technology is a deterrent, the mixture of legacy systems and new digital solutions reduces its transparency. Many stakeholders manage part of the technology chain and the quality requirements are accordingly complex. The introduction of new technology often includes major organizational changes and these changes subsequently introduce "winners" and "losers" in the new situations. Both of these groups will often unite and introduce additional complex political processes on top of the technological complexity. Furthermore, digital innovations always partly depend on external systems and consultants. These external stakeholders again accrue proprietary interests in the complex transition of the organization. This makes digital innovations often extremely difficult to manage, especially in more traditional organizations with vested interests.

Digital innovations, therefore, require extensive management attention, particularly from senior management and supervisory boards. Both value creation and risk management can be aligned with the COSO framework (Everson et al., 2017). Subsequently, one may opt for (parts of) the international COBIT (Control Objectives for Information Technology) framework (ISACA, 2018). In doing so, management makes explicit which management standards are applicable in and around the digital solutions and can determine their design as well as their operational functioning.

In view of all digital changes, new knowledge of the emerging technologies is constantly required. Organizing this in conjunction with an eye for the quality of the solutions and sometimes also the inherent limitations is what makes governance work well. Governance processes and structures require continuous evaluation and adjustments.

The suppliers of the digital solutions also play an important role. They provide increasingly better and safer, often cloud-based, solutions. Some suppliers tend to primarily focus on functional innovation than on cyber security and control. Buyers of digital solutions also insufficiently ask providers to develop “secure by design” systems. While designing the system, sufficient controls can, and should, be built in.

Is the tide turning, in other words are the new digital solutions becoming so complex that no one can determine the correctness of the content? It is not possible to opt for such a “black box” approach from the perspective of management responsibility. Management always remains responsible to balance risk and controls, and this book provides ample frameworks and techniques to do so.

5 Outline of This Book

This book encompasses a total of nine chapters. In the chapter hereafter (chapter “Auditing Complexity”), we will discuss the fundamentals and principles of auditing. Another topic the chapter touches upon is the effects of increasing technological complexity on the IT auditing discipline. The third chapter provides an introduction to several complex information systems like blockchain technology, artificial intelligence and cloud computing. This chapter provides the background for the chapters following thereafter that each present a framework to audit a complex technology. Chapter “The Intercompany Settlement Blockchain: Benefits, Risks, and Internal IT Controls” presents a framework to audit blockchain technology. The framework is based on a case study of a blockchain system implemented at the Royal Dutch KLM. An extensive description of the case, and an analysis of risks and controls of the blockchain system is presented. Following, in chapter “Understanding Algorithms” an extensive analysis of three case studies of algorithms is discussed that are used in practice by Dutch ministries. The analysis has resulted in a framework to audit algorithms in general, supplemented with considerations for algorithms that employ artificial intelligence. Building on the framework in chapter "Understanding Algorithms", chapter "Keeping Control on Deep Learning Image Recognition Algorithms" presents a framework specifically for image recognition. The framework is developed for the specific case wherein a large insurer has developed an algorithm to recognize damage to greenhouses. The seventh chapter introduces the concept of algorithm assurance, to give some background on the relevance and importance of algorithm assurance, and to prepare the auditor for the basic skills needed to organize and execute an algorithm audit. Evermore organizations are working in the cloud increasing the need for best practices and guidance on how to audit cloud-based services. Chapter "Demystifying Public Cloud Auditing for IT Auditors" discusses these best practices and provides guidance to IT auditors. Fortunately, advanced techniques are now also available to IT auditors to aid them in their work. One of these techniques is processes mining employed to lay bare processes within an IS. Chapter "Process Mining for Detailed Process Analysis" provides an elaborate background on process mining along with several examples of how to use it.

References

Everson, M. E. A., Chesley, D. L., Martens, F. J., Bagin, M., Katz, H., Sylvius, K. T., Perraglia, S. J., Zelnik, K. C., & Grimshaw, M. (2017). *Enterprise risk management: Integrating with strategy and performance*. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved from https://www.coso.org/pages/erm-framework-purchase.aspx

Haigh, T., & Ceruzzi, P. E. (2021). *A new history of modern computing*. MIT Press.

ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.

KPMG. (2020). *Harvey nash/KPMG CIO survey 2020: Everything changed. Or did it?* Retrieved from https://home.kpmg/xx/en/home/insights/2020/09/harvey-nash-kpmg-cio-survey-2020-everything-changed-or-did-it.html

Netherlands Court of Audit. (2021, January). *Understanding algorithms*. Retrieved from https://english.rekenkamer.nl/publications/reports/2021/01/26/understanding-algorithms#:~:text=The%20Court%20of%20Audit%20found,use%20and%20operation%20of%20algorithms

Valacich, J., & Schneider, C. (2022). *Information system today managing the digital world* (5th ed.). Prentice Hall.

WilroffReitsma. (2021, December 21). *ICT trends 2021: Dit zijn de 10 belangrijkste*. Retrieved March 25, 2022, from https://wilroffreitsma.nl/nieuws/ict-trends-2021/